March 7, 2016  
**Turner Construction**  
San Diego, California

Turner Construction notified individuals of a data breach when certain personal information was disclosed in an email to an unauthorized party.

The information included names, Social Security number, name of each state in which wages or taxes are reported, federal, state, local and Medicare earnings and tax withholding data.

The company is providing identity monitoring services through Kroll. For those affected call 1-877-451-9366.

More Information:  
[http://oag.ca.gov/ecrime/databreach/reports/sb24-60340](http://oag.ca.gov/ecrime/databreach/reports/sb24-60340)

March 6, 2016  
**Seagate**  
Scottsvalley, California

Seagate notified current and former employees of a data breach when an employee fell for a phishing attack that exposed W2 information of employees.

"Email scam artists last week tricked an employee at data storage giant Seagate Technology into giving away W-2 tax documents on all current and past employees, KrebsOnSecurity has learned. W-2 forms contain employee Social Security numbers, salaries and other personal data, and are highly prized by thieves involved in filing phony tax refund requests with the Internal Revenue Service (IRS) and the states."

The information compromised includes all information found on a W2 form, which includes Social Security numbers.

The company is not saying exactly how many individuals were affected at this time, only that "It’s accurate to say several thousand. But less 10,000 by a good amount."

More information:  

March 4, 2016  
**21st Century Oncology**  
Fort Meyers, Florida

21st Oncology notified individuals of a data breach of patient information via unauthorized access to their database.

The information compromised included names, Social Security numbers, physician's name, diagnosis and treatment information, and insurance information.

The company is offering Experian's Protect My ID to those who were affected.

More information:  
[http://oag.ca.gov/ecrime/databreach/reports/sb24-60307](http://oag.ca.gov/ecrime/databreach/reports/sb24-60307)

March 4, 2016  
**Snapchat**  
Venice, California

Snapchat has notified current and former employees of a phishing scam that targeted their payroll department that compromised employee information.
The information compromised included names, Snapchat employee ID, Social Security numbers, state of residence and work, 2015 wages earned, including stock-option gains, costs of company paid benefits for life and health insurance, relocation reimbursements, employee contributions to retirement, dependent care, and healthcare plans, additional required payments and taxes withheld.

More information: http://oag.ca.gov/ecrime/databreach/reports/sb24-60310

Information
Source: California Attorney General

February 26, 2016 Bailey's Inc.
Woodland, California BSO HACK 15000 credit/debit cards

Bailey's Inc. have notified customers of a data breach when an unauthorized party accessed their website server, obtaining credit card information of customers who purchased items from the company's online store.

More information: http://oag.ca.gov/ecrime/databreach/reports/sb24-59802

Information
Source: California Attorney General

February 18, 2016 Hollywood Presbyterian Hospital
New York, New York BSO HACK Unknown

Hollywood Presbyterian Hospital paid $17,000 in bitcoin in order to retrieve records they held for ransom against the hospital. The hackers installed a malicious ransomware on their server to hold patient records hostage so the hospital staff could not access any record.


Information
Source: Media

February 12, 2016 Magnolia Health Corporation
Tulare, California MED HACK Unknown

Magnolia Health Corporation has notified individuals of a data breach when someone impersonating the CEO in an email, obtained personal information for all active employees of the health center. Magnolia Health Corporation and each of their facilities managed including Twin Oaks Assisted Living, Inc., Twin Oaks Rehabilitation And Nursing Center, Inc., Porterville Convalescent, Inc., Kaweah Manor, Inc., Merritt Manor Inc.

The personal information compromised included employee numbers, names, addresses, city, state, zip code, sex, dates of birth, Social Security numbers, hire dates, seniority dates, salary/hourly, salary/rates, departments, job titles, last dates paid, and names of facility.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-60061

Information
Source: California Attorney General

February 10, 2016 Internal Revenue Service
Washington, District Of Columbia GOV HACK 101,000

"The IRS revealed on Tuesday that it discovered and stopped an automated cyberattack on its e-filing personal identification number (PIN) system last month. According to the IRS, the cybercriminals used information stolen "elsewhere outside the IRS" to generate e-file PINs for stolen Social Security numbers (SSNs). E-file PINs are used by some taxpayers to electronically file their tax returns.

Although no personal taxpayer data were compromised or disclosed by the breach, the IRS noted that the cybercriminals succeeded in using 101,000 SSNs to access e-file PINs (out of 464,000 attempts)."

The IRS is notifying individuals and placing markers on their tax accounts to try and catch any fraudulent tax returns being filed.


Information
Source: Media

February 9, 2016 Washington State Health Authority (HCA)
Washington, Washington GOV INSD 91,000

"The Washington State Health Authority (HCA) said Tuesday that an employee mishandled the Social Security numbers,
The employees involved worked at two different state agencies and they exchanged files of clients which violates HIPAA. They are not clear if any of the files were disseminated beyond the two employees who exchanged the files.


Information
Source: Media

February 8, 2016 BajaBound.com (Mexican Insurance Services) Baja, California

Bajabound.com notified customers of a data breach when they discovered an agent’s email account was compromised through a phishing attack. The company investigated the incident and the phishing was meant to collect email addresses.

The information that was compromised included names, addresses, dates of birth, driver’s license numbers, and credit card numbers.

More information: http://oag.ca.gov/ecrime/databreach/reports/sb24-60000

Information
Source: California Attorney General

February 5, 2016 Gyft Mountain View, California

Gyft notified customers of a data breach when they discovered unauthorized access to two cloud providers used by the company contained personal information of customers.

The information compromised included names, addresses, dates of birth, phone numbers, email addresses, and gift card numbers. Gift cards may have been used to make purchases on their site. The dates of the breach were March 19, 2015 and December 4, 2015.

For additional information on the breach go to www.myidcare.com/gyft.

More information: http://oag.ca.gov/ecrime/databreach/reports/sb24-59990

Information
Source: California Attorney General

February 4, 2016 University of Central Florida Orlando, Florida

The University of Central Florida notified current and former students of a data breach when they discovered unauthorized access into the university system.

The information compromised included financial records, medical records, grades and Social Security numbers.

"We have established a call center that you can contact at 877-752-5527 between 9 a.m. and 9 p.m. EST Monday through Friday if you have questions about this incident."

The university will be providing one year free of credit monitoring to those who were affected

More information: http://www.ucf.edu/datasecurity/

Information
Source: Security Breach Letter

February 2, 2016 Grx Holdings LLC dba Medicap Pharmacy West Des Moines, Iowa

Grx Holdings, LLC dba Medicap Pharmacy notified Health and Human Services of a data breach when they suffered a loss of information. There are no specifics as to what kind of loss it was or what type of information was compromised.

More information: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=9BF4AF...

Information
Source: Government Agency

February 2, 2016 Hawaii Medical Service Association (HMSA) Honolulu, Hawaii
HMSA notified 10,800 members of a data breach when letters communicating care management went to the wrong addresses.

The information compromised included patient names, management of certain health conditions and steps individuals could take to identify or treat an ailment.

"Members are encouraged to visit hmsa.com/media-center to see copies of the letters. Members who have questions about this mailing can visit an HMSA Center or office. They can also call (808) 948-6404 on Oahu and 1 (800) 459-3963 toll-free on the Neighbor Islands or the Mainland, from 8 a.m.- 5 p.m. Hawaii Time, Monday to Friday."

More information: [https://hmsa.com/media-center/2015/12/letter-error/](https://hmsa.com/media-center/2015/12/letter-error/)

February 1, 2016, IATSE Local 134
San Jose, California

IA 134 notified individuals of a data breach when a laptop that belonged to the organization was connected to a network at Levi’s Stadium was hacked compromising personal information.

Individual Social Security numbers may have been compromised.

More information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-59899](http://oag.ca.gov/ecrime/databreach/reports/sb24-59899)

February 1, 2016, Neiman Marcus
Dallas, Texas

Neiman Marcus has notified individuals of a data breach when the company discovered unauthorized access to online accounts on or around December 26, 2015.

The information compromised included usernames, passwords, names, mailing addresses, phone numbers, last four digits of payment card along with purchase histories.

"The firm suspects the attacker obtained the login credentials from large breaches at other companies where login names and passwords were stolen in order to gain unauthorized access to other accounts where victims might use the same credentials. Rawlinson said, customers will be required to reset their passwords on all NMG websites the next time they log into their accounts."


February 1, 2016, Tax Slayer
Evans, Georgia

Tax Slayer is notifying customers of a data breach that may have affected their 2014 tax return information. The company is stating that an unauthorized party accessed the information through a third party vendor. The company is not stating who the vendor is.

The information compromised included names, addresses, Social Security numbers, Social Security numbers of independents and other data contained in a tax return.

"The company is making $1 million worth of identity theft insurance available to those affected for one year along with credit monitoring for the same period. The company is recommending that these individuals change not only their TaxSlayer user names and passwords, but also those on any other accounts on which they are used."


January 29, 2016, Crown Point Health Center
Crown Point, Indiana

Crown Point Health Center notified Health and Human Services of a data breach when the company improperly disposed of paper health files. The specific information compromised was not communicated.


Information Source: Government Agency
Wendy’s, the fast food chain retailer, is investigating reports regarding a potential breach of their credit card systems in their restaurants. The company has hired a security expert to investigate the incidences.

The company received reports from their payment industry contacts alerting them of unusual activity and fraudulent charges after credit/debit cards were used at their locations for legitimate purchases.

A spokesperson for the restaurant chain stated, “We began investigating immediately, and the period of time we’re looking at the incidents is late last year,” he said. “We know it’s [affecting] some restaurants but it’s not appropriate just yet to speculate on anything in terms of scope.”

KrebsOnSecurity heard from banking industry sources stating a possible breach and the reports were coming mostly from financial institutions in the midwest. Krebs has also heard “similar reports from banks on the east coast”.

“The Wendy’s system includes approximately 6,500 franchise and company-operated restaurants in the United States and 28 countries and U.S. territories worldwide. Bertini said most of the U.S.-operated stores are franchises.”


UPDATE (3/2/2016): The Wendy’s credit/debit card breach appears to be much worse then originally thought, according to credit unions.

“This is what we’ve heard from three different credit union CEOs in Ohio now: It’s more concentrated and the amounts hitting compromised debit accounts is much higher that what they were hit with after Home Depot or Target,” Berger said. “It seems to have been been [the work of] a sophisticated group, in terms of the timing and the accounts they targeted. They were targeting and draining debit accounts with lots of money in them.”

More information: https://krebsonsecurity.com/2016/03/credit-unions-feeling-pinch-in-wendy...
January 25, 2016  California Virtual Academies  Simi Valley, California  

California Virtual Academies (CAVA) notified individuals of a data breach to their system. On December 9, 2015 the company discovered a "vulnerability in a data storage system" belonging to a third party provider.

For those with questions call 1-805-587-0202 Monday through Friday 8:00 a.m to 5:00 p.m Pacific Standard Time.

More information:  http://oag.ca.gov/ecrime/databreach/reports/sb24-59786

Information  
Source:  
California  
Attorney General  

January 25, 2016  Community Mercy Health Partners  Springfield, Ohio  

Community Mercy Health Partners notified Health and Human Services of a data breach when improper disposal of paper files was discovered. The specific information compromised was not communicated.

More information:  https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=9BF4AF...

Information  
Source:  
Government Agency  

January 25, 2016  Livongo Health Inc.  Chicago, Illinois  

Per Health and Human Services Livongo Health suffered a breach when paper files/films were breached. There is no information as to what type of information was compromised in the breach.

More information:  https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=9BF4AF...

Information  
Source:  
Government Agency  

January 25, 2016  University of Virginia  Charlottesville, Virginia  

The University of Virginia has notified employees of a data breach, when a cyber attack of their human resources system was discovered. The attack was initiated by a phishing email asking for usernames and passwords to their HR system and one or more employees fell for the phishing scam.

The information compromised included 1,400 W2’s (which includes names, addresses, Social Security numbers, etc) of employees and direct deposit banking information of an additional 40 employees. According to the university the attackers gained access to the system sometime in early November 2014 and continued through February 2015.

The FBI led investigation has resulted in the arrest of suspects who are currently being held in custody, no names have been released.


Information  
Source:  
Media  


Kicky Pants (previously spelled KicKee Pants) notified customers of a data breach when the company discovered unauthorized access into their system. The breach occurred between September 24, 2015 and December 26, 2015.

The information compromised included first and last names, credit card numbers, expiration dates, security codes on the back of cards, billing address, telephone numbers and email addresses.

The company is offering identity theft protection services through ID Experts. They can be reached at 1-866-833-7924 Monday through Friday 6 a.m to 6 p.m Pacific Standard Time. The deadline to enroll is April 22, 2016.

More information: http://oag.ca.gov/ecrime/databreach/reports/sb24-59770

Information  
Source:  
California  

January 25, 2016  University of Virginia  Charlottesville, Virginia  

The University of Virginia has notified employees of a data breach, when a cyber attack of their human resources system was discovered. The attack was initiated by a phishing email asking for usernames and passwords to their HR system and one or more employees fell for the phishing scam.

The information compromised included 1,400 W2’s (which includes names, addresses, Social Security numbers, etc) of employees and direct deposit banking information of an additional 40 employees. According to the university the attackers gained access to the system sometime in early November 2014 and continued through February 2015.

The FBI led investigation has resulted in the arrest of suspects who are currently being held in custody, no names have been released.


Information  
Source:  
Media  


Kicky Pants (previously spelled KicKee Pants) notified customers of a data breach when the company discovered unauthorized access into their system. The breach occurred between September 24, 2015 and December 26, 2015.

The information compromised included first and last names, credit card numbers, expiration dates, security codes on the back of cards, billing address, telephone numbers and email addresses.

The company is offering identity theft protection services through ID Experts. They can be reached at 1-866-833-7924 Monday through Friday 6 a.m to 6 p.m Pacific Standard Time. The deadline to enroll is April 22, 2016.

More information: http://oag.ca.gov/ecrime/databreach/reports/sb24-59770

Information  
Source:  
California  

January 25, 2016  Community Mercy Health Partners  Springfield, Ohio  

Community Mercy Health Partners notified Health and Human Services of a data breach when improper disposal of paper files was discovered. The specific information compromised was not communicated.

More information:  https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=9BF4AF...

Information  
Source:  
Government Agency  

January 25, 2016  Livongo Health Inc.  Chicago, Illinois  

Per Health and Human Services Livongo Health suffered a breach when paper files/films were breached. There is no information as to what type of information was compromised in the breach.

More information:  https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=9BF4AF...

Information  
Source:  
Government Agency  

January 25, 2016  University of Virginia  Charlottesville, Virginia  

The University of Virginia has notified employees of a data breach, when a cyber attack of their human resources system was discovered. The attack was initiated by a phishing email asking for usernames and passwords to their HR system and one or more employees fell for the phishing scam.

The information compromised included 1,400 W2’s (which includes names, addresses, Social Security numbers, etc) of employees and direct deposit banking information of an additional 40 employees. According to the university the attackers gained access to the system sometime in early November 2014 and continued through February 2015.

The FBI led investigation has resulted in the arrest of suspects who are currently being held in custody, no names have been released.


Information  
Source:  
Media  


Kicky Pants (previously spelled KicKee Pants) notified customers of a data breach when the company discovered unauthorized access into their system. The breach occurred between September 24, 2015 and December 26, 2015.

The information compromised included first and last names, credit card numbers, expiration dates, security codes on the back of cards, billing address, telephone numbers and email addresses.

The company is offering identity theft protection services through ID Experts. They can be reached at 1-866-833-7924 Monday through Friday 6 a.m to 6 p.m Pacific Standard Time. The deadline to enroll is April 22, 2016.

More information: http://oag.ca.gov/ecrime/databreach/reports/sb24-59770

Information  
Source:  
California  

January 25, 2016  California Virtual Academies  Simi Valley, California  

California Virtual Academies (CAVA) notified individuals of a data breach to their system. On December 9, 2015 the company discovered a "vulnerability in a data storage system" belonging to a third party provider.

For those with questions call 1-805-587-0202 Monday through Friday 8:00 a.m to 5:00 p.m Pacific Standard Time.

More information:  http://oag.ca.gov/ecrime/databreach/reports/sb24-59786

Information  
Source:  
California  
Attorney General  

January 25, 2016  Community Mercy Health Partners  Springfield, Ohio  

Community Mercy Health Partners notified Health and Human Services of a data breach when improper disposal of paper files was discovered. The specific information compromised was not communicated.

More information:  https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=9BF4AF...

Information  
Source:  
Government Agency  

January 25, 2016  Livongo Health Inc.  Chicago, Illinois  

Per Health and Human Services Livongo Health suffered a breach when paper files/films were breached. There is no information as to what type of information was compromised in the breach.

More information:  https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=9BF4AF...

Information  
Source:  
Government Agency  

January 25, 2016  University of Virginia  Charlottesville, Virginia  

The University of Virginia has notified employees of a data breach, when a cyber attack of their human resources system was discovered. The attack was initiated by a phishing email asking for usernames and passwords to their HR system and one or more employees fell for the phishing scam.

The information compromised included 1,400 W2’s (which includes names, addresses, Social Security numbers, etc) of employees and direct deposit banking information of an additional 40 employees. According to the university the attackers gained access to the system sometime in early November 2014 and continued through February 2015.

The FBI led investigation has resulted in the arrest of suspects who are currently being held in custody, no names have been released.


Information  
Source:  
Media  


Kicky Pants (previously spelled KicKee Pants) notified customers of a data breach when the company discovered unauthorized access into their system. The breach occurred between September 24, 2015 and December 26, 2015.

The information compromised included first and last names, credit card numbers, expiration dates, security codes on the back of cards, billing address, telephone numbers and email addresses.

The company is offering identity theft protection services through ID Experts. They can be reached at 1-866-833-7924 Monday through Friday 6 a.m to 6 p.m Pacific Standard Time. The deadline to enroll is April 22, 2016.

More information: http://oag.ca.gov/ecrime/databreach/reports/sb24-59770

Information  
Source:  
California
An individual contacted a local TV station regarding records found in a dumpster outside a strip mall in Indianapolis, Indiana. These documents were people's tax returns containing addresses, names and Social Security numbers.

The amount of individuals affected or the company that prepared the tax returns is not yet known.


January 18, 2016

Crest Foods
Oklahoma City, Oklahoma

An individual contacted a local news agency in Oklahoma City, Oklahoma when information on Crest Food employees was found in a dumpster at a recycling facility. The information this individual found on one employee included her application of employment, direct deposit form. Another individual's Social Security number and bank routing numbers were exposed.

The grocery store chain is currently investigating the issue with both their internal procedures and procedures with a third party vendor that they use to destroy sensitive information.


January 18, 2016

University of Northern Iowa
Cedar Falls, Iowa

Over 100 University of Northern Iowa employees reported that their tax returns had been rejected in 2014 because someone had filed a return fraudulently on their behalf, collecting their refund.

After further investigation, a 45 year old man, Bernard Ogie Oretekor has been charged with the tax identity theft when computers belonging to Oretekor in connection with a separate investigation, uncovered the information on the employees.

It is still not clear how Oretekor gained this information on the employees.


January 16, 2016

Gas and Shop
San Anselmo, California

The Central Marin Police have been investigating a skimming operation that as many as 20 people may have been victims of after the police received reports from individuals claiming that their credit/debit card information was compromised. The investigation revealed that skimming devices were placed on the gas pumps at the Gas and Shop station in San Anselmo.

"Police said the suspects used physical skimming devices to obtain the cards' information, and detectives have since checked all the gas pumps at the station to make sure the devices are no longer in place.

Police said they expected more than 20 people were victimized and the fraud has been occurring throughout Marin, Sonoma and Contra Costa counties."


January 16, 2016

Berks & Beyond Employment Services
Allentown, Pennsylvania

Stacks of paperwork from an employment agency was found dumped in containers at The City of Allentown Center for Recycling and Solid Waste. The files were not secure as they were placed in a public trash bin.

The information exposed included names, Social Security numbers, addresses and other information.


---

**Information Source:**

Media

**records from this breach used in our total:**

0 0 100 0 20 0
Per Health and Human Services, New West Health Services, dba New West Medicare suffered a data breach when a laptop went missing. The information compromised was not disclosed.

More information: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=9BF4AF...

Information
Source: Government

January 15, 2016 Virginia Department of Human Resources Management
Richmond, Virginia

The Department of Human Resources was notified by a third party that accidental disclosure of employee information was found on their website when improper redaction of documents was discovered.

The information exposed included Social Security numbers, and salary.

More information: http://www.databreaches.net/improper-redaction-exposed-virginia-employee...

Information
Source: Databreaches.net

January 15, 2016 Hyatt Hotels
Chicago, Illinois

The Hyatt hotel chain has notified individuals of a data breach when they discovered 250 of their 627 hotels were infected with malware that stole information, in particular, credit/debit card information.

The malware infected restaurants, spas, parking, golf shops, front desk reception.

The infection may have started as early as July 30, 2015 to December 8, 2015 and affecting hotels in US, UK, China, Germany, Japan, Italy, France, Russia and Canada.

Hyatt is offering one year of credit monitoring for free via CSID.

Click on the link for global list of sites

More information: http://www.zdnet.com/article/250-hyatt-hotels-infected-last-year-with-pa...

Information
Source: Media

January 14, 2016 G&S Medical Associates, LLC
Paterson, New Jersey

G&S Medical Associates, LLC suffered a data breach when a desktop computer was hacked. The type of information hacked was not disclosed by HHS.

More information: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=9BF4AF...

Information
Source: Government

January 14, 2016 Blue Shield of California
Los Angeles, California

Per Health and Human Services Blue Shield of California suffered a data breach when one of their network servers was hacked. No information was provided as to what information was compromised in the hack.

More information: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=9BF4AF...

Information
Source: Government

January 13, 2016 Tax Act
Cedar Rapids, Iowa

TaxAct has notified customers of a data breach when an unauthorized party or party's infiltrated their system.

"According to the letter dated January 11, TaxAct found evidence that certain accounts were entered between Nov. 10, 2015 and Dec. 4, 2015. The attacker viewed and possibly copied or printed stored tax returns and thus had access to Social Security numbers, addressed, names, driver's license numbers and bank account information."

The company has not released how many individuals were affected by this breach. They are claiming that less than 0.25
percent were affected. The company is offering one year free of credit monitoring and a $1 million dollar insurance reimbursement policy.

More information: http://www.scmagazine.com/taxact-breached-customer-banking-and-social-se-

Information
Source:
Media
January 12, 2016 JB Autosports
Des Moines, Iowa

JB Autosports, Inc. notified customers of a data breach when the system their check out page was the target of a cyberattack. The cyberattack affected customers who used their credit cards to pay for purchases from the company's website.

The information compromised included names, addresses, credit card numbers, credit card expiration dates, CID numbers, CAV2 numbers, CV2C numbers and CVV2 numbers.

More information: http://oag.ca.gov/ecrime/databreach/reports/sb24-59575

Information
Source:
California Attorney General
January 12, 2016 Rate My Professors
New York, New York

RateMyProfessors.com notified customers of a data breach when they discovered unauthorized access to a "Decommissioned Site" which allowed the hackers to gain access to the company's live site.

The information compromised included email addresses and passwords for registered users of the site. The site does not collect payment card information, Social Security numbers, driver's license numbers or insurance numbers.

The company is requiring individuals change their username and passwords.

More information: http://oag.ca.gov/ecrime/databreach/reports/sb24-59576

Information
Source:
California Attorney General
January 8, 2016 Time Warner Cable
San Diego, California

Time Warner Cable discovered that their online systems were hacked compromising the username and passwords of approximately 320,000 of its customers.

"The telecommunications giant says the FBI informed it of the apparent breach. As a precaution, the company is now contacting affected customers to advise them to change their account passwords."

More information: http://www.foxnews.com/tech/2016/01/08/time-warner-cable-says-320000-cus-

Information
Source:
Media
January 7, 2016 Aspire Indiana Inc.
Lebanon, Indiana

According to Health and Human Services Aspire Indiana Inc. suffered a data breach when a laptop was stolen from their facility. They did not report as to what specific personal information was on the laptop.

More information: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=9BF4AF-

Information
Source:
Government Agency
January 6, 2016 AHRC Nassau
Brookville, New York

Per Health and Human Services, AHRC Nassau suffered a data breach when unauthorized disclosure of files containing personal information was exposed. The specific information compromised was not communicated.

More information: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=9BF4AF-
January 6, 2016  McFadden
Glendale, Arizona

People who ate at McFadden’s received phone calls about fraudulent charges made to their credit card.

"The victims were told by their banks, the charges were made using a fake credit card. ABC15 found even more victims when we searched on Yelp. One writes, the manager told them they were aware of the problem, suggesting a problem with the bank."


Information Source: Media

January 6, 2016  Indiana University Health Arnett Hospital
Lafayette, Indiana

Indiana University Health Arnett Hospital notified patients of a data breach when the hospital became aware of a missing unencrypted flash drive from their emergency department.

The information compromised included patient information from emergency department visits, names, dates of birth, ages, home telephone numbers, medical record numbers, dates of service, diagnoses and treating physicians.


Information Source: Media

January 5, 2016  Southern New Hampshire University
Hooksett, New Hampshire

Southern New Hampshire University is investigating disclosure of a database that contained student information. The database contained more than 140,000 records including student names, email addresses, and ID’s, course name, course selection, assignment details and assignment score, instructor names and email addresses.

The University claims that a third party vendor exposed the data due to a configuration error.


Information Source: Media

January 5, 2016  Washington Hospital Healthcare System
Fremont, California

Washington Township Health Care District has notified individuals of a data breach to their system located in the Washington Community Health Resource Library. This system is used to maintain library identification cards.

The information compromised included names, addresses, and driver’s license numbers.

For questions call 1-888-668-9189 Monday through Friday 6:00 am to 6:00 pm PST.

**More information:** [http://oag.ca.gov/ecrime/databreach/reports/sb24-59419](http://oag.ca.gov/ecrime/databreach/reports/sb24-59419)

Information Source: California Attorney General

January 4, 2016  Elite Imaging
Aventura, Florida

Per Health and Human Services, Elite Imaging notified HHS of a data breach when they discovered paper files had been stolen. What specific personal information was compromised was not communicated.


Information Source: Government Agency

January 4, 2016  Regional Income Tax Agency
Brecksville, Ohio

The Regional Income Tax Agency notified individuals that it lost personal data when a DVD that contained copies of income tax documents went missing.

"The agency stored DVD’s off-site at a third party vendor’s facility. The missing DVD was discovered when RITA recalled..."
some DVDs to destroy them. The agency has moved to a new more secure backup system, making the DVDs obsolete, according to the agency."


**Information Source:** Media

December 31, 2015

**Hillsides**

**Los Angeles, California**

MED  DISC  Unknown

Hillsides is notifying individuals of a data breach when an employee send internal files that included personal information on both employees of the organization and patients of the organization.

The information included names, hiring dates, job titles, division descriptions, Social Security numbers, home addresses, zip codes and home phone numbers. In some instances the emails also included therapists names, Integrated System numbers, stard dates for services, outcome dates, parent partner names, names of rehabilitation specialists, rehab clinics, and gender.

For questions call 1-323-543-2800 between the hours of 8:30am through 4:30 pm Monday to Friday. Or email taikins@hillsides.org.

**More information:** [http://oag.ca.gov/ecrime/databreach/reports/sb24-59475](http://oag.ca.gov/ecrime/databreach/reports/sb24-59475)

**Information Source:** Media

December 28, 2015

**Unconfirmed**

**Unknown,**

BSO  DISC  191 million

The Hill has communicated that "Security bloggers and researchers claim to have uncovered a publicly available database exposing the personal information of 191 million voters on the Internet.

The information contains voters' names, home addresses, voter IDs, phone numbers and date of birth, as well as political affiliations and a detailed voting history since 2000."

In many states, this information is a matter of public record. However there are several states such as South Dakota that require confirmation of those who are using the information to consent that they will not use or sell the information for commercial purposes or placed on the Internet for anyone to access.

Currently, no company has claimed the database so it is unclear who the information belongs to or how the information was put up on the Internet. As more information is discovered, we will update as appropriate.


**Information Source:** Media

December 27, 2015

**Quincy Credit Union**

**Boston, Massachusetts**

BSF  HACK  670

Quincy Credit Union was a target of malware that allowed hackers to gain access to customers bank accounts when skimmers were found on ATM machines.

"Quincy Credit Union president Stewart Steele told WBZ-TV an estimated 670 accounts were impacted. Steele said he believes skimmers may have been placed on the ATM machines. It's unclear how much money was taken."


**Information Source:** Media

December 27, 2015

**University of Connecticut**

**Storrs, Connecticut**

EDU  HACK  Unknown

The University of Connecticut has notified individuals of a breach when malware was found on their website "prompting
visitors to download a malicious program posing as Adobe Flash Player, according to a university spokesman."


Information
Source: 

Media

December 23, 2015  
Matson Navigation Company (Horizon Lines)  
Phoenix, Arizona  
BSO  PORT  Unknown

Horizon Lines has notified mariners who served on vessels operated by Horizon Lines that a device containing their personal information has been identified as missing.

The device was first identified as potentially missing on or about December 7, 2015 and appears to have been lost between November 9 and December 7, 2015.

The device contained individualized information of mariners who have served aboard vessels operated by Horizon Lines since the year 2000. The information compromised included names, birth dates, addresses, telephone numbers, emergency contact information, Social Security numbers, and in some cases bank account and routing numbers, photocopies of passports, Transportation Worker Identification Credentials (TWIC), Merchant Mariner Documents (MMD) and Merchant Mariner Credentials (MMC), and copies of specific medical documents.

The company is offering AllClear ID for up to 12 months at no cost. For those affected call 1-855-711-5990.

More information: http://oag.ca.gov/ecrime/databreach/reports/sb24-59399

Information
Source: 

California Attorney General

December 23, 2015  
Acclaim Technical Services  
Huntington Beach, California  
BSO  HACK  Unknown

Acclaimed Technical Services has notified individuals of a data breach when their system was hacked compromising personal information of individuals who had a background check done with the company.

The information compromised included names, Social Security numbers, addresses, dates and places of birth, residency, educational and employment history, personal foreign travel history, information about immediate family, as well as business and other personal information contained in a background check.

More information: http://oag.ca.gov/ecrime/databreach/reports/sb24-59396

Information
Source: 

California Attorney General

December 22, 2015  
Alliance Health  
South Jordan, Utah  
MED  DISC  Unknown

Alliance Health has put up a notification on their site regarding a database breach that potentially exposed their customers personal health information.

"Alliance Health had a configuration error in its MongoDB Database installation. The leak was reported to Databreaches.net by Chris Vickery, who has uncovered other leaks including the Systema Software leak affecting numerous clients and millions of insurance or workers compensation claims."

Databreaches.net notified the company of the breach.

More information: http://www.databreaches.net/misconfigured-database-may-have-exposed-1-5-


Information
Source: 

Databreaches.net

December 22, 2015  
Thomas Nelson Community College  
Hampton, Virginia  
EDU  DISC  Unknown

Thomas Nelson Community College notified students of a data breach when their personal information was inadvertently sent to 11 current nursing students.

"We learned on December 9, 2015, that on December 8, 2015, your confidential student information to include name, address, phone number, social security number, student identification number, date of birth, immunization dates, background check results (no offenses listed), grades, and student progress indicators were emailed to eleven current nursing students. Each of the email recipients has been contacted and directed to permanently delete this information.

While there is no indication that your information has been misused in any way, as a precautionary measure, we are offering a complimentary one-year membership to Experian’s® ProtectMyID®."
HealthSouth Rehabilitation Hospital of Round Rock put out a notification on their site regarding a data breach after a laptop was stolen.

"HealthSouth Rehabilitation Hospital of Round Rock, previously Reliant Rehabilitation Hospital Central Texas, is currently notifying potentially affected individuals that a laptop containing unsecured protected health information was stolen from the trunk of an employee’s vehicle on or around Oct. 21, 2015. The information on the laptop varied by individual but may have included an individual’s name, address, date of birth, Social Security number, phone number, insurance number, diagnosis, referral ID number or medical record number. At this time, the hospital is working to notify the 1,359 potentially affected individuals via letter."

Dungarees has notified individuals of a data breach when they discovered their online store was hacked.

The hacking may have been compromised both debit and credit card numbers. The hacking may have compromised customer names, billing information, mailing information email addresses, credit and debit card information, the expiration dated, the CVV on the back of the card.

Hundreds of medical records belonging to Radiology Regional Center were found scattered on the roads in Fort Myers Florida.

The records included financial information on accounts, old phone bills invoice and registration information typically given at the front desk.

It appears that the container that the documents were in that were being collected for destruction by the county, opened and the papers flew out of the truck.

"An Oshkosh counseling center has notified 509 patients of a breach of personal and medical information after an October burglary.

Fox River Counseling Center, 627 Bay Shore Drive, is encouraging clients to change their passwords and monitor their accounts after someone stole an unsecured laptop Oct. 23, said Dr. Scott Trippe, a psychologist at the clinic. The computer contained outpatient mental health records of clients who visited the center from Nov. 7, 2012, to Aug. 19, 2014, and Wisconsin Disability Determination Bureau psychological evaluations from May 13, 2013, to Oct. 21, 2015.

Information included in the data breach included clients’ names, addresses, dates of birth, Social Security numbers, medical histories, mental status interviews, results of psychological testing, diagnoses and statements of work capacity, said Trippe, who himself had personal information on the laptop."

"An Oshkosh counseling center has notified 509 patients of a breach of personal and medical information after an October burglary.

Fox River Counseling Center, 627 Bay Shore Drive, is encouraging clients to change their passwords and monitor their accounts after someone stole an unsecured laptop Oct. 23, said Dr. Scott Trippe, a psychologist at the clinic. The computer contained outpatient mental health records of clients who visited the center from Nov. 7, 2012, to Aug. 19, 2014, and Wisconsin Disability Determination Bureau psychological evaluations from May 13, 2013, to Oct. 21, 2015.

Information included in the data breach included clients’ names, addresses, dates of birth, Social Security numbers, medical histories, mental status interviews, results of psychological testing, diagnoses and statements of work capacity, said Trippe, who himself had personal information on the laptop."
December 18, 2015  
Cottonwood Comfort Dental  
Albuquerque, New Mexico  
MED PHYS Unknown

Thousands of dental records from Cottonwood Comfort Dental were found scattered all over a New Mexico freeway. The paperwork contained addresses, insurance information and Social Security numbers.

The dental company said they have their paperwork shredded and is now investigating the incident.

More information: http://krqe.com/2015/12/18/new-mexicans-medical-records-dumped-along-wes...

Information Source: Media

December 18, 2015  
CBC Restaurant Corporation (Corner Bakery Cafe)  
Dallas, Texas  
BSO INSD Unknown

The Corner Bakery Corporation notified employees of a data breach when an ex-employee of the company may have stolen employee files with the intent to commit identity theft. The company has not been able to verify if this has happened.

The information that may have been exposed includes names, addresses, dates of birth and Social Security numbers.

More information: http://oag.ca.gov/ecrime/databreach/reports/sb24-59339

Information Source: California Attorney General

December 17, 2015  
Landry's  
Houston, Texas  
BSO HACK Unknown

Landry's has notified individuals of a data breach to their card payment systems. The restaurant/hotel and casino chain discovered unauthorized charges to debit and credit card of customers who dined at some of its restaurants.

The company owns 500 locations and owns a variety of brands including Bubba Gump Shrimp Co., Salt Grass Steak House, Willie G’s, the Aquarium, Vic & Anthony's downtown, Kemah Boardwalk, the Pleasure Pier and several Golden Nugget casinos and hotels.

The information compromised included names, card numbers, expiration dates and verification codes on the back of cards.

More information: http://www.chron.com/business/retail/article/Landry-s-investigates-payme...

Update (2/1/2016): Landry's has released the list of locations that were affected by the data breach. You can find the list here: http://www.landrysinc.com/protectingourcustomers/Locations.asp?loc=LDRY

For those with questions on this breach, call 877-238-2151 (U.S. and Canada), Monday through Friday from 9am to 7pm EST.

Information Source: Media

December 15, 2015  
Rivers Casino  
Pittsburgh, Pennsylvania  
BSO HACK Unknown

The Rivers Casino released a statement stating that their system had been infected with malware, but they are claiming that no customer information was compromised.

More information: http://pittsburgh.cbslocal.com/2015/12/15/rivers-casino-hit-with-compute...

Information Source: Media

December 15, 2015  
Toyota Financial Services  
Anaheim, California  
BSF DISC Unknown

Toyota Financial Services has contacted customers regarding a data breach when an unencrypted email that contained customer information was send to a third party vendor that worked on computer system enhancements for Toyota Financial Services.

The information exposed included Toyota Financial System account numbers, bank account numbers and bank routing numbers.

The company is offering one year of credit monitoring for free through ConsumerInfo.com, Inc through Experian. For questions call 1-877-371-7902.

More information: http://oag.ca.gov/ecrime/databreach/reports/sb24-59287
December 14, 2015  Sorrento Pacific Financial LLC
Sacramento, California

Sorrento Pacific Financial LLC notified the California Attorney General's office of a breach. No specifics were communicated on the AG's site.

More information: http://oag.ca.gov/ecrime/databreach/reports/sb24-59275

December 11, 2015  TuneCore
Brooklyn, New York

TuneCore, a music distribution site, notified customers of a data breach, when unauthorized access was discovered affecting potentially compromising customer information.

The information included Social Security numbers or taxpayer ID number, dates of birth, royalty statements for third quarter of 2015, names, addresses, email addresses, TuneCore account numbers, and passwords, billing addresses, last 4 digits of debit or credit card information, expiration dates of cards, last 4 digits of bank account numbers, and last four digits of banking account numbers.

More information: http://oag.ca.gov/ecrime/databreach/reports/sb24-59260

December 11, 2015  Northwest Primary Care
Portland, Oregon

Northwest Primary Care is notifying patients of a data breach when a former employee stole patient information.

The information compromised patient names, dates of birth, Social Security numbers, and credit card numbers. The employee took the information from April 2013 and December 2013.

More information: http://www.nwpc.com/

December 8, 2015  CM Ebar LLC (Elephant Bar restaurants)
Dallas, Texas

CM Ebar LLC (Elephant Bar restaurants) notified customers of a data breach when malware was discovered on their payment systems, potentially compromising customer debit and credit card information.

The breach affected restaurants in California, Colorado, Arizona, Missouri, Nevada, New Mexico, and Florida. The incident was discovered on November 3, 2015 and affective dates are anywhere from August 12, 2015 through December 4, 2015.

Information on specific restaurant locations and dates can be found in the link below.
http://www.elephantbar.com/incident/

(Any questions regarding the incident, individuals can call 1-888-578-5412)


December 8, 2015  George Hills Company Inc.
Sacramento, California

George Hills Company Inc. notified patients of a data breach when a third party software provider, Systema Software, notified the company of a configuration error that allowed unauthorized access to a temporary data backup of claims databases.

The information exposed included names, driver's license numbers, and medical information related to claims.

More information: http://oag.ca.gov/ecrime/databreach/reports/sb24-59212
Middlesex Hospital has notified patients of a data breach when four of its employees were victims of a phishing scam that enabled hackers to get into hospital records compromising patient information.

The information compromised included names, addresses, dates of birth, medical record numbers, medications they took, dates of service and diagnosis.


Muji USA notified customers of a data breach when they discovered malware on their online shopping portal which may have compromised their customers' personal information.

The information compromised included names, addresses, payment card numbers, the expiration dates of cards, the CVV code on the back of cards.

More information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-59200](http://oag.ca.gov/ecrime/databreach/reports/sb24-59200)

Blue Cross Blue Shield of Nebraska notified patients of a data breach when personal information was inadvertently disclosed on dental form claims.

"The company said a printing error caused some dental explanation of benefits forms to be sent to the wrong customers. The forms reveal treatment and services that the insurer paid on a customer's behalf. The company said an internal review found that 1,872 dental plan customers received mail statements that included another customer's name, member identification number and dental claim information. The forms did not disclose birth dates, Social Security numbers, or financial or employment information."


Dover School District has sent out a notification to volunteers that their personal information may have been compromised. The information included names, fingerprint cards and Social Security numbers.

A janitor working for the company S.J Services, accidentally placed envelopes that were to be sent to the state to do background checks on the volunteers, in a trash bag and put into a dumpster outside.

More information: [http://www.unionleader.com/Personal-information-for-Dover-volunteers-mis...](http://www.unionleader.com/Personal-information-for-Dover-volunteers-mis...)

Holly A. Nordhues CPA notified customers of a data breach when she discovered a cyberhack to a computer that housed customer information.

The information compromised included names, addresses, Social Security number, birthdates, sources of income and tax deductions.

She is offering AllClearID for 12 months at no cost. For those affected or questions call 1-877-676-0379.

More information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-59137](http://oag.ca.gov/ecrime/databreach/reports/sb24-59137)
Keenan and Associates, a third party administrator of health insurance benefits, notified individuals of a data breach when one of their vendors inadvertently exposed personal information when a security setting was not configured correctly on their portal system, potentially exposing the information.

The information compromised included names, addresses, telephone numbers, birth dates, medical plan names, plan identifiers and Social Security numbers.

The company is providing 24 months free of theft protection through Kroll. For those affected or with questions call 1-855-287-9328.

More information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-59125](http://oag.ca.gov/ecrime/databreach/reports/sb24-59125)

Cottage Health is notifying patients of a data breach when the personal health information was exposed inadvertently online from October 26, 2015 to November 8, 2015.

The information included patient and/or guarantor names, addresses, Social Security numbers, health insurance information and account numbers. Some medical and diagnosis information was also exposed.

The breach affects the following affiliated hospitals in the healthcare system:
- Goleta Valley Cottage Hospital
- Santa Ynez Valley Cottage Hospital
- Santa Barbara Cottage Hospital

The healthcare company is providing 12 months free of single- Bureau Credit Monitoring through TransUnion credit bureau.

For those with questions call 1-877-866-6056 Monday through Friday 6 am- 6 pm Pacific Time.

More information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-59101](http://oag.ca.gov/ecrime/databreach/reports/sb24-59101)

VTech, a Hong Kong based company notified customers of a data breach when hackers were able to gain access to childrens’ photos, chat logs, children's names, genders and birthdates, account email addresses, passwords, secret questions and answers for password retrieval, IP addresses, mailing addresses and download history.

"The majority of the people hacked - more than 2.2 million parents and nearly 2.9 million kids - are in the U.S. The hacks were spread across more than a dozen countries, including France, the U.K. and Germany."


Pathways Counseling Center has notified patients of a data breach when a company laptop assigned to an employee was stolen from the employees car on September 25, 2015.
The information contained on the laptop included patient names, Social Security numbers, dates of birth, addresses, diagnoses and/or clinical information, names of treating physician names, phone numbers, email addresses, demographic information, insurance information, types of treatments, prescription medication.

Pathways is offering one year free of credit monitoring services.


Information
Source: Health IT Security

November 30, 2015
Private Internet Access
Los Angeles, California

Customers of Private Internet Access were notified via email of a data breach when the company discovered a vulnerability to an IP address affecting the "port forwarding feature" of the service the company provided to customers.

"On November 17, we were privately notified of an IP address leak vulnerability affecting the port forwarding feature of our service. Essentially, anyone connecting to a forwarded port on any of our VPN gateways could have their real IP address leaked to an attacker specifically targeting a PIA user.

Within 12 hours of the initial report, we developed and tested what we thought was a complete fix, and deployed it to all of our VPN gateways.

On November 26, the researchers who discovered the vulnerability made it public and we quickly noticed that our service was still vulnerable to the IP address leak in certain cases, despite our initial fix. After further investigation, we also realized there was a separate but related issue on our desktop client. To fix this issue we are releasing updated VPN apps to prevent any leaks. We released v.52 on November 27."

The company is recommending anyone who uses their service to make sure they have the most recent release v.52 to avoid vulnerability.

More information: [http://www.databreaches.net/private-internet-access-notifies-customers-o...](http://www.databreaches.net/private-internet-access-notifies-customers-o...)

Information
Source: Databreaches.net

November 27, 2015
DeKalb County School System
Decatur, Georgia

DeKalb County School System notified teachers of a data breach when a mass email was sent out to the system's special education teachers. Sensitive information was exposed within the email which included first, middle and last names, and Social Security numbers.


Information
Source: Media

November 27, 2015
Rockland Nissan
Blauvelt,

A Rockland Nissan employee was arrested for identity theft after reportedly stealing customers' personal information to obtain and use their information to get credit cards. He charged more than $3,000 in charges.


Information
Source: Media

November 25, 2015
LANDesk
South Jordan, Utah

LANDesk, an IT automation firm has notified employees of a data breach when they discovered hackers had infiltrated their system and obtained personal information of current and former employees.

According to the company "it is possible that, through this compromise, hackers obtained personal information, including names and Social Security numbers, of some LANDESK employees and former Wavelink employees."


Information
Source: Krebs On Security

November 23, 2015
Yellowfront Grocery
Yellowfront Grocery has notified customers of a data breach when malware was discovered on the POS system called CSTARS of Maine, compromising customers debit and credit card statements. The grocery company is sure that the card numbers were compromised but it is still unclear whether or not additional information was stolen. CSTARS reported that card numbers and expiration dates were stolen and no other information was compromised.

CSTARS is communicating that the hackers were able to gain access through "compromised LogMeIn credentials."

"Authorities believe that cards used at the store between August 11, 2015 to October 16, 2015 are at risk of being compromised. The local branch of First Bancorp and Damariscotta Bank & Trust are replacing nearly 2,000 cards and 1,000 cards, respectively, in relation to the breach. Pierce said he’s heard some reports of fraud." More information: [http://www.scmagazine.com/yellowfront-grocery-notified-customers-via-fac...](http://www.scmagazine.com/yellowfront-grocery-notified-customers-via-fac...)

Jefferson County residents were alerted to a data breach of the Jefferson County Clerks office, when online county records exposed personal information of individuals.

The information exposed thousands of Social Security numbers of current and former Jefferson County residents.

"The issue lingers from an unresolved statewide privacy gap spotted almost a decade ago, when it became apparent county clerks were uploading old records containing personal information to their electronic databases."

"Jefferson County Clerk Carolyn Guidry said she is aware of the online disclosures but said her office lacks the resources to make comprehensive redactions to archived records. Instead, workers have taken a piecemeal approach to removing personal information from the archives, she said."


Starwood Hotel chain is the latest to have been affected by cyber criminals. The hotel has notified customers of exposure of credit/debit card information used at retail shops, gift shops and restaurants at W Hotels, Sheraton Hotels and Westin brands. 54 locations may have been affected and included credit/debit card numbers, names and security codes on the back of the cards.

"The locations and potential dates of exposure for each affected Starwood property is available at [www.starwoodhotels.com/paymentcardsecuritynotice](http://www.starwoodhotels.com/paymentcardsecuritynotice). Customers with questions may call 1-855-270-9179 (U.S. and Canada) or 1-512-201-2201 (International), Monday through Saturday, 8:00 am to 8:00 pm CST or visit [www.starwoodhotels.com/paymentcardsecuritynotice](http://www.starwoodhotels.com/paymentcardsecuritynotice) for more information."


Grainger has notified customers of a data breach when their IT team "recently identified a coding error in the Grainger.com mobile apps for iPhone and Android that resulted in the collection and storage of unsecured user names and passwords on the Grainger system." This particular database could be accessed by unauthorized users.

The company has implement a reset of users passwords to their Grainger.com system. For those with questions or support can call 1-847-647-3275.


Grainger has notified customers of a data breach when their IT team "recently identified a coding error in the Grainger.com mobile apps for iPhone and Android that resulted in the collection and storage of unsecured user names and passwords on the Grainger system." This particular database could be accessed by unauthorized users.

The company has implement a reset of users passwords to their Grainger.com system. For those with questions or support can call 1-847-647-3275.

The Georgia Secretary of State, Brian Kemps office is being sued by two Georgia women who claim that the Secretary's office released personal information that involves 6 million Georgia voters.

Mr. Kemps office has communicated that his office released information to media, political parties and other paying subscribers who legally buy voter information from the state, but due to what they are calling a “clerical” error, individual voters personal information was included in these files.

12 separate entities received the files that contained 6 million Georgia voters and inadvertently included drivers license information, Social Security numbers and dates of birth. It is legal for the state to release public voter information, but the information is only supposed to include voter’s name, residential or mailing address, race, gender, registration date and last voting date.

According to the lawsuit, Mr. Kemps office never notified individuals regarding the breach, nor did they contact the consumer reporting agencies.


---

Dallas County Texas has admitted to a data breach of residents information that has been accessible online for over 6 months. The information included names, addresses, Social Security numbers and birth dates of residents, including children.

The county has had over 6 months to pull the data offline, however as of the time of this report by CBS the information had not yet been pulled.


---

Swiss Cleaners notified customers of a data breach to their credit card system that may have compromised customers debit/credit card information.

The company investigated the incident and discovered malware on their system that handles their payment card system. The malware made copies of the payment card information as it was being routed from Swiss Cleaners system to the payment processor. The malware installed gathered cardholder names, card numbers, expiration dates and the verification code on the back of cards.

The cards compromised were used at the location at 35 Windsor Avenue, PO Box 825, Vernon Connecticut from December 30, 2014 through October 26, 2015 as well as any other Swiss Cleaner stores from December 30, 2014 through October 23, 2015. The breach affected the company's drycleaning services only.

For those affected with questions call 1-888-760-4869 Monday-Friday 9 am to 9 pm EST.


---

Fashion Figure is notifying customers of a data breach to their system when they discovered unauthorized access to names, customer ID’s, addresses, phone numbers, email addresses, and credit card information. After investigation, the company found malware installed on their webserver.
The company is providing ID Experts for free for one year for those who were affected. For those with questions call 1-877-868-0171 Monday through Friday from 8:00 am-8:00 pm CST.

More information: https://oag.ca.gov/ecrime/databreach/reports/sb24-58851

Information
Source: California Attorney General
November 9, 2015
California Department of Motor Vehicles
Sacramento, California

The California Department of Motor Vehicles notified individuals of a data breach when one of the agencies employees inadvertently sent a file with individual drivers license numbers and names to the Riverside Probation Department.

More information: http://oag.ca.gov/ecrime/databreach/reports/sb24-58698

Information
Source: California Attorney General

November 9, 2015
Comcast
Pomona, California

Comcast may be the latest victim of a breach when 590,000 customer email addresses and passwords were posted on the Dark Web website, an underground site selling people's information for money. The company is denying that they were a victim of a breach, and were "certain that none of their systems or apps had been compromised."

The company took precaution and reset passwords of those affected.

"Over the weekend, a reader (@flanvel) directed Salted Hash to a post on a Dark Web marketplace selling a number of questionable, if not outright illegal goods. The post in question offered a list of 590,000 Comcast email addresses and corresponding passwords.

As proof, the seller offered a brief list of 112 accounts with a going rate of $300 USD for 100,000 accounts. However, one wished to purchase the entire list of 590,000 accounts, the final price was $1,000 USD."

More information: http://www.csoonline.com/article/3002604/cyber-attacks-espionage/comcast...

Information
Source: Media
November 4, 2015
Avis Budget Group
Parsippany, New Jersey

Avis Budget Group notified customers of a data breach when the third-party provider that manages their open enrollment process accidentally sent a file to another company that is also their client.

The information exposed to this other client included names, addresses and Social Security numbers. For those affected the company is offering a Experian's ProtectMyID for free for one year.

More information: http://oag.ca.gov/ecrime/databreach/reports/sb24-58635

Information
Source: California Attorney General
November 2, 2015
Accuform Signs
Brooksville, Florida

Accuform Signs notified customers of a data breach when they noticed order information from their site and possible the site of a distributor of the company, which was hacked from an outside source.

The information compromised included names, addresses, emails, phone and credit card information.

For those with questions, call 1-800-233-3352 8 a.m- 7 p.m EST or go to www.safetybreach.info.

More information: http://oag.ca.gov/ecrime/databreach/reports/sb24-58598

Information
Source: California Attorney General
October 30, 2015
American Bankers Association
Washington, District Of Columbia

American Bankers Association notified individuals of a data breach of their Shopping Cart affecting 6,400 records. The
information compromised included Shopping Cart user names and passwords, which were posted online. At this time the
cOMPANY has stated that they do not believe that any financial information was compromised.

More information: http://oag.ca.gov/echrome/databreach/reports/sb24-58430

Information
Source: California Attorney General
October 29, 2015 Stiletto Solutions
Inglewood, California

Stiletto Solutions notified consumers of a data breach when they noticed suspicious activity on their e-Commerce server
which may have compromised customers personal information.
The information compromised included customer credit/debit card information, the CVV code on the back of the cards,
names, billing and shipping addresses, e-mails, usernames and passwords. Customers affected used their cards between
November 1, 2013 through September 16, 2015.

More information: http://oag.ca.gov/echrome/databreach/reports/sb24-58547

Information
Source: California Attorney General
October 28, 2015 Digital Theatre, LLC (ShowTix4U)
Las Vegas, Nevada

Digital Theatre, LLC which operates ShowTix4U notified individuals of a data breach when some payment cards were
affected. Investigators found between late April 2015 and late September 2015 unauthorized access was discovered on a
computer server hosting ShowTix4U’s website.
The information compromised names, addresses, payment card account numbers, card expiration dates, and payment card
security codes of customers.

More information: http://oag.ca.gov/echrome/databreach/reports/sb24-58535

Information
Source: California Attorney General
October 26, 2015 Emergence Health Network
El Paso, Texas

Emergence Health Network has notified patients of a data breach to their system when a server was accessed without
authorization.
“It is not apparent that any medical information was disclosed based upon a third-party audit of the computer server and
EHN does not have any proof that information such as social security number, date of birth, home address, was accessed
or otherwise misused”

More information: http://emergencehealthnetwork.org/wp-content/uploads/2015/10/EHN-Compute...

Information
Source: HHS via Databreaches.net
Databreaches.net
October 22, 2015 Noble House and Resorts
Kirkland, Washington

The Nobel House Hotels and Resorts notified customers of a data breach when guests informed them of unauthorized
charges on their payment cards used at one of their hotels, The Commons.
The company identified malware on the payment card system on September 25, 2015. The information compromised
included cardholder name, card numbers, expired dates, and the CVV number on the back of the cards. The dates cards
were potentially compromised were from January 28, 2015 to August 3, 2015.

More information: http://oag.ca.gov/system/files/General%20Notice_0.pdf?

Information
Source: California Attorney General
October 22, 2015 Xero
San Francisco, California
The online accounting software company Xero is notifying customers of a data breach when "a small number" of their customers had their accounts compromised. In particular, they had been seeing a large increase in phishing scams pretending to be the company.

The company is asking those who are compromised to change their account passwords.


---

The county of Osceola in Florida, specifically the Juvenile Division of the Clerk of Courts, when children's information was inadvertently exposed on their website. The names for every child charged in court cases and names of children in their foster system were exposed online via their e-file system.

Currently the disclosure is being investigated.

Currently the disclosure is being investigated.


Information
Source: Media
October 16, 2015 Department of Health and Human Services
Granville, North Carolina
MED DISC 1,615

The Department of Health and Human Services (DHHS) in Granville County North Carolina notified patients of a data breach when an employee inadvertently sent an email to the Granville County Health Department when the file was not encrypted.

The information compromised included first and last names, Medicaid identification numbers, provider names, provider ID numbers, and other Medicaid related services.

For those with questions call 1-800-662-7030.


Information
Source: Media
October 16, 2015 Community Catalysts of California
San Diego, California
NGO PORT 1,182

Community Catalysts of California notified customers of a data breach that may have compromised their information when a thumb drive was stolen from an employee’s car.

The information included names, addresses, diagnosis, dates of birth, ages, genders and telephone numbers. They are claiming that no Social Security number, financial account numbers, medications or client identification numbers were compromised.

For those with questions call Alesia Forte at (888) 344-1237 Monday through Friday from 8:30 a.m. through 5:00 p.m, Pacific Time.

More information: http://oag.ca.gov/ecrime/databreach/reports/sb24-58324

Information
Source: California Attorney General
October 16, 2015 NextBus
Emeryville, California
BSO HACK Unknown

NextBus has notified customers of a data breach to their system that disclosed usernames, email addresses, telephone numbers and passwords of customers.

The company is advising customers to change their passwords.

More information: http://oag.ca.gov/ecrime/databreach/reports/sb24-58315
October 16, 2015

**Scripps Network LLC. (Food.com)**
Knocksville, Tennessee

Food.com notified customers of a databreach to their system that may have affected emails, usernames and passwords. These credentials were used to login onto the site for managing their recipe box and posting recipes on the site. These same credentials are used to Foodnetwork.com website as well as mobile applications through the site.

This intrusion occurred between August 8, 2015 and September 2, 2015. According to the company no financial information or Social Security information was compromised.

The company is recommending that customers change their usernames and passwords. Those with questions can call 1-800-380-6336 between 9 a.m. through 7 p.m. EST Monday to Friday and use the reference number 1031100715.

More information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-58311](http://oag.ca.gov/ecrime/databreach/reports/sb24-58311)

---

October 14, 2015

**University of Oklahoma's Urology Clinic**
Oklahoma City, Oklahoma

The University of Oklahoma College of Medicine - Department of Obstetrics & Gynecology notified patients of a data breach when a physicians laptop was stolen from their car.

"The laptop had a list of information on it related to two groups of individuals. For one group of individuals, the information included full name, medical record number, date of birth, age, the name and date of a gynecologic or urogynecologic medical procedure, patient account number, and admission and discharge dates for that procedure (if the procedure was an inpatient procedure). Social Security numbers and credit card numbers were not included. Addresses were not included. These individuals had gynecologic or urogynecologic procedures at the OU Outpatient Surgery Center or the Presbyterian Tower between January 1, 2009, and December 31, 2014. The information for other group of individuals included last name and first initial, age, and information related to pregnancy, such as lab results and medications, delivery date, and problem and allergy list."

More information: [https://www.oumedicine.com/OBGYN/contact-us](https://www.oumedicine.com/OBGYN/contact-us)

---

October 13, 2015

**Uber**
San Francisco, California

The "Uber partner" app that was designed by the company apparently has leaked drivers information which included their license and Social Security number.

An Uber driver found the glitch and communicated his findings with a reporter.


Update (1/7/2016): New York has agreed to a $20,000 settlement with Uber over their "god view" rider-tracking system that compromised driver information.


---

October 13, 2015

**Streets of New York**
Phoenix, Arizona

The Streets of New York restaurant in Phoenix Arizona notified customers of a breach when hackers infiltrated the payment card system of the restaurant. According to the restaurant a few hundred customers were affected. The hackers then tried extorting the owners for $10,000.


---

October 13, 2015

**Peppermill Resort Spa & Casino**
Reno, Nevada

The Peppermill Resort Spa & Casino notified customers of a breach when their front desk system compromising customer payment card information and the security codes on the back of the cards.

According to the casino, the hack occurred between October 12, 2014 and February 16, 2015. The casino was asked to delay notifying individuals by federal authorities while they investigated the incidence.
October 13, 2015  **Uniformed Services University**  
**Bethesda, Maryland**  
EDU  
HACK  
Unknown

A hacker by the name of Kuroi SH infiltrated the United States based Uniformed Services University (USU) leaking 2014 login credentials online.

USU educates service members in for the military’s medical corps in the US and abroad. The university also provides training to military physicians, nurses and educators.

“The hacker uploaded a deface page on 8 of the USU websites on which a database of all the websites, names, emails and clear-text passwords of those working for the university are held.”

**Information**  
Source: Media  

October 13, 2015  **Service Systems Associates, Inc.**  
**Denver, Colorado**  
BSO  
HACK  
60,000

Service Systems Associates, Inc. notified customers of a data breach when their point-of-sale software contained malware that compromised payment card information of individuals who visited gift shops in several zoos from March 24 and May 20, 2015.

The following zoo locations were affected:
- Dallas Zoo
- Detroit Zoo
- El Paso Zoo
- Fresno Chaffee Zoo
- Herman Park Conservancy
- Honolulu Zoo
- Houston Zoo
- Zoo Miami
- Museum of Science and Industry (Tampa Florida)
- Pittsburgh Zoo & PPG Aquarium


**More information:**  
[http://oag.ca.gov/ecrime/databreach/reports/sb24-58264](http://oag.ca.gov/ecrime/databreach/reports/sb24-58264)

**UPDATE** (10/20/2015): Service Systems Associates lawyer sent a letter to the New Hampshire Attorney General’s office affected approximately 60,000 consumer credit cards.

**More information:**  

October 12, 2015  **Dow Jones & Company**  
**New York, New York**  
BSF  
HACK  
3,500

Down Jones & Company notified individuals of a breach when they discovered unauthorized access to their system, affecting payment card information of customers.

The unauthorized access also included names, addresses, email addresses and phone numbers of current and former subscribers.

**More information:**  

**Company letter:**  
Humana is notifying Wisconsin members of a breach of customers information after an employee’s vehicle was broken into and a company laptop was stolen along with a file containing customer information.

The information compromised included member names, dates of birth, Humana and clinic names. The documents also included Humana member identification numbers of 250 of those individuals.

More information: http://www.wsaw.com/home/headlines/Laptop-with-Humana-member-information...

The Vacaville Housing Authority (VHA) notified individuals of a data breach when a VHA employee inadvertently sent an email with a file that had customers personal information in it.

The information included names and Social Security numbers. The file reportedly was sent to only one person and she immediately contacted the VHA. According to the VHA authorities verified that the email was deleted from this persons computer.

The VHA is offering 12 months free of credit monitoring services through Kroll for those individuals that were affected.

More information: http://oag.ca.gov/ecrime/databreach/reports/sb24-58203

America’s Thrift Stores notified customers of a data breach when they thrift store chain discovered the software used through a third-party service provider was compromised.

The hacking, allegedly from Eastern Europe, compromised customer credit card or debit card information was compromised.

More information: www.waaytv.com/appnews/data-breach-at-americas-thrift-store/article_54d...

CarePlus Health Plans have notified customers of a data breach when an error in processing their statements exposed their personal information to other members. The machine that processed these statement had a programming error that inserted two statements into one envelope vs. just one.

According to the company, no Social Security numbers were on these statements. The information compromised included names, addresses and CarePlus identification numbers.

For those affected, call 1-800-794-5907 from 8:00 a.m. to 8 p.m EST seven days a week.


E-Trade has notified customers that their information may have been compromised as a result of a hacking to their system back in 2013.

E-Trade claims that there was no evidence that any sensitive information was compromised such as Social Security
numbers or financial information. The information they are stating was compromised were customer email names, email and physical addresses.

E-Trade learned of the cyberattack shortly after it occurred in 2013 and launched an internal investigation while it worked with law enforcement, according to a person familiar with the investigation who spoke on the condition of anonymity. But at the time, the company did not believe customer information had been compromised, the person said.

Recently, however, federal law enforcement officials alerted the company to evidence that customer contact information may have been breached, prompting E-Trade to inform customers about the incident "out of an abundance of caution," according to the e-mail."

More information: https://www.washingtonpost.com/news/the-switch/wp/2015/10/09/e-trade-not...

Information
Source:                 Media
October 8, 2015  GlamGlow Hollywood, California            BSO      HACK     Unknown

GlamGlow notified customers of a data breach when their online ecommerce site was compromised. The information accessed occurred between September 19 and September 21, 2014 and May 12 and May 15, 2015 and included names, addresses, telephone numbers, payment card numbers, expiration dates, security codes, email addresses and GlamGlow account passwords.

For those affected with questions call 1-800-219-2031 between 9:30 am and 4:30 pm EST.

More information: http://oag.ca.gov/ecrime/databreach/reports/sb24-58194

Information
Source:                 Media
October 8, 2015  North Shore Care Supply Austin, Texas            BSO      HACK     Unknown

North Shore Care Supply notified customers of a data breach when their online ecommerce site was compromised exposing customers' personal information.

The information accessed included debit/credit card information, names, addresses, card numbers, verification codes and expiration dates. Online purchases made between June 7, 2015 and August 24, 2015 are at risk.

The company has set up AllClearID for 12 months for free. Those affected can call 1-855-229-0069.

More information: http://oag.ca.gov/ecrime/databreach/reports/sb24-58183

Information
Source:                 Media
October 6, 2015  Lake Norman High School Mooresville, California            EDU      DISC     Unknown

Lake Norman High School notified students of a breach when a Lake Norman High School student who obtained an administrative password, however the student was able to manipulate the script that contains the admin password.

“We have a script that we send out that runs on the computers that does contain the admin password,” Blattner said in an email. "It runs and then deletes itself...The file was made invisible and the script to delete the file was provided by the software manufacturer, but it did not work as designed."

Seven students used the password to access school computers were charged with accessing computers without authorization by the Iredell County Sheriff's Office.


Information
Source:                 Media
October 6, 2015  Affinity Health Plan Bronx, New York            MED      DISC     Unknown

Affinity Health Plan (AHP) notified customers of a data breach when letters for renewing Child Health Plus for customers children, contained on the back of the letter information and addressed of another Affinity member. “This led to a number of Affinity members’ information being shared with other Affinity members.”

This was a printing error that included information on another Affinity member including their children’s names, addresses, and AHP identification numbers. The company is reporting that no children's health information or Social Security numbers were disclosed.

Letter released to members: http://www.affinityplan.org/uploadedFiles/Affinity/Who_We_Are/Press_Rele...

Information Source: Health IT Security

October 3, 2015  **Sentara Heart Hospital**
**Suffolk, Virginia**

MED INSD 1040

Sentara Heart Hospital notified patients of a data breach when two portable hard drives were stolen. According to authorities the theft occurred the weekend of August 14, 2015.

The information on the hard drives included birthdates, names, diagnoses, types of procedures and other clinical notes. According to the clinic no Social Security numbers or addresses were on the portable drives.

For those affected can call 844-322-8235 between 8 a.m. and 6 p.m. and refer to incident No. COE151471.


Information Source: Media

October 2, 2015  **Sentara Heart Hospital**
**Norfolk, Virginia**

MED PORT 1,040

Schwab Retirement Plan Services Inc. (SRPS), notified customers of a data breach when a spreadsheet containing Social Security numbers, names, addresses, dates of birth, dates of termination, employment status, division code, marital status and account balance was accidentally emailed to a participant in another retirement plan serviced by SRPS.

For those affected they can call 1-800-724-7526.


Information Source: California Attorney General

October 1, 2015  **American Bankers Association**
**Washington, District Of Columbia**

BSF HACK 6,400

The American Bankers Association has notified customers of a data breach when email addresses and passwords used to make purchases on their site or used to register for events were compromised.

“6,400 users’ records had been posted online, the trade group said, though there was no evidence that credit card or other personal financial information had been accessed.”


Information Source: Media

October 1, 2015  **Scottrade**
**St. Louis, Missouri**

BSF HACK 4,600,000

Scottrade notified customers of a data breach, when one of their systems was hacked into exposing customers records.

The information compromised included client names and street addresses.

The company is providing AllClear ID to those affected for one year for free. Those affected can call 855-229-0083 Monday through Saturday 8:00 am to 8:00 pm.

*More information: [https://oag.ca.gov/system/files/Scottrade%20California%20notice%20only%2...](https://oag.ca.gov/system/files/Scottrade%20California%20notice%20only%2...)*

*UPDATED (10/2/2015): The Scottstrade data breach appears to have affected 4.6 million customers. The company stated “Based upon our subsequent internal investigation coupled with information provided by the authorities, we believe a list of client names and street addresses was taken from our system,” the email notice reads. “Importantly, we have no reason to believe that Scottrade’s trading platforms or any client funds were compromised. All client passwords remained encrypted at all times and we have not seen any indication of fraudulent activity as a result of this incident.” The notice sent out also stated that “that although Social Security numbers, email addresses and other sensitive data were contained in the system accessed, “it appears that contact information was the focus of the incident.”*
Experian has announced a breach to their system affecting over 15 million T-Mobile customers. T-Mobile uses Experian to run credit checks on potential customers.

"Who Is Affected

Experian said the incident is "isolated" and is only limited to consumers who applied for T-Mobile USA services between Sept. 1, 2013, and Sept. 16, 2015.

What's Been Exposed

The information exposed to hackers includes names, addresses, social security numbers, dates of birth, and various identification numbers, including a passport, driver's license or military identification number, according to Experian.

T-Mobile is offering 2 years free of identity theft monitoring services through Experian.


UPDATE (10/07/2015): T-Mobile is now offering a secondary service to customers who were part of the Experian breach that is not an Experian service. See the link below for the information.

[https://www.csid.com/t-mobile/]

Barrington Orthopedic Specialists notified patients of data breach when a laptop and EMG machine was stolen from their offices.

The information compromised included patient names, dates of birth and EMG results and reports.


"An inspector general’s report revealed that Palo Alto’s Department of Veterans Affairs facility provided patient information to a private IT company whose employees had not been cleared through background checks."

The investigation was initiated when a complaint by House Committee on Veteran’s Affairs alleged that the Informatics Chief at the Palo Alto VA had "entered into an illegal agreement with a healthcare tech company, Kyron, for sharing patient information."

According to the VA, they removed identifiable information prior to releasing this data to Kyron. The Office of Inspector General determined that the VA did not verify whether or not the individuals at Kyron had received background checks prior to handling this type of sensitive information. Nor did the receive proper security or privacy training.

They also discovered that the information loaded into Kryon’s software was not yet approved by VA Information security officers prior to installation.


The Big Blue Bus has notified customers of a data breach when the company discovered unauthorized access at NextBus, a third party company that Big Blue Bus works with to provide real-time bus arrival information to customers.
The individual(s) may have gained access to account information of customers. The company claims that no Social Security numbers or financial information was compromised. The company is recommending that customers change their passwords and to watch for potential phishing scams.

For those with questions call 1-877-639-8287.


<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 25, 2015</td>
<td>Hilton Hotels McClean, Virginia</td>
<td>BSO HACK Unknown</td>
</tr>
</tbody>
</table>

"Multiple sources in the banking industry say they have traced a pattern of credit card fraud that suggests hackers have compromised point-of-sale registers in gift shops and restaurants at a large number of Hilton Hotel and franchise properties across the United States. Hilton says it is investigating the claims."

According to Krebs on Security, five banks have determined that a breach of credit card payment systems has a common thread in that they were all used at Hilton properties. Hilton runs Embassy Suites, Doubletree, Hampton Inn and Suites, Waldorf Astoria Hotel & Resorts and Hilton hotels.

Currently it is not clear at this time how many hotels have been affected.


Update (11/24/2015): Hilton Worldwide has sent an update to the California Attorney General’s office regarding the credit card breach. The company confirms they were a victim of a malware attack that affected debit and credit card information of customers from November 18, 2014 through December 5, 2014 or April 21, 2015 through July 27, 2015.


<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 25, 2015</td>
<td>Bed Bath and Beyond New York, New York</td>
<td>BSO INSD Unknown</td>
</tr>
</tbody>
</table>


Customers who used their cards during that time period have been encouraged to notify their banks of the potential for credit card theft.


<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 25, 2015</td>
<td>Horizon Blue Cross Blue Shield Newark, New Jersey</td>
<td>GOV DISC 1,100 members</td>
</tr>
</tbody>
</table>

Horizon Blue Cross Blue Shield of New Jersey notified customers of a data breach when several individuals pretended to be doctors or a health care professionals and obtained member identification numbers, and other personal information. These individuals then submitted claims to Horizon Blue Cross Blue Shield with these member ID numbers. During the investigation it was confirmed that names, dates of birth, gender and member ID numbers were accessed. The company is claiming that no Social Security numbers or financial information or medical information was accessed.


<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 25, 2015</td>
<td>Ginger Blossom Springfield, Massachusetts</td>
<td>BSO PHYS Unknown</td>
</tr>
</tbody>
</table>

The owner of a Chines restaurant called the Ginger Blossom discovered that one of her employees stealing customer credit and debit card information.

The employee was caught on surveillance video with a skimming device. The police recovered a bag that was hidden in a planter outside of the restaurant that contained the scanner and numerous pre-pad gift cards and credit cards.


<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 25, 2015</td>
<td>Blue Cross Blue Shield of North Carolina (BCBSNC)</td>
<td>BSE DISC Unknown</td>
</tr>
</tbody>
</table>

**Information Source:**

- [Media](http://smdp.com/data-breach-involves-big-blue-bus-customers/151000)
- [Vermont Attorney General](http://ago.vermont.gov/assets/files/Consumer/Security_Breach/Bed%20Bath%...)
- [Media](http://wwlp.com/2015/09/25/waiter-charged-with-credit-card-fraud/)

**Records from this breach used in our total:** 0
Blue Cross BlueShield of North Carolina notified customers of a data breach when they discovered two incidences that may have exposed personal information.

The first incident occurred when a printing error resulted in members' billing invoice information printed on the back of other members' invoices. The information exposed here included names, addresses, internal BCBSNC account numbers, group numbers, coverage dates and premium amounts.

The second incident occurred when payment letters included incorrect information and sent to the wrong members. This information included they type of health plan purchased, effective dates, health insurance marketplace identification numbers, payment amounts, telephone numbers and payment identification numbers.

More information: http://www.bcbsnc.com/content/corporate/privacy-breach-20150925.htm
http://healthitsecurity.com/news/theft-printing-error-lead-to-health-dat...

Silverberg Surgical and Medical Group notified patients of a data breach when a "scanning device inadvertently exposed some patient health records to the Internet."

The information exposed included names, addresses, dates of birth, admission records, telephone and fax numbers, email addresses, medical information, medical record numbers, health plan data, beneficiary numbers, Social Security numbers, state license numbers and facial photographic images.

The medical group is providing Kroll identity theft monitoring for one year for free. For those affected visit kroll.idMonitoringService.com or call 1-844-530-4126.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-57984

Systema Software has communicated that a "single individual gained unapproved access into our data storage system."

It has been communicated that this breach exposed over 1.5 million records of public agencies in California, Kansas and Utah.

The records included police injury reports, drug tests, detailed doctor visit notes and Social Security numbers.


The Outback Steakhouse in Northridge, a franchise location for the restaurant group T-Bird Restaurant Group, Inc. notified employees of a data breach when the location was burglarized. The individual (s) managed to steal computer equipment including their point of sale computer terminal and back office computer.

The point of sale computer contained information that included employee time sheet information, files that contained names and Social Security numbers.

The company is offering ID Experts theft protection for one year for free. Those affected call 1-888-773-9953 or go to www.IDExpertsCorp.com/protect.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-57861

The Kardashian Website notified employees of a data breach when employees were burglarized. The individual(s) had access to personal information on the Kardashian Website.

More information: http://oag.ca.gov/ecrime/databreach/reports/sb24-57881
The Kardashian brand recently launched a new website design which appears to have some security holes. One developer discovered a misconfiguration in the site that allowed him to access full names and emails of over 600,000 users who signed up for Kylie Jenner’s website.

This developer stated "I’ll admit I downloaded Kylie’s app just to check it out. I also checked out the website, and just like most developers, I decided to take a look around to see what was powering the site. After I started digging a little bit deeper, I found a JavaScript file named kylie.min.75c4ceae105adbbf8f8270595e77cb0.gz.js. Just for fun, I decided to unminify this file to see what kind of data they were collecting from users and other metrics they may be tracking. I saw several calls to an API, which of course made sense. I popped one of those endpoints into my browser, and got an error just like I expected." 

The developer then logged in with his own username and password and was "directed to a web page that contained the first and last names and email addresses of the 663,270 people who had signed up for the site."

More Information: http://techcrunch.com/2015/09/16/kardashian-website-security-issue-expos...

---

A doctor associated with the LSU Health New Orleans School of Medicine had his laptop stolen which may have exposed 5,000 patients personal information.

The laptop computer was stolen from the doctors vehicle when it was parked in front of his home on July 16th or 17th. The theft was reported but has not yet been recovered.

The information contained on this laptop included names, dates of birth and medical information. It did not contain Social Security numbers, credit card or banking information.

For those with questions, call 1-504-568-8672 or 1-844-578-2656.


---

Gildewell, Dental Ceramics, Inc. and its subsidiaries notified employees of a breach to their system that maintains employee files was discovered.

The unauthorized individual(s) may have taken documents that contained personal information of employees, including names, addresses, Social Security numbers, and financial account information related to direct deposit accounts.

The company is offering one year free of fraud resolution and identity theft protection services through ProtectMyID. Those affected can call 888-227-1416 or www.protectmyid.com/alert and engagement number PC96191.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-57775

---

YapStone payment systems has sent notification to the California Attorney General’s office and individuals who were affected by the breach. Unfortunately no detailed information was available as to they type of breach, the information affected or the number of individuals involved in the breach. As more information is available, this post will be updated.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-57770

UPDATED (9/30/2015): YapStone is being sued by a New Jersey man who filed in a California federal court accusing YapStone of "negligence and breach of contract for failing to protect customer data from a possible breach."

More information: http://www.law360.com/articles/708884/vrbo-payment-processor-hit-with-da...
Sutter Health has notified patients/customers of a data breach when they discovered that a former employee had emailed documents of individuals to a personal email address on April 26, 2013.

The information in these electronic documents included names, dates of birth, insurance identification numbers, dates of services and billing codes. They have stated that no Social Security numbers, drivers' license or ID numbers, credit card or bank information was contained in these documents.

Sutter Health is offering one year free of Experian's ProtectMyID Alert for those who were affected. Those with questions call 1-877-235-0796 Monday through Friday, 6:00 a.m. to 5:00 p.m. Pacific Time.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-57764

Excellus has revealed that in August the company discovered a breach to their system that may have started two years prior by hackers, gaining access to its customers' information.

The information accessed included names, birth dates, Social Security numbers, mailing addresses, telephone numbers, claims and financial payment information, which included some credit card numbers.

"Excellus spokesperson Cane confirmed in a phone call with WIRED that between 10 and 10.5 million customers had their data potentially accessed in the breach. Beyond just Excellus itself, the company says that even some of its insurance partners within the Blue Cross Blue Shield network may be affected, accounting for about 3.5 million of those victims. Everyone affected will receive a letter from Excellus, along with two years of free credit monitoring from the company."

More information: http://www.wired.com/2015/09/hack-brief-health-insurance-firm-excellus-s-

UPDATE (9/21/2015): A class-action lawsuit has now been filed against Excellus as a result of the data breach the company suffered exposing 10.5 million individuals to potential identity theft.


ReverbNation was contacted by law enforcement regarding an unauthorized access to their customer data sometime in January of 2014. The individual who accessed this information was caught and charged.

The customer information this individual may have viewed included email addresses and encrypted passwords, names, addresses, phone numbers, and/or dates of birth.

The company automatically reset users passwords to combat those customers who used a common password. According to the company no credit card information was accessed as they do not store that information on their servers.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-57665

We End Violence LLC notified individuals of a data breach when they discovered unauthorized access into their website server that may have gained access to personal information.

The information accessed included names, student ID numbers, email addresses, Agent of Change usernames, Agent of Change passwords, gender identity, race, ethnicity, age, relationship status, sexual identity and the name of an individuals college or university.

The company is encouraging individuals to change their passwords. For information call 1-877-218-2930 6 a.m to 4 p.m PST, Monday through Friday. Provide the reference number 6751090215 when calling.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-57701
The Heritage Foundation was the victim of a data breach when hackers infiltrated an external server that contained personal information of private donors.

"We experienced a malicious, unauthorized data breach of six-year-old documents on an external server that appear to contain personal information of private donors, who we are notifying," said spokesman Wesley Denton. "We are unable to verify the authenticity of files circulated online."


Information Source: Media
records from this breach used in our total: 0

September 1, 2015 UCLA Health System Los Angeles, California MED PORT 1,200

UCLA Health notified approximately 1,242 patients of another data breach to their health system when an faculty employee was stolen that contained personal information of patients.

According the UCLA Health the lap top did not contain Social Security numbers or financial data, but may have contained other personal and health information of these patients.

UCLA Health has set up a special phone line at 1-888-236-0447 to provide assistance for those who received a letter from the health system notifying them of the breach.

UCLA Health has also issued a statement regarding the breach here: https://www.uclahealth.org/news/ucla-health-notifying-patients-of-stolen...


Information Source: Media
records from this breach used in our total: 1,242

August 31, 2015 State of Minnesota St. Paul, Minnesota GOV DISC 18

Driver's license information of 18 St. Paul residents "were accessed after a password-protected portal was inadvertently opened online."

According to officials a server update inadvertently removed the authentication processes in place when accessing the online portal system for drivers license information. According to these same officials, only two individuals utilized this portal 55 time from August 2, 2015 and August 24, 2015, showing 18 individuals information was accessed during this time frame.

The information included pictures, names, addresses and dates of birth.


Information Source: Media
records from this breach used in our total: 18

August 26, 2015 Dr. Robert E. Soper M.D Eureka, California MED PORT Unknown

Dr. Robert Soper's office notified patients of a data breach when the doctors laptop was stolen out of his car when visiting San Francisco.

The computer contained patient names, dates of birth, some phone numbers, and clinical notes and emails. According to the doctor no addresses, Social Security numbers or insurance information was stored on this laptop. Additionally, "the clinical notes were protected by two passwords, and were maintained in a format unique to the software used to prepare them. The software program itself was not on the computer, making the data almost impossible to decipher."

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-57565
Volkswagen of Oakland notified customers of a data breach when the dealership was broken into and boxes of files were stolen.
The company stated that "We believe that some of the stolen boxes held sold vehicles jackets. Each sold vehicle jacket typically contains copies of the forms signed by the vehicle purchaser including the name, address, phone number, driver’s license information, bank account information, car insurance information and information on the vehicle purchased. In some cases where financing is provided in connection with the purchase of a vehicle, the deal jacket will also contain a copy of the consumer’s credit application, credit report, pay stubs, job information and references."

More Information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-57502](http://oag.ca.gov/ecrime/databreach/reports/sb24-57502)

Buyers Protection Group (BPG) notified customers of a data breach to their personal information.
"On July 19, 2015, a company laptop was stolen from an employee’s car during a large-scale break in of at least 20 vehicles in the Greater Atlanta Area."

The personal information contained on these laptop(s) included names, addresses, dates of birth and Social Security Numbers.

For further questions about this incident individuals can send an email to [privacy@bpowi.com](mailto:privacy@bpowi.com).


Web.com notified customers of a data breach to their systems, when hackers were able to infiltrate their system gaining personal information of customers.

The information included credit card numbers, names, addresses, card validation numbers and the security codes associated with the credit cards.


The University of Virginia has notified individuals of a hacking originating from China and accessed the IT systems of the university. The university has stated that no Social Security numbers or banking information was compromised.

The university has asked all users to change their "Eservices" login passwords. Reportedly the hackers were targeting email account belonging to "two employees whose work is connected to China."


Lee’s Deli, which has a location at 75 Battery Street in San Francisco and 4200 Bohannon Drive in Menlo Park California, have notified individuals of a data breach of their information when the company found malware installed on their credit
card processing system.

The information captured through this malware included payment card account numbers, card expiration dates, and the CVV code on the back of the card. Any transaction made from January 4, 2015 through May 20, 2015 at the Battery Street location and between November 3, 2014 through February 13, 2015 at the Bohannon Drive location, those cards are at risk.

For those affected contact the company at 415-986-1892 between the hours of 9:00 am and 5:00 pm, Monday through Friday or via email at info@leesdeli.com.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-57419

Information
Source: California Attorney General
August 12, 2015 ICANN.org
Los Angeles, CA 90094-2536,

ICANN.org notified individuals of a data breach when they discovered unauthorized access to an external service provider. The non-profit believes that usernames/email addresses and encrypted passwords were compromised.

User profiles contain a users preference for the website, public bio, individual interests, subscription to newsletters and other information.

They are requiring that all members change their password to the site. The password change can be accessed via this link https://www.icann.org/users/password/new

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-57383

Information
Source: California Attorney General
August 12, 2015 Nationstar Mortgage LLC
Dallas, Texas

Nationwide Mortgage notified customers of a data breach when copies of their W2’s were inadvertently emailed to an employee at Greenlight Mortgage. The information compromised included names, addresses, Social Security numbers and other information that is common with a W2 form.

The company is providing one year free of Experian’s ProtectMyID Elite. Those who are affected can call 877-441-6943 or www.protectmyid.com/enroll.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-57381

Information
Source: California Attorney General
August 7, 2015 Sterling BackCheck
New York, New York

SterlingBackcheck notified customers of a data breach when a laptop was stolen from an employee's vehicle. The laptop contained customer information including names, Social Security numbers, and dates of birth.

The company is providing AllClear ID for 24 months for free. For those who are affected can call 1-855-227-9823 Monday through Sunday 8:00 am - 8:00 pm Central Time.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-57330

Information
Source: California Attorney General
August 7, 2015 Ubiquiti Networks Inc.
San Jose, California

Ubiquiti Networks Inc. announced that cyber thieves stole $46.7 million using a scam " in which crooks spoof communications from executives at the victim firm in a bid to initiate unauthorized international wire transfers."

Ubiquiti disclosed the attack when they filed a report with the U.S. Securities and Exchange Commission. " The company said it discovered the fraud on June 5, 2015, and that the incident involved employee impersonation and fraudulent requests from an outside entity targeting the company's finance department."

More Information: http://krebsonsecurity.com/2015/08/tech-firm-ubiquiti-suffers-46m-cyberh...
Sabre Corporation is investigating a possible recent data breach that was brought to light by the announcement of the American Airlines breach. American Airlines uses the reservation software developed by the Sabre Corporation.

“Sabre said in a statement Friday, "We recently learned of a cybersecurity incident, and we are conducting an investigation into it now. At this time, we are not aware that this incident has compromised sensitive protected information, such as credit card data or personally identifiable information, but our investigation is ongoing.”"


---

WP Technology (dba Wattpad) informed customers of a cyber attack to their system that may have compromised customer information.

The information compromised included email addresses, Wattpad passwords, Tumblr usernames and passwords, last login IP, and other user profile information provided.

The company is recommending that their customers change their Wattpad password and your Tumblr password. For questions contact security@wattpad.com

More Information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-57318](http://oag.ca.gov/ecrime/databreach/reports/sb24-57318)

---

Mama Mio informed customers of a cyber-attack to their system where their personal information may have been compromised. According to the company, the attack happened on July 28, 2015.

The information compromised included first names and surnames, emails, billing addresses and telephone numbers, card numbers, expiration dates, and the 3-digit security code on the back of the card.

For those affected call 1-888-962-6264 or send an email at privacy@mioskincare.com.

More Information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-57280](http://oag.ca.gov/ecrime/databreach/reports/sb24-57280)

---

The office of Olartino Dyoco, M.D. notified patients of a data breach when his offices were burglarized and several computers were stolen that contained patient information used for billing. The information compromised included names, addresses, birth dates, telephone numbers, insurance numbers, treatment codes, and billing information.

The incident has been reported to the authorities. For those who were affected call 1-888-233-2305.

More Information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-57245](http://oag.ca.gov/ecrime/databreach/reports/sb24-57245)

---

The VA Hot Springs hospital notified patients of a data breach when files containing their Social Security numbers along with additional personal information were thrown in a trash bin without being shredded.

The incident took place in May and the 1,100 patients that were affected were not notified until July 29, 2015. Reportedly, an employee discarded a box of patient files in a dumpster. The box of files was found two days later by another employee who removed them from the trash.


---
East Bay Perinatal Medical Associates (EBPMA) has notified patients of a data breach when they were contacted by the Berkeley Police regarding an employee who had a patient list on their personal laptop. The list according to the company was created as a part of the employee’s duties to catalogue their 2012 records. The information was deleted from the employee’s hard drive by EBPMA.

The information contained in the document included first and last names, and dates of birth. The company is providing those who were affected Kroll ID monitoring services for free for one year. They can be reached at 1-855-205-6940.

More Information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-57193](http://oag.ca.gov/ecrime/databreach/reports/sb24-57193)

United Airlines may be the latest victim of Chinese hackers. It is being reported that the hackers are potentially the same group that infiltrated OPM and Anthem.

"United, the world’s second-largest airline, detected an incursion into its computer systems in May or early June, said people familiar with the probe. According to three of these people, investigators working with the carrier have linked the attack to a group of China-backed hackers they say are behind several other large heists -- including the theft of security-clearance records from the U.S. Office of Personnel Management and medical data from health insurer Anthem Inc."

The information compromised included flight information, passenger itinerary, passenger information, origins and destinations. The airline has not announced whether or not any financial data was compromised in this hack.


The Orange County Employees Association (OCEA) notified members of a data breach when they were a recent victim of a cyber attack. The attack affected OCEA members, certain non-members, OCEA Health & Welfare Trust participants, OCEA staff, customers of Velece Corporation and dependents.

The information included names, addresses, dates of birth, Social Security numbers, driver's license numbers, payroll information, dental, vision, life and disability enrollment information, retirement status, information concerning dependents and usernames and passwords.

OCEA is providing one year free credit monitoring and identity theft recover and restoration services.

More Information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-57170](http://oag.ca.gov/ecrime/databreach/reports/sb24-57170)

Golden State Credit Union notified members of a data breach when a credit union employee viewed member accounts without authorization. The information viewed included names, Social Security numbers, driver’s license numbers and additional financial information.

The credit union is providing Credit Watch through Equifax to those affected for 12 months at no cost. Those affected must apply by April 15, 2016.

More Information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-57170](http://oag.ca.gov/ecrime/databreach/reports/sb24-57170)

The lawfirm of Atkinson, Andelson, Loya, Ruud & Romo notified clients of a data breach, when one of their attorney’s laptops was stolen that contained personal information of their clients.

The personal information on the laptop included names, addresses, telephone numbers, Social Security numbers.
possible financial information, and medical records information.

The firm is providing MyIDCare, ID Experts for free for 12 months for those who were affected. They can be reached by calling 1-877-341-4604. Monday through Friday from 6:00 a.m to 6 p.m Pacific Time.

More Information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-57094](http://oag.ca.gov/ecrime/databreach/reports/sb24-57094)

Information Source: California Attorney General

July 20, 2015  PNI Digital Media

Vancouver, British Columbia

BSO HACK Unknown

PNI Digital Media is investigating their online photo printing service that they either manage or host for a number of large retailers such as Costco, Walmart, Walgreens, CVS, Rite to name a few. The photo printing service has been taken off line while the company and their customers investigate the breach. The concern is that the hackers gained credit card information from customers of the retailers they service.


Information Source: Media

July 19, 2015  Ashley Madison (owned by Canadian Avid Life Media)

Toronto,

BSO HACK 37 million

Ashley Madison, the online cheating website, confirmed a hack of their system, exposing 40 million records.

The data that was stolen included the company’s user databases, financial records along with other confidential information. The company has not stated the exact personal information compromised.

"Reached by KrebsOnSecurity late Sunday evening, ALM Chief Executive Noel Biderman confirmed the hack, and said the company was “working diligently and feverishly” to take down ALM’s intellectual property. Indeed, in the short span of 30 minutes between that brief interview and the publication of this story, several of the Impact Team’s Web links were no longer responding.”

"Besides snippets of account data apparently sampled at random from among some 40 million users across ALM’s trio of properties, the hackers leaked maps of internal company servers, employee network account information, company bank account data and salary information."


UPDATE (8/18/2015): Hackers who stole sensitive customer information originally reported back in July, have now stated that because the company has not taken down their site as requested by the hackers, sensitive customer information has been posted online.

"A data dump, 9.7 gigabytes in size, was posted on Tuesday to the dark web using an Onion address accessible only through the Tor browser. The files appear to include account details and log-ins for some 32 million users of the social networking site, touted as the premier site for married individuals seeking partners for affairs. Seven years worth of credit card and other payment transaction details are also part of the dump, going back to 2007. The data, which amounts to millions of payment transactions, includes names, street address, email address and amount paid, but not credit card numbers; instead it includes four digits for each transaction that may be the last four digits of the credit card or simply a transaction ID unique to each charge.”

Raja Bhatia, AshleyMadison’s founding Chief Technology Officer stated that these recent data dumps are not legitimate. His team has been reviewing 30 to 80 reported data dumps daily and that “most of these dumps are entirely fake and being used by other organizations to capture the attention that’s been built up through this release"


[http://krebsonsecurity.com/2015/08/was-the-ashley-madison-database-leaked/](http://krebsonsecurity.com/2015/08/was-the-ashley-madison-database-leaked/)

Information Source: Krebs On Security

July 18, 2015  CVS Pharmacy, Imperial Beach

Imperial Beach, California

BSR INSD 100

A pharmacy technician at the CVS Pharmacy on Saturn Boulevard in Imperial Beach California has admitted to stealing customer records and providing the information to her property manager who then used the information to gain credit and credit cards.

An further investigation is currently being conducted. The California State Board of Pharmacy has suspended the license
North East Medical Services notified patients of a security breach when an employee's laptop was stolen from the trunk of the employee's car.

The information compromised included names, dates of birth, gender, contact information, payer/insurer and limited personal health information. According to the medical office no Social Security number or credit card information or actual medical record was involved.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-57240

Richard Berger CPA notified customers of a data breach when external hard drives were stolen from his residence. The drives contained personal customer information. The information included names, tax information, Social Security numbers, bank and investment account information, dependents, beneficiaries, employees or contractors (including their names and Social Security numbers).

Authorities were notified and according to Mr. Berger's office, no drives have been recovered. His office is providing Kroll identity theft protection services to those affected for 12 months for free.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-57066

UCLA Health System's has informed as many as 4.5 million patients of a data breach of their network, exposing sensitive personal and medical information.

The information compromised included names, dates of birth, Social Security numbers, Medicare and health plan identification numbers, patient diagnosis and procedures.

It has been reported that UCLA did not take basic steps to encrypt the patient data.

Patients who are affected can call UCLA at (877) 534-5972 or check the website www.myidcare.com/uclaprotection.


Mule Creek State Prison notified individuals of a breach when documents submitted to the prison were scanned into a computer folder where employees outside of the prison may have access to it.

The information contained names, Driver License numbers and Social Security numbers.

For those with questions, call Ed Ayo, Senior Information System Analyst (Supervisor) at 209-274-5978.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-57023

Insurance Services Office (ISO) notified individuals of a breach when documents submitted to the prison were scanned into a computer folder where employees outside of the prison may have access to it.

The information contained names, Driver License numbers and Social Security numbers.

For those with questions, call Ed Ayo, Senior Information System Analyst (Supervisor) at 209-274-5978.
Insurance Services Office, which provides information and analytics to the property and casualty insurance industry has notified customers of a data breach of policyholder information.

The company has been working with the County Prosecutor’s office and the National Insurance Crime Bureau investigating the breach. Authorities informed ISO that an unauthorized individual(s) viewed personal information of policyholders.

The information included contact information, dates of birth, Social Security numbers, insurance policy numbers, and driver's license numbers.

For those with questions, contact a representative at 1-800-888-4476 7:00 a.m to 9:00 p.m Eastern Time or email nisupport@iso.com

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-57032

Information Source:
California Attorney General

July 10, 2015 Mandarin Oriental
New York, New York BSO HACK Unknown

The Mandarin Oriental Hotel Group has informed customers of a breach when malware was found on their credit card transaction systems, at the following locations:

Boston Geneva
Hong Kong Hyde Park, London
Las Vegas Miami
New York San Francisco
Washington DC The Landmark Mandarin Oriental, Hong Kong

The information compromised included names and credit card numbers.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-56994

Information Source:
California Attorney General

Austin, Texas BSO HACK Unknown

New Horizons Computer Learning Centers, Inc. notified business owners of a data breach when unauthorized access to employee and vendor information stored on the company network may have been compromised.

The information included names and bank account information.

For those with questions can call their confidential inquiry line at 1-866-979-2512 Monday through Saturday, 8:00 a.m - 8:00 p.m. Central Time.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-57002

Information Source:
California Attorney General

July 9, 2015 Service Systems Associates
Denver, Colorado BSO HACK Unknown

Service Systems Associates, who specifically services zoos, restaurants and various cultural centers across the US, has notified customers of a breach of its credit and debit card processing systems.

"The violation occurred in the point of sale systems located in the gift shops of several of our clients," the company said in a written statement. "This means that if a guest used a credit or debit card in the gift shop at one of our partner facilities between March 23 and June 25, 2015, the information on that card may have been compromised."

SSA has not communicated the specific locations affected, however Krebs on Security sources communicate the following locations are most likely affected.

Birmingham, Ala.
San Francisco, Calif.
Sacramento, Calif.
Palm Desert, Calif.
Honolulu, HI
Fort Wayne, Ind.
Baltimore, Md.

Tucson, Ariz.
Fresno, Calif.
Colorado Springs, Colo.
Miami, Fla.
Boise, Id.
Louisville, Ky.
Battle Creek, Mich.
Evans Hotels
San Diego, California

Evans Hotels has notified customers of a breach of backup card readers used to encrypt payment card data. The hotel chain kept the card readers as backup for IT disaster recovery. These back-up readers were being used in conjunction with their current system for check-in with large groups.

For those with questions they can call 888-738-3786 Monday through Friday between 9:00 a.m and 9:00 p.m

Automotive Recovery Services Inc.
Westchester, Illinois

Automotive Recovery Services (ARS) notified customers of a breach when an unauthorized party gained access to one of their legacy systems compromising customer information.

The information compromised included names, Social Security numbers, street addresses, email addresses, phone numbers, driver's license numbers, the type of vehicles donated, name of the charity that the vehicle was donated to.

The company is providing identity theft protection for 12 months for free with AllClear ID. For those with questions call 1-855-861-4023.

Harvard University
Cambridge, Massachusetts

Harvard University is notifying individuals of a data breach to their system that included 8 colleges and administrations.

Those colleges and administrations include the Faculty of Arts and Sciences, Harvard Divinity School, Radcliffe Institute for Advanced Study, Central Administration, the Graduate School of Design, Harvard Graduate School of Education, Harvard John A. Paulson School of Engineering and Applied Sciences, or Harvard T.H. Chan School of Public Health.

The university has not commented on how many individuals were affected or what information was compromised. The university is requesting that anyone who is associated with any of the entities to change their username and password.

The Bonita Unified School District notified parents and students of a breach when unauthorized access was discovered at San Dimas High School server.

On June 2, 2015 the district discovered the unauthorized access to the high school's student database and noticed that several students grades had been changed. The district believes that the individual(s) that changed the grades also downloaded personal information of students.

The information compromised included names, Social Security numbers, birthdates, medical information, the school's systems usernames and passwords, addresses, email addresses, and phone numbers.

The district is providing 12 months free of ProtectMyID Alert from Experian for those affected. Those with questions can call 1-909-971-8320 and ask for Donna Martin at ext. 5201 Monday through Friday 8:00 am to 4:30 pm Pacific Time.
July 2, 2015  The Trump Hotel Collection  New York, New York  

The Trump Hotel Collection appears to be the latest victim of a credit card breach. Banks noticed a string of fraudulent debit and credit card charges all coming from several Trump Hotels.

"The Trump Organization just acknowledged the issue with a brief statement from Eric Trump, executive vice president of development and acquisitions: "Like virtually every other company these days, we have been alerted to potential suspicious credit card activity and are in the midst of a thorough investigation to determine whether it involves any of our properties."

The Trump Hotels have locations in Chicago, Honolulu, Las Vegas, Los Angeles, Miami, and New York. How many individuals affected is not yet known.


June 29, 2015  State Department  Washington, District Of Columbia  

Two brothers, Muneeb and Sohaib Akhter, have pleaded guilty to various charges including conspiracy to access a protected computer without authorization, wire fraud, and accessing government computers without authorization. Muneeb Akhter pleaded separately to additional charges including accessing a protected computer without authorization, obstructing justice and making false statements.

Muneeb Akhter "stole thousands of customers' credit card details, along with other personal information of consumers, by hacking into a cosmetic company's website in March 2014. Then, the brothers and co-conspirators used to the stolen data to purchase "goods and services, including flights, hotel reservations, and attendance at professional conferences," The DOJ release said. "Muneeb Akhter also provided stolen information to an individual he met on the 'dark net,' who sold the information to other dark-net users and gave Akhter a share of the profits."

Sohaib Akhter was employed in a contract position with the State Department and began obtaining passport and visa information, as well as additional sensitive data from the agency's servers.

Sohaib "devised a scheme to ensure that he could maintain perpetual access to desired State Department systems. Sohaib Akhter, with the help of Muneeb Akhter and co-conspirators, attempted to secretly install an electronic collection device inside a State Department building. Once installed, the device could have enabled Sohaib Akhter and co-conspirators to remotely access and collect data from State Department computer systems. Sohaib Akhter was forced to abandon the plan during its execution when he broke the device while attempting to install it behind a wall at a State Department facility in Washington, D.C.," as communicated by a DOJ spokesperson.

More Information:  http://www.scmagazine.com/brothers-accused-of-state-dept-hack-plead-qui...  

June 26, 2015  Medical Informatics Engineering  Fort Wayne, Indiana  

Medical Informatics Engineering has notified individuals of a data breach when they noticed suspicious activity on one of their servers.

The company has determined that some protected health information was exposed including names, home addresses, email addresses, dates of birth, Social Security numbers, lab results, dictated reports and medical conditions.

More Information:  http://oag.ca.gov/ecrime/databreach/reports/sb24-56609

UPDATE (7/23/2015): Medical Informatics Engineering put out a notification on their website regarding the data breach to their system in June. The company is claiming that only certain clients were affected by their breach and notifications went out.


UPDATE (8/6/2015): Two class action status lawsuits have been filed against Medical Informatics Engineering regarding the data breach that affected 3.9 million people (this article shares the total numbers and PRC has updated the total number affected according to this article).

More Information:  http://www.ibj.com/articles/54329-patients-suing-indiana-medical-company...  

June 25, 2015  Bank of Manhatten Mortgage Lending  

Medical Informatics Engineering has notified individuals of a data breach when they noticed suspicious activity on one of their servers.

The company has determined that some protected health information was exposed including names, home addresses, email addresses, dates of birth, Social Security numbers, lab results, dictated reports and medical conditions.

More Information:  http://oag.ca.gov/ecrime/databreach/reports/sb24-56609

UPDATE (7/23/2015): Medical Informatics Engineering put out a notification on their website regarding the data breach to their system in June. The company is claiming that only certain clients were affected by their breach and notifications went out.


UPDATE (8/6/2015): Two class action status lawsuits have been filed against Medical Informatics Engineering regarding the data breach that affected 3.9 million people (this article shares the total numbers and PRC has updated the total number affected according to this article).

More Information:  http://www.ibj.com/articles/54329-patients-suing-indiana-medical-company...
The Bank of Manhattan Mortgage Lending notified customers of a data breach when an employee handled mortgage information of customers that did not meet the company policies, which may have resulted in disclosure of customers loan file information.

The information compromised included names, addresses, loan numbers, phone numbers, Social Security numbers, birth dates, credit information, tax information, and other financial information.

The company is offering free identity theft protection services through Kroll. For those who were affected call 1-866-775-4209.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-56587

Trustmark Insurance Company contacted customers regarding a data breach. The company discovered that "our automated billing e-mail system generated and sent encrypted e-mails to certain insurance carrier clients. While each encrypted email should have contained a single file with information related to each carrier's insureds, on May 14, 2015, we discovered that a software error resulted in each carrier receiving file attachments for all of the carriers instead of just the one file related to their own insureds."

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-56493

Summit Financial Group contacted customers regarding a data breach of their information. An employee of Summit Financial Group inadvertently copied data of other clients onto CD's that should have contained only the individuals information. Those CD's were mailed to clients and soon thereafter Summit clients contacted the company alerting them to the fact that other individuals personal information was on their CD.

The information contained names, addresses, dates of birth, Social Security numbers, and income. The company has claimed that they have contacted all the individuals who received a CD and they have either been gathered by the company or destroyed.


Dungarees notified customers of a breach to their system when they discovered an illegal hack that may have compromised customer credit card or debit card information. Based on the investigation the company believes that information provided with orders placed on their website between March 26, 2015 and June 5, 2015 was compromised.

The information compromised included names, billing information, address, email addresses, credit or debit card number, the card expiration number and the CVV codes on the back of the card.

The company is providing those affected with identity theft protection through ID Experts. Those affected can call -866-833-7917 to speak to a representative.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-56488

UC Irvine Medical Center has notified patients of a data breach when an employee reviewed patient records without authorization.

The information this individual may have gained access to included names, dates of birth, gender, medical record numbers, height, weight, Medical Center account number, allergy information, home addresses, medical documentation, diagnoses, test orders/results, medications, employment status, and names of your health plan and employer.
The medical center is providing those who were affected FraudStop free for one year. For questions call 1-888-653-6036.

More Information: [Link to California Attorney General's website](http://oag.ca.gov/ecrime/databreach/reports/sb24-56428)

Information Source: California Attorney General

June 16, 2015 Houston Astros
Houston, Texas

The FBI is investigating allegations that the St. Louis Cardinals baseball club hacked into the network of the Houston Astros baseball club to gain information regarding the Astros statistics, scouting reports and internal documents regarding players and trades.

The St. Louis Cardinals will not comment on the ongoing investigation.


Information Source: Media

June 15, 2015 LastPass
Fairfax, Virginia

LastPass notified customers of a data breach when they discovered suspicious activity on their network. The company has communicated that "In our investigation, we have found no evidence that encrypted user vault data was taken, nor that LastPass user accounts were accessed. The investigation has shown, however, that LastPass account email addresses, password reminders, server per user salts, and authentication hashes were compromised."

The company is requiring that "all users who are logging in from a new device or IP address first verify their account by email, unless you have multifactor authentication enabled. As an added precaution, we will also be prompting users to update their master password."


Information Source: Media

June 12, 2015 Fred's Inc.
Memphis, Tennessee

Fred's Inc. announced that it is investigating a potential breach when malware was discovered on their point-of-sale system. The discount merchandiser operates 650 stores in multiple states and the company is not clear on how many stores were affected.

"Sources said it was unclear how many Fred's locations were affected, but that the pattern of fraudulent charges traced back to Fred's stores across the company's footprint in the midwest and south, including Alabama, Arkansas, Georgia, Indiana, Kentucky, Louisiana, Mississippi, Tennessee and Texas."


Information Source: Krebs On Security

June 10, 2015 Missing Link Networks Inc.
Calistoga, California

Missing Link Networks Inc notified customers of a breach of their networks exposing customer credit cards. Missing Link Networks provides credit card processing and point of sale services.

The company began reaching out to its customers notifying them that "Beginning on May 27, 2015, we began notifying our winery customers that eCellar Systems, our consumer-direct sales platform, had been breached during the month of April, 2015 by an unknown intruder". This particular platform services numerous wineries in California and elsewhere.

The information compromised included customer names, credit/debit card numbers, billing address, and dates of birth. The company is confirming that Social Security numbers, the CVV and pin numbers were not compromised.

More Information: [News article](http://krebsonsecurity.com/2015/06/breach-at-winery-card-processor-missing-link/)

UPDATE (7/3/2015): The vineyards reportedly affected by this breach include the following: All notificatons can be found on the California Attorney General's data breach site at [Link to California Attorney General's website](http://oag.ca.gov/ecrime/databreach/list)

- Cain Vineyard
- Corison Winery
- Charles Krug Winery (C. Modavi & Family)
- Flora Springs Winery and Vineyard
- Gemstone
- Heitz Wine Cellars
- Jessup Cellars
- Larkmead Vineyards Vinter and Grower
The Office of Personnel Management will be notifying over 4 million current and former federal employees of a data breach thought to be perpetrated by Chinese hackers. Federal officials stated that the hacking exposed employee’s job assignments, performance and training. Officials stated that no “background or clearance investigations” were exposed. They are not stating whether or not the information that was exposed included any Social Security information or financial information.


UPDATE (06/15/2015): Very interesting timeline laid out by Brian Krebs which includes the OPM breach, along with connections to various other breaches that are very similar attacks to OPM. [http://krebsonsecurity.com/2015/06/catching-up-on-the-opm-breach/](http://krebsonsecurity.com/2015/06/catching-up-on-the-opm-breach/)

UPDATE (06/24/2015): The 4.2 million individuals reported to have been affected by the OPM breach, has now increased to approximately 18 million individuals, including individuals that applied for jobs but never ended up being hired.


UPDATE (06/25/2015): The head of OPM has publicly stated that they are investigating the breach of 18 million Social Security numbers as part of the recent hacking at the OPM. Currently we are now including the 18 million in our breach total number as prior the office would not state specifically what information in the records was obtained.

Authorities are also stating that the hack can be defined as two distinct breaches.


UPDATE (7/2/2015): The Office of Personnel Management has had a class-action lawsuit filed against them over the recent data breach by a federal employee’s union. The suit claims that OPM’s negligence led to the breach. Since 2007 when OPM had been notified by the Office of Inspector General that there were deficiencies in the agency’s cybersecurity processes, the agency failed to correct the issues. Here is OPM’s website explaining the breach and what to do. [https://www.opm.gov/cybersecurity](https://www.opm.gov/cybersecurity)


UPDATE (7/9/2015): OPM admits that hackers breached 21.5 million Social Security numbers in the recent data breach.


UPDATE (9/23/2015): OPM has stated that 5.6 million finger prints were part of the cyber attack to the agencies computer systems. This is almost 5 times greater than initially communicated.

their system from October 15, 2014 through April 27, 2015.
The information compromised included names, addresses, payment card account numbers, expiration dates, and CCV/CVV numbers.
The company is providing free access to ProtectMyID Elite through Experian. For questions call 1-866-348-1808 from 8 am through 5 pm Mountain Time, Monday through Friday.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-56231

Information
Source: California
Attorney General
June 3, 2015
Gallant Risk and Insurances Services
Corona, California

Gallant Risk and Insurances Services notified customers of a potential data breach when their offices were broken into and several company laptops were stolen. The laptops were password protected according to the company.

The company did not disclose what type of information may have been stored on the laptops.

The company is providing ID theft protection through Kroll free for one year. For those affected call 1-855-330-6366 from 8:00 a.m to 5:00 p.m Central Time.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-56236

Information
Source: California
Attorney General
May 26, 2015
Internal Revenue Service
Washington, District Of Columbia

A previous story that was broken by Brian Krebs, Krebs On Security, regarding fraudulent tax returns being filed by identity thieves who gained the information using data directly from the IRS website, was confirmed today by the IRS Commissioner Josh Koskinen.

Mr. Koskinen confirmed that the identity thieves pulled data off of the IRS website to file fraudulent tax returns on unsuspecting individuals. The IRS became suspicious due to a large increase of individuals requesting their tax transcripts. The investigation revealed that approximately 200,000 suspicious attempts occurred and 100,000 of those were successful in being authenticated through the IRS website. According to the IRS these attempts started in February and continued through mid-May 2015 and totaled over $50 million dollars in fraudulent refunds.


UPDATE (5/28/2015): The IRS has communicated that the recent breach of 100,000 individuals they believe originated from Russia. The IRS is claiming that this was not a hack, instead that they "went in the front door of the IRS and unlocked it with the key".


UPDATE (8/17/2015): The IRS is now announcing that the data breach that was first reported in May, is three-times larger than originally reported. After a review of the 2015 filing season, the IRS is sending additional letters to individuals warning them that their information may have been compromised and the possibly threat of potential identity theft.


Privacy Rights Clearinghouse has changed our original number of 100,000 individuals to 330,000 individuals affected in this breach on Aug.19, 2015 as is being reported in the media.

UPDATE (2/26/2016): The hacking incident according to the IRS, has increased to 700,000 individual Social Security numbers being affected.

May 22, 2015  **Adult Friend Finder (owned by Penthouse Media)**  
**Miami, Florida**  
BSO  HACK  3.5 million

The adult website Adult Friend Finder was hacked and personal information posted publicly for people to see. The information included customers' email addresses, usernames, passwords, birthdays and zip codes, and sexual preferences. To date they have not yet discovered if customer credit card information was exposed.


---

May 20, 2015  **CareFirst BlueCross BlueShield**  
**Baltimore, Maryland**  
BSF  HACK  1.1 million

The largest insurer in the Baltimore regions, CareFirst BlueCross BlueShield notified customer of a cyberattack to a single database, comprising the information of approximately 1.1 million individuals.

The hackers were able to access names, birth dates, email addresses and insurance identification numbers. CareFirst has stated that they did not gain Social Security numbers, credit card numbers, passwords or medical information in the breach.

The insurer is offering free credit monitoring for two years even though individual no financial or Social Security data was compromised.

The company has posted more answers to the attack at [www.carefirstanswers.com](http://www.carefirstanswers.com).


---

May 15, 2015  **Penn State College of Engineering**  
**University Park, Pennsylvania**  
EDU  HACK  18,000

Penn State's College of Engineering announced that their servers were hacked in two different intrusions. The hackers are believed to be based in China and may have exposed "at least 18,000 people and possibly other sensitive data".

Penn State's President sent a letter out to students and faculty informing them that the college's network had been disconnected to the Internet while they investigate the intrusion. Read more here: [http://news.psu.edu/story/357654/2015/05/15/administration/message-president-semestersmydepartment-...](http://news.psu.edu/story/357654/2015/05/15/administration/message-president-semestersmydepartment-...)

The information compromised has not yet been made public, all College of Engineering faculty, staff and students were affected. Those who also had taken at least one engineering class would be affected as well. The university is requiring those who meet this criteria change their username and password. They have set up a VPN and will be required to use two-factor authentication.


---

May 12, 2015  **Starbucks**  
**Seattle, Washington**  
BSR  HACK  Unknown

Starbucks is responding to unauthorized access by hackers into the Starbucks mobile application, draining dollars out of customers bank accounts, credit cards and paypal accounts.

According to one report, "The Starbucks app lets you pay at checkout with your phone. It can also reload Starbucks gift cards by automatically drawing funds from your bank account, credit card or PayPal.

That’s how criminals are siphoning money away from victims. They break into a victim’s Starbucks account online, add a new gift card, transfer funds over -- and repeat the process every time the original card reloads."

Starbucks had denied the unauthorized activity was a result of a hack or intrusion into its servers. Starbucks has received complaints from customers regarding unauthorized activity and they claim it is "primarily caused when criminals obtain reused names and passwords from other sites and attempt to apply that information to Starbucks." The company will be reimbursing those who had fraudulent charges to their account.

The company suggest customers use stronger, unique usernames and passwords and turn off the "reload" feature in the application.


Salley Beauty has announced the possibility of another data breach to their payment systems. The company said they were investigating “unusual activity of payment cards at some stores” but do not know yet how many customer cards were affected.

Last March the company announced a similar attack to their payment systems, compromising over 25,000 customer payment cards. The company thought they had shut down the malicious attempts.


Harbortouch, a POS vendor, announced a breach of several of the companies restaurant and bar customers. Patrons to the restaurants and/or bars were notified that their payment cards may have been compromised when malicious software was found on the POS systems.


Stater Brothers Markets in West Covina has sent out a notice to the public to help apprehend three suspects who placed a skimmer device on a pin pad in the deli department of the grocery chain located at 375 North Azuza Avenue, West Covina California.

They have also send the notification out for those who may have used their debit or credit card at the West Covina location from March 5, 2015 and March 29, 2015 to review their bank or credit card statements for any unauthorized activity. They are cautioning to change the pin if a debit card was utilized and contact the financial institutions that hold the card so new cards can be issued.

For those with any information on the suspects, they are asking individuals to call 1-855-782-8377 between 8:99 a.m and 5:00 p.m Monday through Friday.

More Information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-55627](http://oag.ca.gov/ecrime/databreach/reports/sb24-55627)

American Sleep Medicine has notified patients of a data breach that has occurred when an external hard drive was stolen from a locked server room at their facility. The hard drive contained patient data from previous sleep studies. The specific information included names, dates of birth, name of referring doctor, name of interpreting doctor, medical history and sleep study results. According to the facility no Social Security numbers or financial information was on the external hard drive.

For questions, call 858-277-7353 or toll free at 844-238-9431.

More Information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-49386](http://oag.ca.gov/ecrime/databreach/reports/sb24-49386)

A Sheriffs Department in Damariscotta Maine was forced to pay hackers $300 in bitcoins to retrieve confidential records being held hostage by hackers who broke into their system. The FBI traced back the bitcoins to a Swiss account but have no other details as to who perpetrated this hacking.
The malware installed on the system happened when someone at the Sheriffs department clicked a link allowing the malware to be installed on their system, which in turn the hackers then held the information hostage until they were paid a ransom to release the malware.


---

**April 13, 2015**

**Homebridge (formerly In-Home Supportive Services)**  
San Francisco, California

Homebridge, formerly the In-Home Supportive Services, notified current and former employees of a data breach on several computers when malware was installed potentially compromising individual information.

The information accessed between January and March 2015 included first and last names, addresses, and Social Security numbers. The company has been informed that the information obtained may have been used to file fraudulent tax returns.

The company is offering one year free of ID Guard. For questions call Human Resources at 415-659-5331.

More Information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-49328](http://oag.ca.gov/ecrime/databreach/reports/sb24-49328)

---

**April 13, 2015**

**Stanislaus Surgical Hospital**  
Modesto, California

Stanislaus Surgical Hospital notified individuals of a data security breach that occurred on April 5, 2015. They do not state exactly how the breach occurred in their notification letter. The information compromised included names, addresses, account numbers, Social Security numbers and other personally identifiable information.

The hospital is providing one year free of Experian’s ProtectMyID Elite to those affected. For questions call 1-877-441-6943.

More Information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-49325](http://oag.ca.gov/ecrime/databreach/reports/sb24-49325)

---

**April 13, 2015**

**Grapevine Police Departments**  
Grapevine, Texas

A group demanding the dashcam video of a shooting be released to the public, hacked the database of the Grapevine Police Department posting a video demanding this release.

The police department is currently investigating the hacking of their system.


---

**April 10, 2015**

**Kellogg & Andelson Global Management**  
Woodland Hills, California

Kellogg & Andelson Global Management notified individuals of a data breach when a server containing client account information was hacked. The information exposed included names, addresses, dates of birth, Social Security numbers, financial account numbers of both the individual account holder and potential family members.

The company is provided identity protection services for 2 years for free through Experian's ProtectMyID Elite. Victims can go to [www.protectmyide.com/protect](http://www.protectmyide.com/protect) and provide the activation code provided by Kellogg & Anderson's notification letter.

More Information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-49323](http://oag.ca.gov/ecrime/databreach/reports/sb24-49323)

---

**April 10, 2015**

**HSBC Finance Corporation**  
Brandon, Florida

The company is provided identity protection services for 2 years for free through Experian's ProtectMyID Elite. Victims can go to [www.protectmyide.com/protect](http://www.protectmyide.com/protect) and provide the activation code provided by Kellogg & Anderson's notification letter.
HSBC notified customers of a data breach when customer mortgage information was inadvertently exposed via the Internet, which included personal information.

The personal information included names, Social Security numbers, account numbers and old account information.

The company is providing Identity Guard for 12 months free for those affected. They can be reached at the Identity Guard Victim Recovery Services phone line at 1-800-901-7107 Monday-Friday 8 a.m-11 p.m, and Saturday 9 a.m-6 p.m Eastern Time.

More Information:  [http://oag.ca.gov/ecrime/databreach/reports/sb24-49318](http://oag.ca.gov/ecrime/databreach/reports/sb24-49318)

Information
Source: California
Attorney General

April 10, 2015
University of California, Riverside Graduate Division offices
Riverside, California

EDU PORT Unknown

The University of California, Riverside’s Graduate Division offices notified individuals of a theft of a laptop computer that included graduate student application information including Social Security numbers, first and last names.

For questions call UCR’s Risk Management Office at 1-866-827-4844

More Information:  [http://oag.ca.gov/ecrime/databreach/reports/sb24-49300](http://oag.ca.gov/ecrime/databreach/reports/sb24-49300)

Information
Source: California
Attorney General

April 8, 2015
AT&T
Dallas, Texas

BSO INSD 280,000 US citizens affected

The FCC has fined AT&T $25 million dollars after an investigation revealed that three separate international call centers are at the center of a data breach of customer information.

Call centers in Mexico, the Phillipines and Columbia all had similar incidences “when employees accessed sensitive customer data without adequate authorization. Those employees took payment from third parties who were apparently interested in customer names and Social Security numbers so they could unlock stolen cell phones for sale on secondary markets.”

As part of the settlement, AT&T has agreed to notify those customers that were affected and offer one year free of credit monitoring services.


Information
Source: Media

April 6, 2015
Tulare County Health and Human Services
Visalia, California

GOV DISC 845

The Tulare County Health and Human Services Agency notified individuals of a breach of their personal information when an HHSA employee emailed approximately 845 patients from the Visalia and Farmersville clinics exposing information to access their medical portal. The agency disabled all patient portal accounts and are asking individuals to change their email addresses, re-register through the portal and change the PIN to login to the patient portal. The agency did not disclose specifically what personal information may have been viewable.

More Information:  [http://oag.ca.gov/ecrime/databreach/reports/sb24-49239](http://oag.ca.gov/ecrime/databreach/reports/sb24-49239)

Information
Source: California
Attorney General

April 3, 2015
Microsoft/Xbox One
Redmond, Washington

BSO HACK 11,266 login-credentials stolen from unnamed company

A 19 year hacker has pleaded guilty to hacking and stealing “11,266 log-in credentials from an unnamed which he then shared amongst the other members.” Austin Alcala was part of a larger hacking network that stole software and data from gaming companies such as Microsoft, Valve, Epic. The group stole internal documents from companies, source code and games that had not yet been released to the public.

The items stolen were stated to be worth approximately $100 million dollars. The hacking took place from 2012 to 2014.

Intuit informed customers of a potential breach to their information after reviewing customer accounts. In this review, Intuit identified certain TurboTax accounts may have been accessed by someone other than the account holder. The company believes that usernames and passwords were stolen by using username/password combinations from other sources, not directly from the Intuit site.

The company automatically changed usernames and passwords to protect from further potential unauthorized access. The company is offering credit monitoring through ProtectMyID through experian for free. For information, email TTaxInvestigations@intuit.com or call 1-866-602-4279.

More Information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-49249](http://oag.ca.gov/ecrime/databreach/reports/sb24-49249)

SRI, Inc. notified customers of a data breach when they discovered an unauthorized access of their website software. The unauthorized access may have been going on since December of 2014 and files containing individual personal information may have been accessed.

The information accessed included names, addresses, Social Security numbers, tax identification numbers, and financial information which included bank account and routing numbers.

For questions call 1-800-800-9588

More Information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-49214](http://oag.ca.gov/ecrime/databreach/reports/sb24-49214)

The California Department of Business Oversight notified both registered investment advisers and broker-dealers that some of their personally identifying information was accidentally disclosed when typical procedure to redact the information either failed or was neglected. The information exposed included Social Security numbers of these individuals. The DBO did not mention the other information exposed on the forms.

For those with questions call 1-866-275-2677.

More Information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-49208](http://oag.ca.gov/ecrime/databreach/reports/sb24-49208)

Premera Blue Cross notified customers of a data breach of their system by a cyberattack that compromised medical, personal and financial data of 11 million customers.

The information compromised included medical information, bank account numbers, Social Security numbers, birth dates, names, addresses and other personal information.

"About six million of the people whose accounts were affected are residents of Washington state, where customers include employees of Amazon.com, Microsoft and Starbucks, according to Premera. The rest are scattered across the United States."

The breach was uncovered on January 29, 2015.

March 16, 2015 Advantage Dental
Redmond, Washington MED HACK 151,626

Advantage Dental notified 151,626 patients of data breach when their database of patient information was hacked between February 23rd and February 26th. The hackers had access to patient names, dates of birth, phone numbers, Social Security numbers and home addresses.

Advantage is offering credit monitoring and call center support through Experian. For further information go to Advantage homepage https://secure.advantagedental.com


Information Source:
Media
records from this breach used in our total: 151,626

March 16, 2015 Apple America Group LLC
Independence, Ohio BSF PORT Unknown

Apple America Group, LLC informed employees of a data breach when a portable USB flash drive owned by a third party vendor containing payroll information was lost.

The information on the portable usb drive included names, addresses, Social Security numbers, and wage and tax information.

More Information: http://oag.ca.gov/system/files/Non-Massachusetts%20consumer%20notificati...

Information Source:
Massachusetts Attorney General
records from this breach used in our total: 0

March 16, 2015 Bistro Burger
San Francisco, California BSO HACK Unknown

Bistro Burger confirmed that malware was installed on the point-of-sale system at their San Francisco location between October 2, 2014 and December 4, 2014. The information compromised included names, payment card account numbers, card expiration dates and security codes.

Information Source:
Media
records from this breach used in our total: 0

March 9, 2015 Inland Empire Health Plan/Children's Eyewear Sight
Rancho Cucamonga, California MED STAT Unknown

Inland Empire Health Plan notified customers of a data breach when a desktop computer and other items were stolen from Children's Eyewear Sight. The police were able to apprehend the individual who perpetrated the theft.

The files on the computer included names, dates of birth, genders, addresses, contact phone numbers, email addresses, IEHP Member ID number, dates of appointments, dates of purchases, and the names of doctors who provided services.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-47991

Information Source:
California Attorney General
records from this breach used in our total: 0

March 4, 2015 Mandarin Oriental Hotel Group
New York, New York BSO HACK Unknown

The hotel chain Mandarin Oriental has announced that their point-of-sale systems were hacked and infected with malware that stole customer credit card data. The hacking, according to the hotel chain, is limited to hotels in the U.S and Europe.

The company has not communicated exactly how many of the hotels locations were compromised only stating that "Mandarin Oriental can confirm that the credit card systems in an isolated number of our hotels in the US and Europe have been accessed without authorization and in violation of both civil and criminal law. The Group has identified and removed the malware and is coordinating with credit card agencies, law enforcement authorities and forensic specialists to ensure that all necessary steps are taken to fully protect our guests and our systems across our portfolio.Unfortunately incidents of this nature are increasingly becoming an industry-wide concern. The Group takes the protection of customer information very seriously and is coordinating with credit card agencies and the necessary forensic specialists to ensure our guests are protected."

According to Krebs on Security, "banking industry sources say the breach almost certainly impacted most if not all Mandarin hotels in the United States, including locations in Boston, Florida, Las Vegas, Miami, New York, and Washington D.C. Sources also say the compromise likely dates back to just before Christmas 2014."

More Information: http://krebsonsecurity.com/2015/03/credit-card-breach-at-mandarin-orien...

Information Source:
records from this breach used in our total: 0
Toys "R" Us contacted customers that their passwords to their reward program account would be reset in order to avoid an unauthorized attempt to their rewards program account.

The company communicated that those notified did not necessarily have their accounts accessed, however, the risk was higher due to the discovery by the company of "recycled login details used by some of its customers."

Between January 28th and January 30th, 2015, the company discovered a number of "illegal login attempts made to its Rewards "R" Us accounts." The current announcement is an additional security measure so that other customer accounts cannot be accessed in a similar way. "Out of an abundance of caution, we are therefore treating your account password as compromised and taking appropriate steps to address the situation," in a letter sent by the company to its customers.


credit card information.
The company is asking customers to change their passwords. The company is offering one year free of credit monitoring
and identity theft services.


Information
Source: Media
February 27, 2015
Uber Technologies Inc.
San Francisco, California
BSO HACK 50,000

Uber notified 50,000 drivers of an unauthorized access to their database which resulted in compromising driver data. The
hacking took place in May of 2014. According to the company only names and driver’s license numbers were compromised.

The company is offering identity protection services for affected drivers.


Information
Source: Media
February 25, 2015
Lime Crime
New York, New York
BSO HACK Unknown

Lime Crime, an online cosmetics company notified customers of an unauthorized access to their website server which
resulted in malware being installed. This malware allowed customer data to be captured, including credit card payment
information.

The information compromised included names, addresses, card account numbers, expiration dates, security codes and
Lime Crime website usernames and passwords. The malware affected customers who purchased items on the website from
October 4, 2014 through February 15, 2015. For those customers that used PayPal to purchase items, their Lime Crime
website usernames and passwords may have also been compromised.


Information
Source: Media
February 24, 2015
The Urban Institute
Washington, District Of Columbia
BSO HACK 600,000 to 700,000
organizations affected

The Urban Institute alerted charitable organization that utilize their National Center for Charitable Statistics (NCCS) to
file their taxes, was compromised when the system was hacked.

"An official with the Urban Institute estimated that between 600,000 and 700,000 organizations were affected by the
breach. At this point, there is apparently no evidence that tax filings themselves were compromised. There were also no
Social Security numbers or credit card information in the system, the official said."

The tax filings by these organizations are said to be compromised in this particular hack. The Urban Institute has stated
that there were no Social Security numbers or credit card information on this system.


Information
Source: Media
February 24, 2015
Cathrine Steinborn, Dentist
Santa Clara, California
MED PORT Unknown

The office of Cathrine Steinborn, DDS was broken into and a server containing patient and other personal information in
it. The information compromised included names, addresses, dates of birth, telephone numbers, Social Security numbers,
dental and/or medical insurance information, health information, treatment information, and billing information.


Information
Source: Media
February 23, 2015
Lone Star Circle of Care
Georgetown, Texas
BSO DISC 8,700

Lone Star Circle of Care notified individuals of a data breach after the discovery of a back-up file containing containing
names, addresses, phone numbers, and birth dates was accidentally posted on their website for view.
Lime Crime has warned customers of a data breach when they discovered malware installed on their website server potentially compromising payment cards and personal data of their customers who used their site.

The compromised data included names, addresses, website usernames, passwords, payment card account numbers, card expiration dates and payment card security codes.

The Office of Jeb Bush inadvertently exposed 12,500 individuals' personal information as part of a larger cached file of 332,999 emails sent to him when he was the Governor of Florida.

The email was sent as part of a measure for transparency, however his team neglected to remove personal information if 12,500 of those individuals exposing names, Social Security numbers, and birthdates.

The office has since redacted the information, which were believed to have been individuals on a family services waiting list from 2003.

The University of Maine notified students of a data breach when a laptop was stolen with student roster information on it including Social Security numbers, phone numbers, email addresses, grade data and course information.

According to the university only 604 Social Security numbers were involved in the total of 941 records exposed.

Liberty Tax Services contacted customers to inform them of a data breach due to a burglary. The thieves took some files and electronic records that included personal information of their customers. The information included names, addresses, dates of birth, identification numbers, Social Security numbers, income documents and names of dependents, their dates of births, and their Social Security numbers. The company is offering those who were affected one year free of credit monitoring. For those affected they can call 1-909-864-8122 to set up an appointment. For further questions contact a member of their team at the following: Linda Sowell, Office Manager at 909-864-8122 or Jeanette Burr, District Manager at 909-533-0448.
Big Fish contacted customers of a data breach when they discovered malware installed on their billing and payment pages of their online stores that affected purchases from December 24, 2014 through January 8, 2015. The information affected included names, addresses, and payment card information, including the card number, expiration date, and CVV2 code.

The company is providing one year free of Experian's ProtectMyID Alert. For those affected with questions they can call 877-534-7032.


---

Anthem, the second largest health insurance company operating under Anthem Blue Cross, Anthem Blue Cross and Blue Shield Amerigroup and Healthlink has suffered a massive data breach.

The company announced that they have been the victim of a “very sophisticated external cyber attack” on their system. The information compromised includes names, birthdays, medical ID’s, Social Security Numbers, street addresses, e-mail addresses, employment and income information.

Over the next several weeks, those who were affected will be receiving some form of identity theft protection.

For those members with questions regarding the breach, the company has set up a toll-free line at 1-877-263-7995 FREE.

More Information: For the statement by Anthem's CEO Joseph R. Swedish and the dedicated website created for customer information, click [here](http://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-se...).


UPDATE (2/10/2015): As further investigations are pursued regarding the Anthem breach, research by Brian Krebs and others show that the hacking began as early as April 2014 and is pointing to Chinese hacker group known as “Deep Panda”.

At the time, Anthem was called Wellpoint, and upon further investigation Krebs “discovered a series of connected domain names that appear to imitate actual Wellpoint sites, including wellpoint.com and myhr.wellpoint.com.”

Because these sites were contracted almost 10 months prior, the question has now been raised as to why it took the company such a long time to uncover the hacking.


---

A fire at the CitiStorage warehouse in Brooklyn, inadvertently put individual’s privacy at risk. This warehouse stored thousands of records for law firms, medical practices, government agencies, financial companies and other businesses.

Amongst the charred paperwork were visible Social Security numbers, medical information, bank checks, lawyers’ letters, court transcripts and more. Much of the paperwork was strewn out for blocks with clearly visible personal information making it very easy to steal someone’s identity.

"New York City sent disaster recovery contractors, equipped with nets, shovels and protective boots, to try to collect the debris. But still, beachcombers sifted freely through the trove of documents, picking their way through remnants of the days when many records were on paper and the city government was one of the few takers for north Brooklyn’s waterfront land."

The various government agencies that stored information at the warehouse included the state court system, the city's Administration for Children’s Services and the Health and Hospitals Corporation.


---

CICS Employment Services notified customers of a data breach when their system was accessed by an unauthorized user(s) gaining access to employment application information on individuals.

The information accessed included names, addresses, dates of birth and Social Security Numbers.

The company is providing 12 months free of AllClearID. Call 1-855-865-4453. For additional questions or concerns a company representative can be reached at 1-888-593-5379.

**More Information:** [http://oag.ca.gov/ecrime/databreach/reports/sb24-48292](http://oag.ca.gov/ecrime/databreach/reports/sb24-48292)

**Information**
**Source:** California Attorney General

January 30, 2015 **Phoenix House Foundation Inc.**
New York, New York

On December 22, 2014, the Phoenix House discovered a data breach when their payroll system when a consultant they hired made unauthorized changes to their electronic payroll systems.

The information accessed included names, addresses, Social Security numbers, salary information, and benefit information. The company has terminated the contracted with the consultant and contacted authorities.

The company is offering a 12 month membership in Experian’s ProtectMyID Alert for free for those affected.

**More Information:** [http://oag.ca.gov/ecrime/databreach/reports/sb24-48355](http://oag.ca.gov/ecrime/databreach/reports/sb24-48355)

**Information**
**Source:** California Attorney General

January 29, 2015 **Kaiser Foundation Health Plan of the Mid- Atlantic States, Inc.**
Mid-Atlantic, Maryland

Kaiser Foundation Health Plan of the Mid-Atlantic States, Inc. notified patients of a data breach when a printing error patients received appointment reminders containing other patients health information. The breach affected 630 individuals.

The information compromised included names, medical record numbers, types of appointments to be scheduled, and providers’ names and departments.


**Information**
**Source:** Government Agency

January 29, 2015 **North Dallas Urogynecology**
Dallas, Texas

North Dallas Urogynecology notified patients of a data breach when a laptop was stolen from their offices that contained personal information of patients.

No specifics were provided as to what kind of personal information the laptop contained.


**Information**
**Source:** Government Agency

January 29, 2015 **David E. Hansen DDS PS**
Tacoma, Washington

David E. Hansen DDS PS notified patients of a data breach when a portable electronic device was stolen.

Specifics on what information was compromised was not provided.


**Information**
**Source:** Government Agency

January 29, 2015 **Riverside County Regional Medical Center**
Moreno Valley, California

Riverside Regional Medical Center notified patients of a databreach when one of their employee laptops used in their Ophthalmology and Dermatology clinics was stolen that contained patient information.

The information on the laptop included names, phone numbers, addresses, dates of birth, Social Security Numbers, and clinical information such as medical record numbers, physicians, diagnosis, treatments received, medical departments
and health insurance information.

The facility has set up 12 months free of Experian's ProtectMyID Alert for those affected. For questions call 1-866-313-7993.

**More Information:** [http://oag.ca.gov/ecrime/databreach/reports/sb24-48266](http://oag.ca.gov/ecrime/databreach/reports/sb24-48266)

**Information Source:**
California Attorney General

**January 23, 2015** Diana S. Guth DBA Home Respiratory Care Los Angeles, California

Diana S. Guth DBA Home Respiratory Care notified individuals of a data breach when information was disclosed through email.

No specific details on how the breach occurred or what specific information was compromised.


**Information Source:**
Government Agency

**January 23, 2015** California Pacific Medical Center San Francisco, California

California Pacific Medical Center through an audit discovered that one its employees accessed medical records of 13 coworkers. A subsequent audit showed that this same employee accessed records of an additional 845 individuals.

The information compromised included patient demographics, last four digits of a Social Security numbers, clinical information about diagnoses, clinical notes, physician order information, laboratory and radiological data, and prescription information.


**Information Source:**
Government Agency

**January 23, 2015** St. Peter's Health Partners Albany, New York

St. Peter's Health Partners notified individuals of a data breach when a portable device containing personal health information was stolen from their offices.


**Information Source:**
Government Agency

**January 23, 2015** Ronald D. Garrett-Roe MD Corpus Christi, Texas

Dr. Ronald D. Garrett-Roe notified patients of a data breach when hackers gained unauthorized access to two hard drives located on the desktop computers of the physicians office. The hard drive had been removed and all the files contained on the hard drive were copied. The hard drive was then formatted to erase all of the information on the computer system. No specific information was provided as to what patient information was compromised.


**Information Source:**
Government Agency

**January 23, 2015** California Pacific Medical Center/Sutter Health San Francisco, California

California Pacific Medical Center notified 844 patients of a data breach to their system when an employee accessed records without authorization.

A total of 844 patients between October 2013 and October 2014, were accessed by this person who has since been terminated. The information obtained included patient demographics, last four digits of Social Security number, clinical information such as diagnosis, clinical notes, and prescription information.

The company states that the employee did not have access to full Social Security numbers, credit card or financial information, driver's license numbers, or California identification numbers.
Those with questions can contact Sutter Health’s Chief Privacy Officer toll-free at 1-855-771-4220 FREE Monday through Friday from 8:00 am to 5 pm Pacific Standard Time.

More Information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-48217](http://oag.ca.gov/ecrime/databreach/reports/sb24-48217)

Information
Source: California Attorney General

January 21, 2015 Sunglo Home Health Services Harlingen, Texas MED PORT Unknown

Sunglo Home Health Services notified customers/patients of a data breach when their facility was broken into and stole one of their company lap tops. The laptop contained patient information including Social Security Numbers and personal health information.

Currently the company does not know the number of affected patients.


Information
Source: Media

January 21, 2015 Mount Pleasant School District Mount Pleasant, Texas EDU HACK 915

Mount Pleasant School District has informed approximately 915 present and former staff members that their personal information may have been compromised between January 18th 2015 and January 21st 2015.

A spokesperson for Mount Pleasant School District stated “Forest Hills District had a denial of service and discovered they had been hacked,” she said. “The district’s technology director found a Tweet that mentioned us. She looked us up on the Web and called us to let us know on Tuesday.”

When the technology director for Mount Pleasant clicked on the link, it directed him to a file that included names, addresses and Social Security numbers” of MPISD staff.


Information
Source: Media

January 16, 2015 Rainier Surgical, Incorporated Dallas, Texas MED PHYS 4920

Rainier Surgical Incorporated reported a file drawer that contained personal information on patients was stolen from a warehouse.

The information compromised included names, addresses, dates of birth, health insurance information, explanations of benefits, credit card numbers and Social Security numbers.

The company offered one year of free credit monitoring services.


Information
Source: Government Agency

January 16, 2015 Grill Parts.com Santa Rosa, California BSR HACK Unknown

Grillparts.com notified customers of a data breach to their website from January 2014 through October 2014.

The information compromised included first and last names, addresses, personal card account numbers, expiration dates, and credit/debit card security codes. It is currently unknown or has not been reported as to the number of people who were affected.

The company is providing the services of Kroll identity theft protection for one year at no cost to those who might have been affected by the breach.

Visit kroll.idMonitoringService.com and follow the online instructions to take advantage of the Identity Theft Protection Services. You will need to enter the membership ID provided by the company sent in a letter to those whose information has been or could have been compromised.

More Information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-48107](http://oag.ca.gov/ecrime/databreach/reports/sb24-48107)
January 15, 2015 National Pain Institute  
Winter Park, Florida  
MED PHYS 500

"From July 13, 2013, to August 13, 2013, the covered entity (CE), National Pain Institute, distributed outdated computers to its employees for their personal use without first deleting all electronic protected health information (ePHI) from the computers. The computers contained the PHI of approximately 500 individuals, including names, addresses, dates of birth, diagnoses, and other treatment information. The CE provided breach notification to HHS, affected individuals, and the media. In response to the incident, The CE tracked the computers, repossessed those computers that it was able to locate, and obtained written acknowledgement from the former employees that the PHI from the computers was not used or disclosed to others. In addition, the CE improved safeguards by encrypting all computers, upgrading the malware and software of desktop computers, improving network and email security, improving identity management, and automating and standardizing security for devices containing ePHI. The CE also updated its HIPAA policies and procedures, including a policy for responding to security incidents. OCR obtained assurances that the CE implemented the corrective actions listed."

More information: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=9BF4AF...

January 15, 2015 Oppenheimer Funds  
Denver, Colorado  
BSF DISC Unknown

Oppenheimer Funds was notified by a brokerage firm that works with Oppenheimer Funds that customer information that was mistakenly made available to a representative of the associated brokerage firm.

The information included names, addresses, Oppenheimer Fund account numbers and Social Security numbers.

The company is offering credit protection through Equifax Consumer Services, LLC. For those affected they can reach out to Equifax Consumer Services at 1-888-766-0008 FREE for information regarding the credit monitoring. Oppenheimer Funds provided a monitoring code to all those affected. The company can be reached at 1-800-225-5677 FREE Monday through Friday from 8:00am to 8:00pm Easter time or visit the website at www.oppenheimerfunds.com.

More Information: http://oag.ca.gov/ecrimw/databreach/reports/sb24-48071

January 12, 2015 Tennessee Rural Health Improvement Association  
Cucamonga, California  
MED PHYS 1030

Children’s Eyewear Sight notified individuals of a data breach when a desktop computer was stolen containing individuals personal information. What specific personal information was contained in the computers was not communicated.

More information: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=9BF4AF...

January 7, 2015 VA Corporate Data Center Operations/Austin Information Technology Center  
Austin, Texas  
MED HACK 7029

According to the Health and Human services website the VA Corporate Data Center suffered a data breach when they discovered their network server was hacked compromising personal information. The types of information compromised was not communicated.

More information: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=9BF4AF...

January 7, 2015 Saint Louis County Department of Health  
St. Louis, Missouri  
MED HACK 4000

"On November 18, 2014, an employee of the covered entity (CE), Saint Louis County Department of Health, resigned her position and then impermissibly emailed her personal email account a spreadsheet that was used to reconcile bills for medical services provided to the CE’s patients. The types of protected health information (PHI) contained in the spreadsheet included the names, social security numbers, and dates of service of approximately 4,000 patients, along with the names of the medical providers. The CE provided breach notification to HHS, affected individuals, and the media, and also filed a police report. The CE terminated the former employee’s access to its patient database and retrained employees on its HIPAA policies and procedures regarding HIPAA. OCR obtained assurances that the CE
implemented the corrective actions listed."

More information: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=9BF4AF...

Information
Source: Government
Agency

January 7, 2015 Lokai
New York, New York

Lokai informed customers of a data breach to their system from July 18, 2014 to October 28, 2014 by hackers who gained access to their server that hosts their website. The hackers installed a program that was designed to record information entered by customers.

The information affected included names, addresses, payment card information, expiration dates, verification codes, and user name and passwords.

For those affected who have questions they can call 1-800-981-7571 Monday through Friday between the hours of 9:00 a.m and 9:00 p.m. Eastern Time.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-47853

Information
Source: California Attorney General

January 6, 2015 NVIDIA Corporation
Santa Clara, California

NVIDIA Corporation suffered a data breach when hackers infiltrated their network and stole employee usernames and passwords.

The company is requesting that those affected change their password and be cautious of “phishing” emails that look like they are coming from a colleague or friend requesting sensitive information.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-47824

Information
Source: California Attorney General

January 5, 2015 mdlNR LLC
Jacksonville, Florida

As reported through Health and Human Services, mdlNR LLC a healthcare provider in Jacksonville Florida had unauthorized access in emails.

Additional specific information as to what personal information was compromised was not available.

More information: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=9BF4AF...

Information
Source: Government Agency

January 5, 2015 Morgan Stanley
New York, New York

An employee of Morgan Stanley stole customer information on 350,000 clients including account numbers. Additional information on what other information was captured has not yet been released. Files for as many as 900 clients ended up on a website.

The employee has since been fired and the bank is notifying all of the individuals affected. The FBI is currently investigating the incident.


Information
Source: Media

January 2, 2015 Chic-Fil-A
Atlanta, Georgia

Chic-Fil-A has announced they are investigating a possible data breach to their payment card system. They have not released any details as to the reality of the breach, however, many experts are predicting it could be extensive.

The restaurant chain operates over 1,850 stores nationwide. Suspicious activity on their payment systems and a report provided to the on December 19, 2014 as to suspicious activity, prompted the company to launch an investigation.
Additional information will be posted as soon as information is available.


**Information Source:** Media

**January 1, 2015**  
**Fast Forward Academy**  
**Altamonte Springs, Florida**  
**EDU**  
**HACK**  
**Unknown**

The Fast Forward Academy LLC has notified customers of a data breach to their systems that store customer and partner information. The information compromised included names, addresses, Social Security numbers, and email addresses.

The company is providing access to Triple Bureau Credit Monitoring services at no charge for 12 months. Those affected can enroll at [https://www.myidmanager.com/promo_code.html](https://www.myidmanager.com/promo_code.html) and provide the code provided by the company or call 1-866-717-9429 FREE to set up services or their help line at 1-800-405-6108 FREE Monday through Friday between the hours of 8 a.m. to 5 p.m. EST.

**More Information:** [http://oag.ca.gov/ecrime/databreach/reports/sb24-47924](http://oag.ca.gov/ecrime/databreach/reports/sb24-47924)

**Information Source:** Media

**January 1, 2015**  
**United Airlines**  
**Chicago, Illinois**  
**BSO**  
**HACK**  
**Unknown**

United Airlines notified customers of an unauthorized access to their MileagePlus account with usernames and passwords obtained from a third-party source.

The unauthorized access began on December 9, 2014, where the hacker(s) attempted to infiltrate the accounts of United Mileage Plus accounts. The hackers obtained MileagePlus numbers and possible account details. The company has stated that if the profile included a credit card number, only the last 4 digits of the card were visible.

United temporarily suspended Mileage Plus accounts. For those with suspended accounts they can call 1-800-421-4655 FREE to change usernames, passwords, PIN's, and security questions.

**More Information:** [http://oag.ca.gov/ecrime/databreach/reports/sb24-47959](http://oag.ca.gov/ecrime/databreach/reports/sb24-47959)

**Information Source:** Media

**December 31, 2014**  
**La Jolla Group**  
**Irvine, California**  
**BSO**  
**HACK**  
**Unknown**

The La Jolla Group has informed customers of a data breach in connection with ecommerce sites that the company manages for various apparel brand licensees.

On December 3, 2014 they noticed unauthorized access to check-out pages on the websites of certain clients. The company then launched an investigation and confirmed that certain information had been breached. The information included names, addresses, phone numbers, email addresses, credit card numbers, CVV2 data and credit card expiration dates of customers who checked out at their clients websites. According to the company no Social Security numbers were compromised.

The company has set up AllClearID for those who were affected for one year for free. Those with questions can contact their hotline at 1-877-403-0281 FREE between 9:00 a.m and 9 p.m. Eastern Standard Time, Monday through Saturday.

**More Information:** [http://oag.ca.gov/ecrime/databreach/reports/sb24-47915](http://oag.ca.gov/ecrime/databreach/reports/sb24-47915)

**Information Source:** Media

**December 29, 2014**  
**LeapLab**  
**Chandler, Arizona**  
**BSO**  
**INSD**  
**Unknown**

LeapLab is being sued by the Federal Trade Commission for purchasing "payday loan applications of financially strapped consumers, and then sold that information to marketers whom it knew had no legitimate need for it".

In another FTC case, Ideal Financial Solutions, used this information sold to them to withdraw millions of dollars from individual accounts without permission.


**Information Source:** Media
PlayStation and Xbox networks over the holiday season. A group calling itself "LizardSquad" hacked both gaming networks on Christmas Day.

According to the group and KrebsOnSecurity, "various statements posted by self-described LizardSquad members on their open online chat forum - chat.lizardpatrol.com - suggest that these misguided individuals launched the attack for no other reason than because they thought it would be amusing to annoy and disappoint people who received new Xbox and PlayStation consoles as holiday gifts".


Microsoft Xbox Live networks were hacked by a group called "LizardSquad", preventing users from playing games over the holiday.

The assault was a DDoS attack (distributed denial-of-service) which "harness the Internet connectivity of many hacked or misconfigured systems so that those systems are forced to simultaneously flood target network with junk Internet traffic. The goal, of course, is to prevent legitimate visitors from being able to load the site or use the service under attack."


On November 14, 2014 an employee laptop and hard drive were stolen when their car was broken into. According to the company the laptop was password protected.

The information stored on the laptop included images taken during the course of treatment, names, banking, full routing numbers, credit card numbers, some financing applications that included Social Security Numbers, dates of birth, mailing address, email address, income, rent payments and employer names.

The company is providing 12 months free of AllClearID, call 1-877-437-3998

More Information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-47861](http://oag.ca.gov/ecrime/databreach/reports/sb24-47861)

Boersma Brothers, dba DutchWear suffered a data breach when their website was breached exposing the payment information for customers from November 7 and December 6, 2014.

The information compromised included names, addresses, phone numbers, credit card numbers, expiration dates, and credit card security codes.

The company has set up a toll-free help line for customers at 1-844-835-8656 from 8 a.m. and 4 p.m PST, Monday through Friday.

More Information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-47840](http://oag.ca.gov/ecrime/databreach/reports/sb24-47840)

Corday Productions, Inc. has payroll administered by Sony Pictures Entertainment. As part of the Sony breach, Corday Production Inc.'s employees, independent contractors or employees of contractors providing services to Corday may have had personal information compromised.

The incident is still under investigation as part of the larger Sony investigation. Corday is offering AllClear ID to those who may have been affected. They can be contacted at 1-855-434-8077 or [https://www.allclearid.com](https://www.allclearid.com/)
Information
Source: California Attorney General
December 23, 2014
Rob Kirby, CPA
Santa Rosa, California
BSO PORT Unknown

Rob Kirby CPA notified customers of a data breach when the car he was driving was broken into and his briefcase, a password protected laptop and flash drive containing confidential client information was stolen.

The information stolen included tax returns for current and previous years, copies of supporting documents associated with the returns, including names, addresses, birth dates, and Social Security numbers for clients, spouses, and dependents.

Information
Source: California Attorney General
December 23, 2014
Public Architecture/theonepercent.org
San Francisco, California
BSO HACK Unknown

On December 8th, 2014 Public Architecture, theonepercent.org, was breached when a hacker broker through the sites security protocols and firewalls to put up a brag page touting his success in hacking.

The hacker deleted files that affected the operation of the site, and possibly stole usernames, passwords, and contact information.

Information
Source: California Attorney General
December 18, 2014
KeyPoint Government Solutions
Fairfax, Virginia
BSO HACK 48,439

KeyPoint Government Solutions notified over 48,000 individuals of a data breach when their computer network was hacked. KeyPoint Solutions was hired by the Office of Personnel Management to take over the background checking process for the agency, when the agency did not renew the contract of USIS who suffered a breach earlier in the year.

Information
Source: Media
December 12, 2014
Acosta Sales and Marketing
Jacksonville, Florida
BSO PORT Unknown

Acosta, Inc. and its subsidiaries (Mosaic Sales Solutions US Operating Co. LLC) informed customers of a data breach when an employee of their Human Resources department had a laptop containing personal information stolen from their car on November 11, 2014.

For those affected, the company has set up a toll free number to assist with questions at 1-877-237-4971 Monday through Friday 9:00 a.m to 7:00 p.m Eastern Standard Time. The reference number to the incident is #5316120814.

Information
Source: California Attorney General
December 12, 2014
University of California Berkeley
Berkeley, California
EDU HACK Unknown

The University of California Berkeley has notified individuals of a data breach in their Real Estate Division that resulted in unauthorized access to servers used to support a number of Real Estate programs and work stations.
These workstations contained files that included some personal information. The investigation of the hacking showed that these servers were breached in mid-to late September.

The personal information included names, Social Security Numbers, credit card numbers and driver’s license numbers.

The university is offering identity theft protection and fraud resolution through ID Experts for free for one year. For those affected call 1-877-846-63401-877-846-6340 Monday through Friday from 6 a.m. to 6 p.m. Pacific Time or go to www.mvidcare.com/ucbinfo.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-47717

Information
Source: California Attorney General
December 11, 2014 Emcor Services Mesa Energy Systems El Cajon, California BSO PORT Unknown

Emcor Services Mesa Energy Systems notified individual of a data breach when a company laptop was stolen that contained customers personal information.

The information contained on the laptop included names, Social Security numbers, dates of birth, dates of hire, addresses, salaries, gender and ethnicity. The theft occurred on or around November 25, 2014.

The company is offering the services of Kroll for one year at no cost. For those who were affected they can call 1-866-775-4209 from 8:00 a.m. to 5 p.m. Central Time, Monday through Friday.

For those with questions for the company can call Mike Cook at 1-949-460-4605.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-47705

Information
Source: California Attorney General
December 11, 2014 ABM Parking Services St. Louis, Missouri BSO HACK Unknown

ABM Parking Services notified customers of a data breach when the point of sale software system implemented by Datapark USA Inc, a third party vendor for several Chicago, Illinois parking facilities was hacked. The information was compromised from October 6, 2014 through October 31, 2014.

The hackers were able to compromise certain customer credit and debit card information, including payment card numbers.

A toll-free information line has been made available for those affected. Customers can call 1-877-238-3790. The company is offering one year free of Experian’s ProtectMyID Elite for those affected.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-47710

Information
Source: California Attorney General
December 9, 2014 Charge Anywhere LLC South Plainfield, New Jersey BSF HACK Unknown

The electronic payment provider Charge Anywhere has notified individuals of a data breach of their networks when an unauthorized person(s) installed “sophisticated malware” that allowed the hackers to "capture segments of outbound network traffic" as the company has explained in a statement released December 9, 2014.

The information captured included customer names, card numbers, expiration dates and verification codes of debit/credit cards.

The company stated that transactions completed from August 17, 2014 through September 24, 2014 were compromised. However, information as far back as November 5, 2009 could have been captured as well.

"The incident is the latest reminder of what happens to businesses that handle credit card data and other sensitive information and yet fail to fully encrypt the data as it traverses their network. The company has provided a searchable list of merchants who may have been affected by the breach."

More Information: http://krebsonsecurity.com/2014/12/unencrypted-data-lets-thieves-charge...
December 6, 2014  

**WellCare Health Plans**  
*Monroe County, New York*

MED DISC 47

500 Monroe County residents were notified by WellCare Health of disclosure of some of their personal information when their Medicare records were "mishandled" by a sub-contractor for the insurer.

The insurer's vendor had an error in their computer coding causing denial letters to be sent to the wrong members. The information on the letters included names, addresses, member ID numbers and general descriptions of the procedure. According to the insurer, no Social Security numbers or financial information was disclosed in the letter.

Subscribers with questions can call WellCare at (888) 240-4946.


December 5, 2014  

**Bebe Retail**  
*Brisbane, California*

BSR HACK Unknown

Bebe Stores have notified customers of a data breach to their point of sale systems that took place last month for several weeks. The goal of the hackers was to obtain payment card information. The hacking took place between November 8, 2014 and November 26, 2014.

The retailer is not stating how many cards were affected and the breach is currently being investigated by forensic IT specialists.

Bebe has more than 200 stores that could have been affected.


December 2, 2014  

**Dallas Fire-Rescue**  
*Dallas, Texas*

MED PORT Unknown

Dallas Fire-Rescue had several laptops containing patient information come up missing from several of their ambulances.

"According to the city, those computers disappeared between January 1, 2011, and August 29, 2014. The city's release did not say how many laptops were unaccounted for — or how they disappeared. Messages have been left for Sana Syed, the city's spokesperson."

No specific information was provided as to what information was in the files. For those patients who have questions can call the Dallas Fire-Rescue EMS staff at (844) 532-5527.


December 1, 2014  

**American Residuals and Talent Inc.**  
*Los Angeles, California*

BSO HACK Unknown

American Residuals and Talent Inc, dba ART Payroll, a specialized payroll company for the entertainment, advertising and events production industry, notified customers of a breach to their system when hackers infiltrated their servers and obtained personal information.

The information included names, addresses, dates of birth, Social Security number, email addresses, phone numbers, ART account numbers, bank account information, ART account user ID and password.

The company is providing ProtectMyID for 1 year at no cost to those who were affected. For questions call 1-877-297-7780.

More Information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-47623](http://oag.ca.gov/ecrime/databreach/reports/sb24-47623)

December 1, 2014  

**Highlands-Cashier Hospital**  
*Highlands, North Carolina*

MED DISC 25,000

Highlands-Cashier hospital in North Carolina informed patients of a data breach to their servers that contained patient data. The disclosure of the data was due to an error by one of their third party vendors, TruBridge a subsidiary of...
Computer Programs and Systems, Inc. when they were contracted to complete some specialized computer services.

A data security screening caught the disclosure on September 29, 2014 that exposed patient information between May 2012 through September 2014.

The information exposed included patient names, addresses, dates of birth, treatment information, diagnosis, health insurance information and Social Security numbers. All of this information could be accessed via the Internet.

For those who might have been affected you can call 1-888-227-1416-1-888-227-1416 Monday through Friday between 9:00 a.m and 9:00 p.m Eastern Time.

More Information: http://www.phiprivacy.net/highlands-cashiers-hospital-discovers-patient-

Information Source: PHIPrivacy.net
Records from this breach used in our total: 25,000

November 28, 2014

University Hospitals
Cleveland, Ohio

University Hospital has informed 692 patients of that their personal information has been compromised. An employee of the hospital had been accessing the personal information of patients for over 3 years. The employee has been dismissed.

The information this person accessed included names, addresses, phone numbers, email addresses, medical and health-insurance account numbers, financial information including debt/credit card information and Social Security numbers.

Those with additional questions or concerns can call (866) 329-5860


Information Source: Media
Records from this breach used in our total: 692

November 26, 2014

Shutterfly/Tiny Prints/Treats/Wedding Divas
Redwood City, California

Tiny Prints, Treat and Wedding Paper Divas, owned by Shutterfly Inc. notified customers of a data breach to their online system by hackers. The hacking may have exposed customer usernames and passwords. The company is urging customers to change all usernames and passwords to each site.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-47602

Information Source: California Attorney General
Records from this breach used in our total: 0

November 25, 2014

Texas Health and Human Services
Houston, Texas

The Texas Health and Human Services department discovered a data breach it appears by "chance" after terminating their relationship with Xerox Corporation.

"In August, after the transition to a new Medicaid vendor, the Texas commission filed a lawsuit against Xerox, alleging that the contractor had failed to turn over computer equipment, as well as paper records, containing Medicaid and health information for 2 million individuals, "putting the state out of compliance with federal regulations and at risk of massive federal fines," says a statement issued by Texas HHSC in August."

The Texas Health and Human Services department has notified individuals of the data breach communicating that their information may have been compromised. The information includes "Medicaid clients' names, birthdates, Medicaid numbers, and medical and billing records related to care provided through Medicaid, such as reports, diagnosis codes and photographs."


Information Source: Media
Records from this breach used in our total: 0

November 25, 2014

State Compensation Insurance Fund
Pleasanton, California

The State Compensation Insurance Fund, a state agency that provides workers compensation insurance to businesses informed customers of a data breach when one of their brokers suffered a data breach to their system.

Lucy Gomez Blankley Interpreting Inc., a provider of Stat Fund was the victim of a computer hack that resulted in theft of
emails in which contained information regarding patient workers compensation claims.

The specific information included names, addresses, phone, Social Security Number, dates of birth and workers compensation claim number.

The agency is providing one year free of Experian ProtectMyID services to those who were affected. Those with questions can call 1-877-220-1388,

More Information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-47592](http://oag.ca.gov/ecrime/databreach/reports/sb24-47592)

Information
Source: California Attorney General

November 25, 2014  Godiva Chocolatier Inc.
New York, New York  BSR  PORT  Unknown

Godiva notified employees of the company of a data breach when a Human Resources employee, who was traveling to retail sites, had a briefcase stolen from a car. The briefcase contained a lap top that had employee information on it. The lap top was not encrypted.

The information included names, addresses, Social Security numbers and drivers license numbers.

The company is providing Experian ProtectMyID Alert for 12 months for free. For questions call 1-866-328-1993 Monday through Friday 6:00 a.m to 6:00 p.m Pacific time.


Information
Source: California Attorney General

November 24, 2014  Sony Pictures
New York, New York  BSO  HACK  47,000

Sony Pictures Entertainment has suffered a data breach when hackers posted threatening messages on company computers.

According to a report the threat "began with a skull appearing on screens, and then a strangely ominous message telling users they'd been hacked by something called #GOP. It gets more bizarre as the message claims this is just the beginning and then threatens to release documents by 11 PM this evening."

The company has completely shut down all email communications and employees are not allowed to use company computers while the entertainment giant works through where and what the threat is and if it is real. The original threat did not give specifics or communicate any kind of "ransom" for the data that had supposedly been hacked.


UPDATE (12/5/2014): A data security analyst has discovered information leaked by the hacker (s) goes beyond what was originally reported.

According to the security company Identity Finder, showed that leaked files included vast amount of personal data on "more than 47,000 celebrities, freelancers, and current and former Sony employees".

"An analysis of 33,000 leaked Sony Pictures documents by data security software firm Identity Finder showed that the leaked files included the personal information, salaries and home addresses for employees and freelancers who worked at the studio. Some of the celebrities include Sylvester Stallone, director Judd Apatow and Australian actress Rebel Wilson, according to the Wall Street Journal, which first reported on the analysis”.

Additional information such as contracts, termination dates, termination reason and other data was also leaks. Unfortunately these files were in Excel format without any password protection.


UPDATE (12/16/2014): "Sony Pictures Entertainment has been sued by two self-described former employees who accuse the movie studio of failing to protect Social Security numbers, healthcare records, salaries and other data from computer hackers who attacked it last month.

The proposed class action lawsuit against Sony Corp's studio was filed on Monday in federal court in Los Angeles. It alleges that the company failed to secure its computer network and protect confidential information."


UPDATE (06/16/2015): Sony Pictures Entertainment has been denied a dismissal of a lawsuit brought on by former employees who claim that their personal data was stolen in the 2014 hacking.

The judge stated "Sony created a "special relationship" with its employees by requiring them to provide personal information to be eligible for salaries and benefits."
UPDATE (09/02/2015): "Lawyers for former Sony Pictures Entertainment employees whose data was breached last year say they have tentatively reached a settlement with the company.

Wednesday's filing in a proposed class-action lawsuit does not detail settlement terms or how many current and former Sony employees would be covered by the settlement.

Plaintiffs' attorney Daniel Girard wrote that he and fellow lawyers believe the settlement is favorable to employees whose personal, financial and medical information was posted online.

Additional details about the settlement are expected to be filed in a Los Angeles federal court by mid-October."


Information
Source: Media
November 17, 2014 US State Department Washington, District Of Columbia GOV HACK Unknown

The US State Department shut down one of its computer networks when it was believed to have been hacked. Experts believe this is related to the breach to the White House's unclassified computer network.

On Monday Jeff Rathke, a State Department spokesperson said "the department had recently detected "activity of concern" in portions of the system handling non-classified emails, and the weekend maintenance included security improvements responding to the breach."


Information
Source: Media
November 14, 2014 Seattle Public Schools Seattle, Washington EDU DISC 8,000

The Seattle Public School District announced in a letter to parents Thursday about a data breach that involved their children's information.

"Late Tuesday night Seattle Public Schools learned that a law firm retained by the district to handle a complaint against the district inadvertently sent personally identifiable student information to an individual involved in the case. The district promptly removed the law firm from the case and is working to ensure that all improperly released records are retrieved or destroyed."

Over 800 special education students were involved in a breach. The information involved in the breach included their names, addresses, student identification numbers, test scores and disabilities.


Information
Source: Media
November 14, 2014 Cone Health Greensboro, North Carolina MED DISC 2,076

Cone Health notified patients to a data breach when after letters sent from one of its facilities were addressed to the wrong patients.

The information on 2,076 patients included names, Social Security numbers, dates of birth and insurance information.


Information
Source: Media
November 14, 2014 Reeve-Wood Eye Center Chico, California MED UNKN Unknown

The Reeve-Wood Eye Center reported a data breach to the California Attorney General's office. No specific details were provided as to the scope of the breach, type of breach or individuals affected.

Information
Source: California Attorney General
November 13, 2014 U.S. Weather System Washington, District Of Columbia GOV HACK Satellite systems that forecast weather

Officials from the National Oceanic and Atmospheric Administration (NOAA), which includes the National Weather Service, have notified officials of a data breach to the National Weather Service’s satellite network.
Reports are stating "hackers from China breached the federal weather network recently, forcing cybersecurity teams to seal off data vital to disaster planning, aviation, shipping and scores of other crucial uses, officials said."

It appears the system was affected in September, but officials did not communicate that there was a problem until late October. an NOAA spokesman Scott Smullen did confirm that there were hacks and communicated that "incident response began immediately".


Information Source: 
Media 
November 12, 2014 
Onsite Health Diagnostics 
Dallas, Texas 
MED HACK 60,582

Dallas-based Onsite Health Diagnostics, a third party contractor with state of Tennessee, who completes medical testing and health screenings for various government insurance plans has suffered a data breach. The company discovered hackers had gained access to a computer system that houses personal information for members of the Tennessee’s State Insurance Plan, Local Government Insurance Plan and Local Education Insurance plan.

The information affected in the breach included health benefit member names, dates of birth, addresses, emails, phone numbers and gender.


Information Source: 
Media 
November 12, 2014 
US Postal Service 
Washington, District Of Columbia 
GOV HACK 800,000

The US Postal Service is releasing information today that they have been the victim of a cyber attack with Chinese hackers being suspected of hacking into their computer networks compromising the information of over 800,000 employees.

Currently the FBI is investigating the breach and it appears that information obtained included names, dates of birth, Social Security numbers, addresses, dates of employment. According to officials, all postal service employees were affected and they are not yet clear why their information was of interest to these hackers. They are not seeing any evidence of customer information being compromised. The investigators are calling the hackers "sophisticated actors". More information will be posted as additional information comes out with the investigation.


Information Source: 
Media 
November 10, 2014 
Anthem Blue Cross 
Southern and Northern California cities, California 
BSF DISC Unknown

Anthem Blue Cross in California sent text emails with personal details about individuals health information and member specific demographic information such as age, language spoken, specific medical test received or not received as part of the text message.

The company is reviewing whether or not they have to report this information as part of the specific notification laws in California, which does include the breach of medical history, mental or physical condition, medical treatment or diagnosis by a health care professional.

A spokesperson for Blue Cross stated that they are investigating the incident.


Information Source: 
Media 
November 10, 2014 
Central Dermatology Center 
Chapel Hill, North Carolina 
MED HACK Unknown

Central Dermatology Center notified patients of a data breach to their system when malware was found on one of their servers.

The information compromised included patient names, addresses, phone numbers, dates of birth, Social Security Numbers, sex, treatment dates, account balances, email addresses, insurer, providers, employers and race.

Currently, the center has hired an forensic IT firm to investigate the breach. They did not provide the number of
individuals at risk.


Information
Source: Media
November 7, 2014

Jessie Trice Community Health Center
Miami, Florida

MED  HACK  8,000

Jessie Trice Community Health Center announced a data breach when members of an identity theft ring accessed the personal information of 8,000 patients.

The information accessed included names, dates of birth and Social Security Numbers. No medical information was compromised according to the facility.

The FBI and the IRS are currently investigating the breach.

More Information: http://www.clinical-innovation.com/topics/privacy-security/identity-theft...

Information
Source: Media
November 3, 2014

Fidelity National Financial
Jacksonville, Florida

BSF  HACK  Unknown

Fidelity National Financial, Inc (FNF) informed customers of a breach to their system due to a targeted phishing attack to certain employees.

FNF is the parent company of Ticor Title Company of Oregon, Ticor Title of Nevada, Inc., Lawyers Title Company, and Lawyers Title of Oregon, LLC, which provides title insurance and real estate settlement services in Oregon, Nevada, and/or California.

From April 14, 2014 and April 16, 2014 a certain number of employees were targeted in a phishing attack that allowed the hackers to obtain username and password information for employees of the company. The company hosts their email with a third party vendor and after investigating did not find any evidence that the hackers were able to breach FNF’s internal network or systems.

However, the investigation did reveal that personal information was obtained including Social Security numbers, bank account numbers, credit/debit card numbers and driver’s license numbers.

The company is offering 12 months free of AllClear ID to those affected. Those affected can call 1-877-676-0374 to reach an AllClear investigator.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-47112

Information
Source: Media
November 3, 2014

Palm Springs Federal Credit Union
Palm Springs, California

BSF  PORT  Unknown

The Palm Springs Federal Credit Union was conducting an audit of their systems and realized that one of their external hard drives that contained customer data was missing.

The information contained on the drive included customer names, addresses, Social Security Numbers and account numbers.

The credit union is offering AllClearID and AllClearID Pro for 12 months at no cost to those who were affected by this breach. For those with questions they can call 1-866-979-2595-1-866-979-2595 or the credit union at dpitigliano@palmspringsfcu.com.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-47289

UPDATE (1/16/2015): The National Credit Union Administration has announced that it will be paying Palm Springs Federal Credit Union $50,000 to help cover expenses incurred due to a data breach the credit union suffered. The regulatory agency is taking responsibility for the breach.

More Information: http://www.bankinfosecurity.com/agency-takes-responsibility-for-breach-a...
Reeves International Inc. is informing customers of a data breach of one of their online retail sites called Breyer Horses (www.breyerhorses.com). On September 9, 2014 the company discovered an unauthorized party installed malware on the server hosting the Breyer Horse website, the malware compromised customers' personal data. The dates of the attack were from March 31, 2013 through October 6, 2014.

The information compromised includes names, addresses, website usernames and passwords, payment card account numbers, card expiration dates, and payment card security codes.

For anyone affected or those with questions call 1-877-572-0628 twenty-four hours a day Monday through Sunday (excluding holidays).

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-47096

On October 23, 2014 American Soccer Inc./SCORE Wilmington, California BSR HACK Unknown

On October 21, 2014 SCORE discovered an unauthorized access to their server that processes customer payment information.

According to the company on September 4, 2014 unauthorized access to their website compromised personal information of individuals who completed a transaction.

The information includes names, payment card account numbers, expiration dates of cards, SCORE account numbers. Those who were affected conducted a transaction between June 1, 2014 and September 4, 2014. There was no evidence that customer addresses or security codes being compromised after an investigation was conducted.

For those with questions or concerns call 1-800-626-7774.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-46986

On October 20, 2014 Staples Inc. Framingham, Massachusetts BSR HACK 1.2 million

Several large banks notified Staples Inc. of unusual activity on credit and debit cards used at several locations in Northeastern United States. According to Brian Krebs, Krebs on Security “According to more than a half-dozen sources at banks operating on the East Coast, it appears likely that fraudsters have succeeded in stealing customer card data from some subset of Staples locations, including seven Staples stores in Pennsylvania, at least three in New York City, and another in New Jersey”. Staples Inc. has more than 1800 stores nationwide and is currently investigating the potential breach.

More Information: http://krebsonsecurity.com/2014/10/banks-credit-card-breach-at-staples-s...

UPDATE (11/17/2014): It appears that the breach that happened at Staples was conducted by the same cyber criminals that infiltrated Michaels stores. According to Krebs On Security “Multiple banks interviewed by this author say they’ve received alerts from Visa and MasterCard about cards impacted in the breach at Staples, and that to date those alerts suggest that a subset of Staples stores were compromised between July and September 2014.”

More Information: http://krebsonsecurity.com/2014/11/link-found-in-staples-michaels-breach...

UPDATE (12/19/2014): After an investigation, Staples Inc. said that nearly 1.2 million customers payment cards. “Staples said Friday that the investigation revealed that the hackers used malware that provided access to information for transactions at 115 of its stores. The hackers stole cardholder names, payment card numbers, expiration dates and card verification codes. The company is offering free identity theft protection services.

More Information: http://www.huffingtonpost.com/2014/12/19/staples-breach-payment-cards_n...

Sourcebooks Inc. has informed customers of a breach of their shopping cart software that supports several of their websites. The breach dates were from April 16, 2014 and June 19, 2014. An unauthorized party gained access to specific customer purchase information.

The information breached includes first names, last names, email addresses, phone numbers, addresses, account passwords, credit card numbers, expiration dates of credit cards, cardholder names and card verification values.

The company is conducting an investigation including a forensic audit to determine the full extent of the breach.

For those with questions or concerns call 1-844-810-1155 between 8:30 a.m and 5:30 p.m Central Standard Time or go to http://www.sourcebooks.com/cardfaq.
Cyberswim.com notified customers of a data breach to their online ecommerce store and the discovery of customers' personal information being breached.

On September 24, 2014 the company confirmed that an unauthorized individual(s) or entities installed malware on the server hosting their website. This malware was able to access personal information entered by customers when completing a purchase on the site.

Information breached includes names, addresses, website usernames and passwords, payment card account numbers, card expiration dates, and payment card security codes.

Purchases made between May 12, 2014 and August 28, 2014 are the dates this breach occurred.

For those with questions call 1-844-286-4855 between 9:00 a.m and 5:00 p.m Easter time, Monday through Friday (excluding holidays).

Novant Health Gaffney Family Medical Care informed patients of a data breach when their offices were broken into and two of the facilities laptops were stolen.

The information on the laptops was not disclosed.

Snapsaved.com, a third party vendor to Snapchat, announced that their servers were hacked, which in turn caused thousands of photos and videos from the third party service to show up on the Internet.

"On Sunday, thousands of photos and videos from the Snapchat service were put online, apparently taken from sites including Snapsaved.com, which had allowed people to log in using their Snapchat username and password to offer desktop-based rather than handset-based access to the site - and also the chance to store photos, which are meant to be deleted within seconds of being viewed."

Snapsaved posted on Facebook the following:

"I would like to inform the public that snapsaved.com was hacked" due to a mistake in the setup of its web server. "As soon as we discovered the breach in our systems, we immediately deleted the entire website and the database associated with it," the unsigned statement continues. "As far as we can tell, the breach has affected [sic] 500MB of images, and 0 personal information from the database."

The University California Davis Medical Center discovered abnormal activity in the email account of one of their providers. An investigation determined that the provider's email was compromised by an unknown source. As a result, an unauthorized use and access to their system giving them access to communication between the provider and the patients.

For additional questions regarding the incident contact 1-916-734-8808 or email privacyprogram@ucdmc.ucdavis.edu
The office of Dr. Barry J. Snyder at Penn Highlands Brookville, a healthcare service provider for the Brookville area in Pennsylvania, notified patients of a data breach when a third party accessed the third party vendor's server who maintains records for Dr. Snyder.

The information compromised included patient names, addresses, dates of birth, driver's license numbers, Social Security numbers, phone numbers, insurance information, medical information and genders.

The facility is offering free identity monitoring and identity protection services to affected individuals through Kroll Inc. Those affected can call 1-855-401-2640.


Sears Holding Corp announced Friday that a data breach occurred at their K-Mart stores starting last month, with malicious software targeting their Point of Sale systems that compromised customers' credit card information.

Currently, Sears Holding Corp is not clear as to the number of affected customer cards and the breach is currently under investigation. K-Mart has said that they were able to remove the malware from their systems.

K-Mart is working currently working with federal investigators.

For those with questions, they are asked to call K-Mart's Customer Care Center at 1-888-488-5978.


The Sausalito Yacht Club notified its members of a data breach to their online member roster. The information on the roster included member names linked to private Sausalito Yacht Club member numbers. These two pieces of information together allows for the charging of beverages, goods, services and meals at the club. Additionally, members personal contact information, financial information, including accounts receivable information could have been obtained.

Currently, the breach is under investigation and depending upon what is found, the club may issue new cards and account numbers.

For those affected with questions they may call General Manager, Dave Martel at 1-415-332-7400 or by e-mail at gm@sausalitoyachtclub.org.

The Oregon Employment Department, specifically WorkSource Oregon, discovered a data breach of a database that contained personal information of individuals searching for jobs when an anonymous tip came in alerting officials of the breach.

Social Security numbers of more than 850,000 individuals were compromised in the breach. Officials shut down the website and were investigating the breach.
The Georgia Department of Behavioral Health and Developmental Disabilities (DBHDD) notified individuals of a data breach when one of their departments laptops was stolen out of a car of an employee who was attending a conference. The laptop contained personal information of over 3,000 patients including names, addresses, phone numbers, dates of birth, names of guardians, marital status, Social Security numbers, Medicaid numbers, diagnosis, behavioral data and other personal information. The laptops were not encrypted.

For those who might have been affected, they can call DBHDD at 844-888-5998 until January 9, 2015.

The Department of Human Services' Office of Behavioral Health in Denver Colorado notified individuals of a data breach when a postcard mailing went out to individuals as part of a survey. The cards were specifically addressed to individuals receiving behavioral health services through DHS office and mailed in post-card format.

This information is considered to be protected health information. According to the DHS no Social Security numbers or financial information was on the cards.

Evolution Nature Corp., dba The Evolution Store contacted customers regarding a data breach to their online stores affecting customer credit card information.

The company received a complaint of credit card fraud from a customer and launched an investigation by a data forensics expert. The investigation revealed that the administrative portion of the Evolution e-commerce site was accessed by an unauthorized third party that was using administrative credentials exposing customer order information.

The information exposed included names, email addresses, phone numbers, billing addresses, shipping addresses, order information, and credit/debit card information, including the CVV numbers on the backs of the cards.

The South Texas Veterans Health Care System informed 4,000 patients of a data breach to their personal information.

"South Texas Veterans Health Care tried to send veterans notices on September 15 to explain a new federal rule of Hydrocodone combination they need to be aware of. But in the process of printing the letters, they mistakenly came out double-sided and had one unique veteran's information on one side and another veteran's on the other."

The information breach included full names, addresses and the type of prescription drugs.

U.S Health Holdings, Ltd. on behalf of Macomb County Michigan has suffered a breach when an accidental disclosure of...
personal information was posted on the Michigan Inter-Governmental Trade Network ("MITN") website.

The information exposed included names, dates of birth, Social Security numbers, zip codes, cities, and Plan carrier names.


Information Source: PHIPrivacy.net

October 9, 2014  Albertina Kerr Centers
Gresham, Oregon  MED  PORT  1,300

The Albertina Kerr Centers have notified individuals of a breach when two of their laptop computers and a cell phone were stolen from the Albertina Kerr’s campus.

The laptops contained medical information identifying individuals, the diagnoses they received and treatments applied. The theft took place in August of 2014 when an individual or individuals broke into one the facilities offices at the Kerr’s crisis psychiatric care facility. According to the facility these laptops did not contain Social Security numbers or financial information.

The center is offering a year of free identity theft security monitoring. For those affected they can call 1-888-276-0529.


Information Source: PHIPrivacy.net

October 7, 2014  Municipal Bond Insurance Association (MBIA)
Purchase, New York  BSF  DISC  Unknown

Brian Krebs of Krebs On Security notified MBIA of a breach that exposed numerous customer account numbers, balances and various other sensitive data due to a misconfiguration on a company Web server.

"Much of the information had been indexed by search engines, including a page listing administrative credentials that attackers could use to access data that wasn’t already accessible via a simple Web search."

MBIA is one of the largest bond insurers, that offers municipal bond insurance and investment management products and services companies such as Aetna and Fireman’s Fund.

The company has since shut this website down and is currently investigating. No information is available to the number of individuals that may have been affected by the breach.


Information Source: Krebs On Security

October 6, 2014  AT&T
Dallas, Texas  BSR  INSD  1600

AT&T is at the center of another data breach to their system, this time, by an internal employee.

AT&T has announced that one of its staff members accessed account information of customers, which included Social Security Numbers, drivers license numbers, unique customer numbers, known as Customer Proprietary Network Information (CPNI), which includes information such as times, dates, durations and destination numbers of every call made. No specific numbers have yet been released.


UPDATE (10/7/2014): The Vermont Attorney General posted that 1,600 letters went out to customers regarding the recently announced data breach that happened in August of 2014 by an employee of AT&T. The employee has since been fired and the breach is still under investigation.


Information Source: Media

October 3, 2014  Mount Sinai Beth Israel
New York, New York  MED  PORT  10,790

Mount Sinai Beth Israel announced a data breach when a laptop computer was stolen from a staff room. According to the facility the laptop was password-protected but not encrypted.

The patient information housed on the laptop included patient names, dates of birth, medical record numbers, dates of service, procedure codes and description of procedures along with clinical information about patient care received. The facility has stated that patient Social Security numbers, insurance information, addresses and phone numbers were not stored on this particular laptop.
October 3, 2014  Touchstone Medical Imaging
Brentwood, Tennessee

Touchstone Medical Imaging notified patients of a data breach as a "result of an open share that was exposed to the Internet."

The information exposed included Social Security numbers, names, addresses, dates of birth, and phone numbers. The center stated that no medical information was stored in this exposed folder. They are not sure if any financial information was contained in this folder.

November 10, 2014  Community Technology Alliance
San Jose, California

Community Technology Alliance (CTA) is notifying individuals of a potential compromise of their personal information, when an employee's laptop was stolen on July 28, 2014.

CTA is a non-profit organization that administers the Bay Area Homeless Management Information Systems (HMIS) and helps hundreds of partner agencies. The information in HMIS can include names and Social Security Numbers, and various other pieces of personal information.

If services were being received from an HMIS Partner Agency in Santa Cruz California, those individuals are the ones at risk. The partner agencies include the following:

- Community Action Board
- Families in Transition
- Homeless Services Center
- Salvation Army of Watsonville
- Pajaro Valley Shelter Services
- Housing Authority of the County of Santa Cruz
- Encompass
- Front Street Housing, Inc.
- Mountain Community Resource Center
- Catholic Charities
- Veterans Resource Center
- Santa Cruz County Office of Education
- Santa Cruz County Health and Human Services Agency
- Housing Services Center
- Pajaro Rescue Mission
- New Life Community Services.

Flinn Scientific, Inc.
Batavia, Illinois

Flinn Scientific, an ecommerce site focused on scientific materials for teachers and students, notified customers of a data breach to their online payment system when a cyber attacker inserted malware to gain access to the server that hosts payment information.

The information breached includes payment card numbers, card verification codes, expiration dates, names, addresses, and email addresses.

The company has set up credit monitoring with AllClearID for 12 months for those individuals affected by the breach. For questions individuals can call 1-866-979-2595 to get credit monitoring started.

Provo City School District
Provo, Utah

The Provo City School District notified employees of a "phishing" attack Monday September 29, 2014 which allowed access to employees email accounts. Some employee email accounts contained files that may have had personally identifiable information.

Currently the school district is investigating the breach and notifying those affected.

Fort Hays State University

Fort Hays State University has notified 138 of its graduates that their personal information may have been compromised when personal information was "accidentally" exposed on the Internet. The information exposed included Social Security Numbers and various other pieces of personal information.

The university stopped storing Social Security Numbers of students five years ago, however anyone who attended the university prior to 5 years ago, their SSN information is still part of the university database.


AB Acquisition LLC announced the discovery of a separate criminal investigation involving payment cards of customers who shopped at Albertsons stores, ACME Markets, Jewel-Osco, Shaw's and Star Markets. The company has discovered that a different malware was used in some of the stores than what was discovered in the recent data breach incident on August 2014. This breach is more recent than the August breach and appears to have happened at the end of August, beginning of September 2014.

This newer breach reportedly captured account numbers, expiration dates, other numerical information and/or cardholder names.

The company has different point of sale systems at the different locations. Reportedly Albertson stores in Arizona, Arkansas, Colorado, Florida, Louisiana, New Mexico, Texas and their two Super Saver Food Stores in Northern Utah were not affected.

Those stores that were affected includes Albertsons stores in Southern California, Idaho, Montana, North Dakota, Nevada, Oregon, Washington, Wyoming and Southern Utah. In addition, ACME Markets in Pennsylvania, Maryland, Delaware and New Jersey were affected, along with Jewel-Osco stores in Iowa, Illinois and Indiana and Shaw's and Star Markets stores in Maine, Massachusetts, Vermont, New Hampshire and Rhode Island.

The timeframes of the breach are August 27, 2014 through September 21, 2014. The company is offering free credit monitoring for one year with AllClearID at no cost to those who were affected. For questions, call 1-855-865-4449.

More Information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-46749](http://oag.ca.gov/ecrime/databreach/reports/sb24-46749)

The University of Florida and Texas Health and Human Services Commission (HHSC) a cooperative project called the Texas Wellness Incentives and Navigation (WIN) Project for Medicaid patients, notified patients of a data breach. The University of Florida, acting as a partner of HHSC, sent letters to Houston area physicians requesting health records. Unfortunately, due to a database merging error, some of those health record requests were sent to the wrong physicians.

The information shared with the incorrect physician included names, Medicaid STAR+PLUS identification numbers, and dates of birth.

Those affected with questions can call 1-866-876-HIPA (4472).


"American Family Care of Birmingham is alerting customers following the theft of two laptops containing sensitive information from an employee’s vehicle earlier this summer".

The information on the laptops contained personal information of patients specifically related to work injuries, physicals, immunizations and drug screens. The lap top also included the names, dates of birth, addresses, phone numbers, medical record numbers, Social Security Numbers, additional medical information, insurance information, driver’s license numbers and dates of service.

Those with questions concerning the incident can call (800) 258-7535(800) 258-7535 extension 2588 or e-mail ComplianceOfficer@americanfamilycare.com.


The University of Florida and Texas Health and Human Services Commission (HHSC) a cooperative project called the Texas Wellness Incentives and Navigation (WIN) Project for Medicaid patients, notified patients of a data breach. The University of Florida, acting as a partner of HHSC, sent letters to Houston area physicians requesting health records. Unfortunately, due to a database merging error, some of those health record requests were sent to the wrong physicians.

The information shared with the incorrect physician included names, Medicaid STAR+PLUS identification numbers, and dates of birth.

Those affected with questions can call 1-866-876-HIPA1-866-876-HIPA (4472).

BayBio.org has notified individuals of a data breach to their online payment system. The non-profit organization has notified that the hacking to their payment system compromised credit card numbers in process.

The hacker inserted files that captured keystrokes of visitors to their site which included credit card numbers when individuals were either paying for a membership or an event being held by the non-profit. Payments are being taken by phone until the breach has been repaired.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-46727

Pacific BioSciences of California Inc. has notified patients of a data breach when an employee laptop was stolen from their home that contained some of their personal information.

The information included names, birthdates, and Social Security numbers.

The company has arranged credit monitoring services through AllClearID for one year at no charge. For those affected they can call 1-866-979-2595.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-46702

Viator Inc, was notified of a data breach by their credit card service provider when they had received numerous complaints of erroneous charges to accounts. Their investigation lead to seeing fraudulent charges to Viator customers via their online payment processing system.

The breach includes the compromise of customer credit card and debit card data, card expirations, names, billing addresses, email addresses and Viator "nicknames".

The company is offering 12 month of credit monitoring services at no cost. For those affected they can call 1-888-680-0710 to speak with someone.

The company is also asking customers to go into their accounts and change their passwords.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-46657

Tim McCoy and Associates, also known as NEAT Management Group informed customers of a data breach when the laptop belonging to one of the company's software engineers was stolen on August 27, 2014.

The information on the laptop included names, Social Security Numbers, dates of birth, addresses, phone numbers, employer identification numbers and email addresses.

The company is providing a free membership for a year to ProtectMyID. For those who were affected, they can call 1-888-829-6550.

More Information: http://oag.ca.gov/ecrime/databreach/reports/sb24-46601
The Napa Health and Human Services Department, specifically In Home Supportive Services (IHSS) notified patients of a data breach when one of their flash/thumb drives was missing from their offices on Coombs Street. This portable drive contained information specifically related to their Comprehensive Services for Older Adults Division of HHS.

The discovery was made of the missing drive when clean-up was happening to their offices after the recent Napa earthquake. The offices have not been occupied since the earthquake. The information on the drive included names, addresses, phone numbers and information regarding patients status in the IHSS program. The agency is reporting that no financial or Social Security information was on the flash/thumb drive.

They agency has reported the incident to the police and are treating the missing flash/thumb drive as a burglary.

More Information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-46595](http://oag.ca.gov/ecrime/databreach/reports/sb24-46595)

**Information Source:** California Attorney General

**September 10, 2014**

**Bartell Hotels**

**San Diego, California**

Bartell Hotels, who operates several hotels in San Diego, has announced that they have suffered a data breach of customer credit card information.

The Best Western Plus Island Palms Hotel & Marina, The Dana on Mission Bay, Humphreys Half Moon Inn & Suites, Pacific Terrace Hotel and Days Hotel – Hotel Circle had names, credit card numbers and credit card expiration dates of customers who stayed at these hotels between February 16, 2014 and May 13, 2014 breached.

The breach could have affected up to 55,000 individuals.

For those affected, they can contact a representative at 877-437-4010 Monday through Saturday 8 a.m. to 8 p.m. CT with questions or concerns.


**Information Source:** Media

**September 9, 2014**

**Beef O’Brady’s Restaurants**

**North Port, Florida**

Beef O’Brady restaurants appear to have been a victim of a data breach to their point of sale system, when unauthorized credit card transactions began appearing on financial statement of customers. These transactions were from numerous vendors in Texas, New York, and Massachusetts. The restaurant chain is located in Florida.

Reportedly, a minimum of four Florida Beef O’Brady’s restaurant locations have been compromised.

The information compromised included credit and debit card information.

The company is currently working with local law enforcement to further investigate the breach.


**Information Source:** Media

**September 5, 2014**

**California State University, East Bay**

**Hayward, California**

California State University, East Bay has notified individuals of a data breach that has occurred on August 11, 2014 when the University discovered unauthorized access to individuals information when an overseas IP address appears to have used a software tool designed to access information on a server without being detected. The server targeted contained personal information on various employment record transactions and some extended learning course information.

The specific information breached included names, addresses, Social Security Numbers and dates of birth.

The University has set up 12 months free of Experian’s ProtectMyID for those affected. For additional questions or concerns individuals can contact (888) 738-3759 a toll free number specifically set up to deal with questions/concerns regarding this breach.

More Information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-46513](http://oag.ca.gov/ecrime/databreach/reports/sb24-46513)

**Information Source:** California Attorney General
Yandy.com, an online retailer, notified customers of a data breach to their online payment system when the server that processes this information was hacked. The unauthorized user(s) gained payment card information, including the CVV numbers on the back of the cards, expiration dates, names, addresses and email addresses of customers.

For those affected with questions, they can call the company at 1-844-236-1015.

More Information: [http://oag.ca.gov/ecrime/databreach/reports/sb24-46527](http://oag.ca.gov/ecrime/databreach/reports/sb24-46527)

Reportedly, Healthcare.gov has suffered a data breach to one of their test systems by hackers. Currently the Obama administration is communicating that no personal information was compromised, but authorities are investigating.

According to the administration, “our review indicates that the server did not contain consumer personal information, data was not transmitted outside the agency and the website was not specifically targeted,” said Aaron Albright, a spokesman at the Centers for Medicare and Medicaid Services, which runs the website. “We have taken measures to further strengthen security.”

"Mr. Albright said the hacking was made possible by several security weaknesses. The test server should not have been connected to the Internet, he said, and it came from the manufacturer with a default password that had not been changed.

In addition, he said, the server was not subject to regular security scans as it should have been”.


The Home Depot appears to be another victim of a data breach of their POS systems, reportedly by the same Russian hacking group that hit Target, Michaels, Neiman Marcus and P.F. Chang’s.

Brian Krebs of Krebs on Security reported that a significantly large amount of debit and credit card information went up for sale on the underground cybercrime sites, all leading back to purchases made at Home Depot stores across the US.

Home Depot is currently investigating the potential breach. Updated postings will follow as more information comes in.


UPDATE (9/10/2014): The Home Depot has now confirmed that their credit card processing systems were compromised in 2,200 of its stores across the U.S and Canada. Currently, no information has been released as to the number of individuals affected. Authorities are predicting this could surpass the 40 million individuals affected by the Target hacking.


UPDATE (9/16/2014): “A group of attorneys general have opened a multistate investigation into the recently confirmed data breach at Home Depot Inc.”

Attorneys General in Connecticut, Illinois and California will be leading the investigation to uncover the cause of the data breach and how the retailer has handled the breach with their affected customers.


UPDATE (9/18/2014): The Home Depot has announced the data breach they suffered earlier this month has affected approximately 56 million credit and debit cards. This makes this breach the second largest breach ever, just behind TJX’x co’s breach of 90 million records. The also announced that they see no evidence of any breach of their stores in Mexico or for those who shopped at their online store, HomeDepot.com.


UPDATE (9/26/2014): At least 15 law suits have been filed against The Home Depot for the recent data breach that occurred in US and Canadian stores. The lawsuit alleges that The Home Depot neglected to secure customers’ financial and personal information. Most of the cases were filed by customers, however two credit unions and one bank have also filed suit.


UPDATE (9/29/2014): The Home Depot has posted a page on their website regarding the recent data breach, for consumers who were affected. This page will advise you on what to do and how to obtain information to take advantage of
the free 12 month credit monitoring services. Make sure to scroll down past the photo.

More Information: https://corporate.homedepot.com/MediaCenter/Pages/Statement1.aspx

UPDATE (11/14/2014): The Home Depot has now announced that on top of the 56 million customers who had financial information compromised in the breach, the hackers also made off with 53 million email addresses of customers as well.


UPDATE (11/25/2014): The Home Depot is facing 44 civil lawsuits in the U.S and Canada as a result of the data breach that occurred across the organizations retail stores. Currently the company "has been working to deploy EuroPay MasterCard Visa (EMV) chip-and-pin security at each of its U.S. and Canadian stores. The breach compromised the financial details of customers who shopped at any of Home Depot's 2,266 stores in the U.S. and Canada".


Information Source: Media
September 1, 2014 Apple Cupertino, California records from this breach used in our total: 56,000,000 BSO HACK Unknown

Apple's iCloud service

"A few days ago a group calling themselves hackappcom posted a proof of concept script on the popular code repository called Github that would allow for a user to attempt to breach iCloud and access a user account. This script would query iCloud services via the “Find My iPhone” API to guess username and password combinations. The problem here was that apparently Apple was not limiting the number of queries. This allowed for attackers to have numerous chances to guess password combinations without the fear of being locked out".

The number of celebrity photos or private information breached is still unknown.


Information Source: Media
August 29, 2014 Memorial Hermann Hospital Houston, Texas records from this breach used in our total: 0 MED INSD 10,604

Memorial Hermann Hospital is notifying patients of a data breach when they discovered a former employee accessed medical records of more than 10,000 patients.

Reportedly the former employee had been accessing patient information for over seven years, December 2007 through July 2014, that were outside their normal job description.

The information breached included patients' medical records, health insurance information, Social Security numbers, names, addresses and dates of birth.


Information Source: Media
August 29, 2014 AltaMed Health Services Los Angeles, California records from this breach used in our total: 1,060 MED INSD 2,995

AltaMed Health has notified patients of a data breach when a temporary employee and other individuals were reported to be under investigation for an identity theft scheme, according to Arcadia law enforcement agents. No arrests have been made currently, but the investigation is continuing.

"Law enforcement disclosed it recovered a hard drive and other evidence during its investigation, that this hard drive and evidence may include the organization’s records, and that it believes this information may have been misused by participants in the identity theft ring currently under investigation".

The investigation has shown that this temporary employee accessed electronic and paper records for individuals that attended community events in Orange and Los Angeles counties from October 24, 2013 through June 6, 2014. The temporary employee was hired to help with patient enrollment.

The records this person had access to included names, email addresses, telephone numbers, Social Security numbers, provider information, insurance information, dates of birth, and addresses.

AltaMed is offering AllClear ID and AllClear ID Pro for those individuals affected. You can find information regarding these services by calling (877) 579-2263

More Information: https://oag.ca.gov/system/files/AltaMed%20Individual%20Notice%20Template...
August 29, 2014 Beachwood-Lakewood Plastic Surgery
Beachwood, Ohio

Beachwood-Lakewood Plastic Surgery and Dr. Stevem A. Golman, notified patients of a data breach when their office in the Parkway Medical complex were burglarized. The theives stole computer hardware that included patient information that included names and limited medical information.

The medical practice is offering you one year of credit monitoring at no cost. This service is provided by All Clear ID.

If you have any questions or would like to enroll in the credit monitoring service, call 1-877-615-3745.

August 28, 2014 J.P Morgan Chase
New York, New York

The FBI is investigating a sophisticated hacking attack on JP Morgan Chase and potentially seven other financial institutions. Originally it was reported that possibly one to four other institutions may have been affected, but it appears that the breach could be much larger than originally thought.

The hackers, who are reportedly Russian, gained enough personal information to completely wipe out bank accounts. The sophisticated and coordinated attacks go beyond the typical criminal hacker (s) according to authorities. Investigators are looking into the reasons behind the coordinated attack.

It appears that not only did the hackers gain access to the accounts, but also altered and possibly deleted information.

The attack appears to have been coordinated and directed at specific JP Morgan Chase employees to gain access to their computers and databases at the bank.

Experts are communicating that the hackers would have had to of spent a significant amount of time researching and studying the record system of the bank prior to attempting any kind of unauthorized access. "What was even more concerning is these hackers were able to modify records using high-level credentials and do it in a way that was undetected."


UPDATE (9/16/2014): After further investigation by authorities and Chase Bank, the breach they suffered isn't as severe as originally anticipated. The bank has confirmed that the hackers were able to gain access only to names, addresses and phone numbers, no financial or bank account information was accessed.


UPDATE (10/3/2014): The cyber attack JPMorgan Chase & Co. faced this summer compromised personal information in much greater numbers than first reported. Originally the numbers reported were over 1 million affected customers. After an investigation, JP Morgan Chase reports that hackers gained access to data on more than 76 million account holders—names, addresses, phone numbers and emails. Information on an additional 7 million small businesses was obtained as well. 

"JPMorgan Chase said that names, addresses, phone numbers and email addresses were stolen from the company's servers, but only customers who use the websites Chase.com and JPMorganOnline and the apps ChaseMobile and JPMorgan Mobile were affected".


UPDATE (12/22/2014): The computer breach at JP Morgan Chase could have been avoided according to security experts if the bank had installed an easy security fix to a server that was overlooked.


August 27, 2014 Dairy Queen
Edina, Minnesota

Dairy Queen has reported a data breach of their POS (Point of Sale) system when malware authorities are calling "Backoff" was found on the system. This same malware authorities are attributing to the Target and Supervalu Inc. data breaches. Currently the restaurant chain is unclear as to how many stores were affected.

Dairy Queen operates 6,300 restaurants across the US, many of which are franchisees that are not required to report fraud to Dairy Queens headquarters.

Currently Dairy Queen is working with authorities to uncover the specifics.
UPDATE: (9/10/2014): Dairy Queen has announced that several of its stores will go to a “cash only” model in lieu of the current data breach the fast food restaurant chain suffered. The company stated that only a small portion of its 4,500 stores were affected, but they would not say how many or which restaurants will be going to a cash only system.

UPDATE: (10/10/2014): On Thursday, Dairy Queen confirmed that 400 stores and one Orange Julius location were compromised as a result of the point of sale malware first reported back in August. The investigation also confirmed that the hackers used compromised credentials of a third party vendor to infiltrate Dairy Queen’s POS system.

Information
Source: Media
August 26, 2014 Milpitas Knights PAL Youth Football
Milpitas, California
BSO PHYS 80

Parents of 80 youth football players were notified of a data breach, when a bag of registration materials required by the league were stolen from the back seat of a volunteer’s car.

The information included original birth certificates and physical forms. The league did not comment on what information was entered on the physical form.

Information
Source: Media
August 26, 2014 The Hand Care Center/Shoulder and Elbow Institute
Orange, California
MED PHYS 10,000

The Hand Care Center/Shoulder and Elbow Institute in Orange California notified patients of data breach when they were notified by Iron Mountain Record Management, a facility where the medical practice stores old files, that 25 boxes of X-rays were stolen by two employees of the storage company. The employees sold the X-rays to a recycler who melted them down to recover the silver.

The information in the X-ray files included patient names, dates of birth, gender, treating physician, medical record numbers and the image on the X-ray itself.

For those possibly affected, they can call the center at 1-877-615-3762. The center is reporting that any X-rays taken after 2002 were most likely not affected.

Information
Source: PHIPrivacy.net
August 26, 2014 Long Beach Internal Medical Group
Long Beach, California
MED PHYS Unknown

The Long Beach Internal Medical Group, Inc. in Long Beach California notified patients of data breach when they were notified by Iron Mountain Record Management, a facility where the medical practice stores old files, that boxes of records were stolen by two employees of the storage company. Reportedly the employees sold X-rays files to a recycler who melted them down to recover the silver.

The information in the files stored by the medical practice included names, sex, addresses, dates of birth, telephone numbers, account numbers, office charges, insurance information, diagnosis information, Social Security numbers.

Information
Source: PHIPrivacy.net
August 26, 2014 Geekface LLC
Pawcatuck, Connecticut
NGO HACK Unknown

Geekface LLC, which runs the online sites Hatchwise.com and eLogoContest.com notified customers of a data breach to their server that compromised personal information.

The information breached included names, addresses, birth dates, usernames, passwords, and Social Security numbers.

For those with questions or needing further assistance they can call 1-800-303-0911-800-303-0911 between 10:00 a.m and 5:00 p.m. EST Monday through Friday or visit hatchwise.com.
Imhoff and Associates, a criminal defense law firm notified clients of a data breach when a backup hard drive was stolen from a locked trunk of an employee's vehicle.

The personal information contained on the backup hard drive may have included names, birth dates, Social Security numbers, driver's license numbers, addresses, emails and phone numbers.

The firm is offering those affected 12 months of AllClear ID at no cost. Those individuals with questions can call 1-877-615-3769 to reach an AllClear ID representative, Monday through Saturday 8:00 a.m to 8:00 p.m Central Standard Time.

CareEvolve Inc, a subsidiary of BioReference Laboratories, Inc. have notified patients of a data breach to their system that may have inadvertently exposed personal information of patients.

CareEvolve, Inc. was reconfiguring a test server and accidentally exposed the server, making it accessible via the Internet. This particular server included patient names, home addresses, telephone numbers, ages, patient/medical record numbers, clinical tests, collection dates, dates of birth and Social Security numbers (196 SSN's exposed according to CareEvolve Inc).

Automated search engine data mining applications did access this information starting on February 2, 2014 and ended when the breach was discovered on March 19, 2014.

For those that may have been affected can call 1-800-229-5227 or email compliancedepartment@bioreference.com.

The US Investigations Services (USIS), a firm that performs background checks for U.S government employees had a breach in their data base. Cyber criminals were able to hack their system to gain personal information on employees with the Department of Homeland Security, U.S Immigration and Customs Enforcement and U.S Customs and Border Protection units.

The information breached included Social Security numbers, education and criminal history, birth dates, information on spouses, other relatives and friends including names and addresses.

Officials say the number may increase as the investigation continues.


UPDATE (9/18/2014): "The Office of Personnel Management will not renew any of its contracts with USIS, the major Falls Church, Va., contractor that provides the bulk of background checks for federal security clearances and was the victim of a recent cyberattack, officials confirmed Tuesday evening".

USIS conducted over 21,000 background checks per month for the US government and has been under scrutiny since the data breach in August.

More Information: http://www.washingtonpost.com/business/economy/opm-to-end-usis-contracts...

UPDATE (11/14/2014) It appears that the breach affecting the Department of Homeland Security goes beyond just this US governmental agencies. The Ex-DHS official warns of more USIS breach victims and is warning that the breach likely affected other federal workers beyond DHS.

Cedars-Sinai Medical Center in Los Angeles California has reported a data breach of at least 500 patients at the facility when an employee's laptop computer was stolen from their home during a burglary in June 2014. The laptop was password protected.

The records on the laptop included specific patient data such as lab testing, treatment and diagnosis, Social Security
numbers and other personal information.


**UPDATE** (10/3/2014): The data breach that occurred when an employee laptop was stolen, contained many more files than what was originally reported by the hospital. When the breach was made public, Cedars-Sinai hospital reported that 500 patient files were on the stolen laptop. After an investigation, the laptop actually contained personal information on 33,136 patients.


---

**August 22, 2014 ManagedMed Inc (A Psychological Corporation) Los Angeles, California**

ManagedMed Inc. (A Psychological Corporation) notified patients and the Attorney General's office of a data breach of their patient scheduling system.

According to the facility patient scheduling information was viewed via an unsecured webpage by at least two non-ManagedMed individuals. This information was visible from March, 2013 through May 15, 2014. The breach allowed unauthorized persons to access the facilities calendaring system and view the information.

This information included patient scheduling information, patient names, telephone numbers, names of providers, notes on the patient which could have included information on the type of visit scheduled or medication/test scheduled for the patient, and dates of appointments. According to the facility no SSN's, credit card or medical records information were exposed.

---

**August 20, 2014 The UPS Store Atlanta, Georgia**

The UPS Store, Inc has notified customers of a data breach when they discovered malware in their systems targeting UPS retailers. UPS retained a security firm to review their systems and found malware at 51 locations in 24 states. UPS has a total of 4,470 franchised center locations within the US.

The company announced that both credit and debit card purchases were impacted at the franchised locations from January 20, 2014 through August 11, 2014. The company has since removed the malware from their system.

The company put out the following information:

For those affected with questions, please call us at 1-855-731-6016."

For more information [http://oag.ca.gov/system/files/California%20Distribution_0.pdf](http://oag.ca.gov/system/files/California%20Distribution_0.pdf)

---

**August 18, 2014 Community Health Systems Franklin, Tennessee**

Community Health Systems out of Franklin Tennessee has announced a large data breach of their medical system. The breach occurred when hackers infiltrated the server of the health system compromising Social Security numbers, names and addresses for 4.5 million patients. Authorities believe that the hackers were based out of China and the attacks happened from April 2014 through June 2014.

The company operates 206 hospitals in 29 states and is currently doing further investigations regarding the attack.


**UPDATE** (8/26/2014): Five Alabama residents have filed a class-action lawsuit against Community Health Systems following last week’s announcement of the data breach of 4.5 million patients.

---

**August 18, 2014 MeetMe, Inc. New Hope, Pennsylvania**

For more information [http://oag.ca.gov/system/files/California%20Distribution_0.pdf](http://oag.ca.gov/system/files/California%20Distribution_0.pdf)

---
MeetMe, Inc. has announced a data breach of their system when hackers gained access to their customer information. The information included names, email addresses, and passwords. The company reported that they have contacted their customers to change their usernames and passwords.

**Information Source:**
California Attorney General

**August 15, 2014** Albertsons/AB Acquisitions LLC
Boise, Idaho

The Albertsons grocery chain in Southern California announced a data breach when hackers attempted to obtain customer credit and debit card information from its approximately 180 Southern California stores, as well as stores in several other states.

AB Acquisitions LLC which operates Albertson stores, ACME Markets, Jewel-Osco, Shaw’s and Star Markets all under New Albertson’s, Inc. confirmed that the data breach started as early as June 22, 2014 and ended July 17, 2014.

“Albertson stores in Idaho, Montana, North Dakota, Nevada, Oregon, Washington, Wyoming and southern Utah were also affected. In addition, ACME Markets in Pennsylvania, Maryland, Delaware and New Jersey; Jewel-Osco stores in Iowa, Illinois and Indiana; and Shaw’s and Star Markets stores in Maine, Massachusetts, Vermont, New Hampshire and Rhode Island were all impacted by this incident”. The company is offering customers who may have been affected by the breach a year of complimentary identity-protection services. For more information, customers can call (877) 932-7948 or visit Albertsons’ website.


**Information Source:**
Media

**August 15, 2014** Supervalu
Eden Prairie, Minnesota

Supervalu, which operates 3,763 outlets, both corporate and franchised stores, has reported a data breach in their point-of-sale system which affected some of its retail food stores, along with several of its stand-alone liquor stores. The information compromised includes account numbers and other information on customer payment cards used at the point-of-sale systems. The data breach occurred from June 22, 2014 through July 17, 2014 according to company spokesperson. The retail grocery chain has notified authorities and the breach is currently under investigation.


**Information Source:**
Media

**August 12, 2014** Freedom Management Group, LLC dba The Natural
Hauppauge, New York

The Natural, an online store, notified customers of a data breach to their system when an unauthorized party accessed customer payment card data. The unauthorized access occurred from 4/22/2014 to 7/17/2014.

The information accessed included customer credit and debit card numbers, expirations dates, names, addresses, and phone numbers, account numbers, and passwords.

The company has recommended that those affected change their online passwords to their online account. The company is offering AllClear ID at no cost for 12 months. For those affected they may contact the AllClear ID team at 1-877-615-3771.


**Information Source:**
California Attorney General

**August 12, 2014** Orthopaedic Specialty Institute Medical Group
Orange, California

Orthopaedic Specialty Institute Medical Group has reported a data breach when it was discovered that 742 boxes of patient X-rays were stolen from an Iron Mountain Record Management storage facility. After an investigation by the authorities, it was discovered that two Iron Mountain Record Management employees stole the files and melted them down for the silver.

The information in the records, which are 10 to 15 years old, and could have included patient names, birth dates and medical record numbers.

For those who might have been affected they can call the medical group at 1-714-937-48251-714-937-4825 .

The University California Santa Barbara has notified unauthorized access to some archival payroll data that included names, social security numbers and direct deposit banking information.

The University has contracted with ID Experts to provide free credit monitoring service, and insurance for identity theft restoration.

If you need assistance enrolling or have additional questions, the University is requesting individuals call the UCSB / ID Experts team at 1-877-919-9184, between the hours of 6:00 am and 6:00 pm Pacific Time.

Anderson & Murison, a wholesale insurance broker, notified individuals of a data breach when individual retail insurance agents applied for personal umbrella insurance policies for their customers via Anderson & Murison’s online umbrella rating system.

When the retail agents requested an estimate through this online system, specific information regarding their customers was necessary to obtain the quote/estimate. Information such as first and last names, addresses, policy dates, policy numbers, premium costs, policy amounts, types of policies, dates of birth, all real estate owned and addresses, types of automobiles, other motorized equipment such as watercraft, occupations of both individuals and spouses, employer names and addresses, general information such as traffic violations, etc.

The company is offering identity theft protection through Kroll for one year at no cost. Those affected can call 1-844-263-8605.

San Mateo Medical Center (SMMC) notified individuals of a potential data breach when the facility discovered that an employee who was hired in the payroll unit of the facility failed to disclose a prior conviction for identity theft.

The employee was terminated immediately, but the individual had access to SMMC employee information including names, contact information, Social Security numbers and dates of birth.

The facility reported that they found “no evidence indicating that the employee misused confidential information from SMMC employee records”.

SMMC has engaged Kroll to provide identity theft protection for one year at no cost. For those affected they can contact the county at 1-844-530-4127 from 6:00 a.m. to 3:00 p.m. PDT.

Vibram USA Inc had notified customers of a data breach in their online ordering system. The company contracts with a third party web hosting provider vibramfivefinger.com whose systems were compromised when an unauthorized party accessed their system that manages online transactions and inserted malicious code.

The information that may have been compromised included credit card numbers.

The company has set up credit monitoring services through Experian. Those affected can call 1-877-371-7902

Vibrum USA Inc had notified customers of a data breach in their online ordering system. The company contracts with a third party web hosting provider vibramfivefinger.com whose systems were compromised when an unauthorized party accessed their system that manages online transactions and inserted malicious code.

The information that may have been compromised included credit card numbers.

The company has set up credit monitoring services through Experian. Those affected can call 1-877-371-7902
"A gang of Russian hackers has amassed over 1 billion username and password combinations and more than 500 million email addresses, a security firm reported late Tuesday, calling it the largest-ever haul of stolen Internet credentials.

The massive trove — stolen from hundreds of thousands of websites — was discovered by the Milwaukee firm Hold Security, according to a post on its website*.

According to reports by Hold Security, it took over seven months to identify the gang, "whom the firm dubbed CyberVor, or cyber-thief in Russian".

It appears that no payment card information or Social Security numbers were threatened.

PRC will provide updates as the story unfolds.

*note: state location provided is that of Hold Security LLC.

<table>
<thead>
<tr>
<th>Information</th>
<th>Source: Media</th>
<th>records from this breach used in our total: 0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>July 31, 2014</strong></td>
<td><strong>Recreational Equipment Inc. (REI)</strong></td>
<td><strong>Kent, Washington</strong></td>
</tr>
<tr>
<td><strong>BSR</strong></td>
<td><strong>HACK</strong></td>
<td><strong>Unknown</strong></td>
</tr>
</tbody>
</table>

On July 23, REI discovered that a third-party may have accessed REI customer accounts without authorization obtaining email addresses and passwords.

For those affected who have further questions about this incident, please contact them at privacy@rei.com or 1-800-426-48401-800-426-4840 Monday through Sunday 4 a.m. to 11 p.m. Pacific Time.

<table>
<thead>
<tr>
<th>Information</th>
<th>Source: California Attorney General</th>
<th>records from this breach used in our total: 0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>July 30, 2014</strong></td>
<td><strong>CVS/Caremark</strong></td>
<td><strong>Atlanta, Georgia</strong></td>
</tr>
<tr>
<td><strong>BSR</strong></td>
<td><strong>DISC</strong></td>
<td><strong>350</strong></td>
</tr>
</tbody>
</table>

As reported by a local news station in Atlanta Georgia reported a breach by CVS/Caremark when a mailing went out to CVS Caremark customers offering a switch to a 90-day prescription supply.

Unfortunately the mailings went out to the wrong addresses. "CVS Caremark is in the process of notifying the affected members that due to a programming error, letters intended for fewer than 350 plan members were sent to incorrect addresses".

The company said they sent the mailings July 15 and fixed the error after getting complaints. The information exposed were individual names, addresses and what prescriptions the individuals were on.

<table>
<thead>
<tr>
<th>Information</th>
<th>Source: Media</th>
<th>records from this breach used in our total: 0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>July 30, 2014</strong></td>
<td><strong>Rite Aid Pharmacy</strong></td>
<td><strong>Milton, Washington</strong></td>
</tr>
<tr>
<td><strong>BSR</strong></td>
<td><strong>PHYS</strong></td>
<td><strong>521</strong></td>
</tr>
</tbody>
</table>

Rite Aid Pharmacy in Milton Washington notified customer of a data breach, when someone stole a" stack of expired prescription records from a Rite Aid pharmacy in Milton, the company announced Wednesday".

"The records did not contain Social Security numbers or credit card numbers, and there has been no sign of resulting identity theft", spokeswoman Ashley Flower said.

The theft occurred on June 30 when a burglar entered a back room where the records were stored.

"Flower said 521 customers were notified of the theft via mail. She did not know how many records were stolen. The affected customers were offered a free identity theft consultation".

Those who were affected can contact Kroll Inc. at 855-269-6547 or Rite Aid at 800-RITE-AID.

<table>
<thead>
<tr>
<th>Information</th>
<th>Source: Media</th>
<th>records from this breach used in our total: 0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>July 30, 2014</strong></td>
<td><strong>Lasko Group, Inc.</strong></td>
<td><strong>West Chester, Pennsylvania</strong></td>
</tr>
<tr>
<td><strong>BSR</strong></td>
<td><strong>HACK</strong></td>
<td><strong>Unknown</strong></td>
</tr>
</tbody>
</table>

Lasko Group Inc. announced a data breach of customers who purchased on-line parts from them and Air King America Inc. Both companies were the victims of "phishing" emails from an unknown third party. These fraudulent emails led to unauthorized access to their computer network.
Information breached included names, email addresses, phone numbers, credit card numbers, and credit card expiration dates.

The company is offering AllClearID protect your identity for one year at no cost to those affected. For those who are affected they can sign-up by calling 1-866-979-2595 or at enroll.allclearid.com. The company has also established a confidential assistance line for questions or concerns at 1-877-218-0052 from 9:00 a.m. to 7:00 p.m. EST.

Information
Source: California Attorney General
July 29, 2014 Northern Trust Company Chicago, Illinois BSO DISC Unknown

The Northern Trust Company communicated a data breach to customers that involved their personal information. Northern Trust Company "provides or previously provided payment services for an employee benefits plan or program in which you participate or participated through. In that capacity, Northern Trust is responsible for maintaining certain personal information about you as a participant of that plan. Regrettably, we are writing to inform you about an inadvertent disclosure by Northern Trust of some of that information".

"As part of normal procedures, Northern Trust sends participant information to record-keeping companies that assist in administering those benefit plans and programs. In late May, a Northern Trust employee transmitted a file containing your information to one of our record-keeping companies that was not responsible for the plan in which you participate (d). The information included your name, address, Social Security number, and benefits plan or program account number, as well as other information about your benefits plan or program account, such as your payment /deduction amounts and, in some situations, bank routing and account numbers used for direct deposits".

Information
Source: California Attorney General
July 28, 2014 Backcountry Gear Eugene, Oregon BSR HACK Unknown

Backcountry Gear notified customers of a data breach with a server that handles credit card information. The company discovered malware that was put onto their server that was able to gain customer names, addresses, purchase information, and credit card/debit card information.

The company has stated they do not collect pin numbers or bank account numbers in a transaction so those would not have been compromised in the breach.

For those who were affected and have questions can call 1-800-953-5499 ext. 5 or email at data@backcountrygear.com.

Information
Source: California Attorney General
July 23, 2014 Wall Street Journal New York, New York BSO HACK Unknown

The Wall Street Journal was compromised by a Russian hacker who posted images of a list of user accounts claiming they were from the Wall Street Journal. The Wall Street Journal claimed they had an intrusion but that no data was affected.

The information has yet to be confirmed that it was from the Wall Street Journal, however the same type of intrusion was recently confirmed when this same hacker claimed an intrusion to CNET.

Information
Source: Media
July 22, 2014 Vice.com Brooklyn, New York BSO HACK Unknown

Reportedly a "Russian hacker group known as W0rm tweeted, along with screenshots, that it had hacked popular news, arts and culture site Vice.com and The Wall Street Journal website, and would sell each stolen database for Bitcoin."

The company has communicated that a hacker was able to access a list of Vice.com CMS users. This list included email addresses and hashed passwords. The company communicated that they since have patched the vulnerability.

Information
Source: Media
July 21, 2014 Dominion Resources Inc. Richmond, Virginia BSO HACK 1,700

Personal information of more than 1,700 people at Dominion Resources Inc. were compromised when unauthorized parties hacked the employee wellness plan. The hacker gained access via a subcontractor’s system, StayWell Health Management LLC who runs Dominions “Well on Your Way” program which includes a health screening, to gain the
information hacked.

The hacking actually occurred at a vendor Stay Well uses, Onsite Health Diagnostics, based in Irvine, Texas, that provides the sign-up mechanism for “Well on Your Way’s” health-screening appointments.

The information included individuals’ names, addresses, email addresses, phone numbers, gender and dates of birth of employees, spouses and domestic partners who went online to schedule a health-screening appointment going back to 2012.

“Dominion Resources said the company was notified of the breach on June 24 but didn’t learn the identities of those affected until July 7th. Dominion Resources is investigating why it took so long for the company to be notified. They are no longer using Onsite Health Diagnostics for scheduling”.

Information Source: Media

July 18, 2014

Penn Medicine Rittenhouse Philadelphia, Pennsylvania

Penn Medicine had to announce a data breach involving receipts that were stolen last month from a locked office in Pennsylvania Hospital.

The information on the receipts included combinations of patient names, dates of birth and the last four digits of credit card numbers.

Information Source: Media

July 17, 2014

Total Bank Miami, Florida

Total Bank, a subsidiary of Banco Popular that has 21 locations in South Florida, is notifying 72,500 customers that their account information was potentially exposed after an unauthorized third party gained access to the bank’s computer network.

Information obtained by this unauthorized third party included names, addresses, account numbers, account balances, Social Security numbers and driver’s license numbers.

The bank is offering 12 months free of credit monitoring services for those that were affected.

Information Source: Media

July 17, 2014

Bank of America Baltimore, Maryland

Aon Hewitt, a human resources benefits service provider for Bank of America, was made aware that a vendor’s former employee (Hexaware) sent a copy of certain files and inadvertently uploaded them to an FTP site.

The file contained names and Social Security numbers.

Information Source: Maryland Attorney General

July 16, 2014

Freshology Burbank, California

Only July 1, 2014 Freshology was performing a routine review of its Internet website and discovered unauthorized code. This code may have compromised billing names, addresses and credit/debit card information of customers.

Information Source: New Hampshire Attorney General

July 16, 2014

Central City Concern Portland, Oregon

Central City Concern in Oregon suffered a data breach when an unauthorized access resulted in the breach of clients data.

"On April 2, 2014, a federal law enforcement official notified Central City Concern that a former Central City Concern employee has been accused of improperly copying information from approximately 15 Central City Concern clients from its Employment Access Center (EAC) program with the intent of processing fraudulent tax returns in their names".
The information breached included names, dates of birth, Social Security numbers, addresses, and health information of EAC clients.

Client inquiries regarding this incident may be directed to 866-778-1144, Monday through Friday from 6:00 AM to 6:00 PM Pacific Time.

<table>
<thead>
<tr>
<th>Date</th>
<th>Entity</th>
<th>Geography</th>
<th>Sector</th>
<th>Code</th>
<th>Code</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 16, 2014</td>
<td><strong>Bay Area Pain Medical Associates</strong></td>
<td>Sausalito, California</td>
<td>MED</td>
<td>STAT</td>
<td></td>
<td>2,780</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Bay Area Pain Medical Associates have notified patients of a data breach when several of their desktop computers were stolen.

There were approximately 2,780 patients first and last names, number of years the patients had been seen at their practice. The are reporting that the computer data was encrypted and inaccessible, there was an Excel spreadsheet that containing this information that could have possibly been accessed. No Social Security numbers, dates of birth, financial information, contact information or medical information was exposed.

The facility is offering 12 months free of AllClearID. Those affected can call 1-877-579-2269.

<table>
<thead>
<tr>
<th>Date</th>
<th>Entity</th>
<th>Geography</th>
<th>Sector</th>
<th>Code</th>
<th>Code</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 16, 2014</td>
<td><strong>Apple Valley Christian Care Center</strong></td>
<td>Apple Valley, California</td>
<td>MED</td>
<td>DISC</td>
<td></td>
<td>500</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Apple Valley Christian Care Center has notified individuals of a security breach of their system when a "technical glitch" occurred. The center communicated that the compromised data varied greatly.

The information included Social Security numbers, dates of birth, home addresses, dates of stays, Medi-Cal ID numbers, Medicare ID numbers, and/or other insurance information such as Medi-Cal appeals, diagnosis codes, treatment information and medical history.

<table>
<thead>
<tr>
<th>Date</th>
<th>Entity</th>
<th>Geography</th>
<th>Sector</th>
<th>Code</th>
<th>Code</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 16, 2014</td>
<td><strong>Douglas County School District</strong></td>
<td>Castle Rock, Colorado</td>
<td>EDU</td>
<td>PORT</td>
<td></td>
<td>Unknown</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Douglas County School District notified employees of a data breach of their personal information when a laptop containing their personal information was stolen.

In a letter sent to district employees, the district stated that the stolen computer contained some workers’ Social Security numbers and bank account information.

The district is currently investigating the breach.

<table>
<thead>
<tr>
<th>Date</th>
<th>Entity</th>
<th>Geography</th>
<th>Sector</th>
<th>Code</th>
<th>Code</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 15, 2014</td>
<td><strong>Atlantic Automotive Corporation/dba One Mile Automotive</strong></td>
<td>Towson, Maryland</td>
<td>BSO</td>
<td>HACK</td>
<td></td>
<td>Unknown</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

One Mile Automotive is notifying customers of a data breach of one of their third party vendors, Trade Motion who operates automobile websites and has notified One Mile Automotive that this breach could have included personal information of some of its customers.

The information included names, addresses, email addresses, telephone numbers, credit card information.

Those who are affected should call 1-855-505-2774.

<table>
<thead>
<tr>
<th>Date</th>
<th>Entity</th>
<th>Geography</th>
<th>Sector</th>
<th>Code</th>
<th>Code</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 15, 2014</td>
<td><strong>City of Encinitas/San Dieguito Water District</strong></td>
<td>Encinitas, California</td>
<td>GOV</td>
<td>DISC</td>
<td></td>
<td>Unknown</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

"City of Encinitas and San Dieguito Water District recently were made aware that a Cal-PERS payment document containing Social Security numbers with corresponding employee and former employee names had inadvertently been made accessible to the public on the City's website on or about May 13, 2014 to July 3, 2014. Based on our research, we found the exposure has been limited to (16) people that accessed the document during that period."

The document contained information of employees and former employees who were enrolled in Cal-PERS during the following timeframes:
City of Encinitas–July 1993-October 2011
San Dieguito Water District–July 1989–October 2011

The city of Encinitas is offering 1 year free membership of Protect MyID Alert from Consumer Info.com by Experian.
For those affected with questions contact Courtney Barrett at 760-633-2631 or Jace Schwarm at 760-633-2636.

Information
Source: California Attorney General
July 15, 2014 Bank of The West
San Francisco, California

Bank of The West notified customers of an email scam that involved two employees' remote bank email login credentials being compromised. As a result of this unauthorized access, customer information could be at risk.

The information includes names, account numbers, loan numbers, Social Security numbers.

The bank is offering one year free of First Watch ID for those affected. For those with questions regarding the service they can call 1-866-310-7373 or 1-800-488-2263.

Information
Source: California Attorney General
July 14, 2014 Orangeburg-Calhoun Technical College
Orangeburg, South Carolina

"Orangeburg-Calhoun Technical College in South Carolina is notifying 20,000 former and current students and faculty members that an unencrypted laptop computer stolen this month from a staff member's office contained their personal information."

The information contained on the laptops included names, birth dates and Social Security numbers of individuals.

The college stated that the information goes back 6 or 7 years and that they believe the thief was after the hardware, not the data stored on it. The college neglected to comment on whether or not they are providing credit monitoring services for those affected.

Information
Source: Media
July 14, 2014 Goodwill Industries International Inc.
Rockville, Maryland

Financial institutions are tracking what appears to be fraudulent activity at numerous Goodwill retail stores. The fraudulent activity involves credit card breaches and that the compromised credit cards appear to have started at Goodwill stores across the country. The credit card information is then showing up at other retail establishments, similar to the breaches that occurred at Target, Neiman Marcus, P.F. Changs, etc.

"Goodwill Industries International was contacted last Friday afternoon by a payment card industry fraud investigative unit and federal authorities informing us that select U.S. store locations may have been the victims of possible theft of payment card numbers," the company wrote in an email.

"Investigators are currently reviewing available information," the statement continued. “At this point, no breach has been confirmed but an investigation is underway. Goodwills across the country take the data of consumers seriously and their community well-being is our number one concern. Goodwill Industries International is working with industry contacts and the federal authorities on the investigation. We will remain apprised of the situation and will work proactively with any individual local Goodwill involved taking appropriate actions if a data compromise is uncovered.”

Goodwill Industries stated they learned of the potential breach on July 18th and is working with federal investigators to determine if the breach is legitimate and if legitimate, how many stores were affected.

UPDATE (9/10/2014): Goodwill Industries announced that the data breach they suffered is linked to a third party vendor.

"Goodwill said a forensic investigation had found that a third-party vendor’s systems had been attacked by malware, providing the attackers with access to the credit card data of several of that vendor’s customers intermittently between February 10, 2013 and August 14, 2014.”

According to Goodwill, 330 Goodwill stores in 20 states were affected. Forbes reported that 868,000 individuals were affected.

Russian hackers infiltrated servers of CNET by the name of W0rm and the Twitter handle @rev-priv8, who "posted an image of remote access to a CNET.com server, with a screenshot of a shell proving a compromise of the site".

CNET would not comment on the nature of the attack or what information was compromised, they have just communicated that they have fixed the problem.

"The image posted on Twitter would indicate the hacker could access and upload files to the website. It's pretty difficult to say how they did it, though. One source suggested it was likely a content management system breach - something like a WordPress or Joomla exploit".

"Federal prosecutors have charged the owner of a Chinese aviation firm with trying to steal data about U.S. military aircraft by hacking into the computer networks of Boeing and other U.S. companies, according to a federal complaint unsealed in Los Angeles this week.

According to authorities, the individuals allegedly stole information from Boeing's C-17 transport plane. Evidence shows that the Chinese hackers obtained large amounts of data on dozens of military projects.

"Federal prosecutors have charged the owner of a Chinese aviation firm with trying to steal data about U.S. military aircraft by hacking into the computer networks of Lockheed Martin and other U.S. companies, according to a federal complaint unsealed in Los Angeles this week".

Allegedly, the Chinese hackers stole information about Lockheed's F-22 and F-35 fighter jets. Large amount of data were stolen on a dozen U.S military projects.

The University Illinois Chicago (UIC) notified former students of a data breach to their system that included the exposure of personal data.

"A website security breach made two College of Business Administration documents from the 2002 spring semester accessible — a roster from a Special Topics in Accounting course and an advising list for all junior and senior accounting majors, according to a statement from the university".

Personal information was exposed, including Social Security numbers. The university has not stated how many students were affected, and the breach is currently under investigation.

Penn State has notified 1,176 individuals that a data breach of their personal information had been breached. The Office of University Development and Alumni Relations at the Penn State College of Medicine was found to be "infected with malware that enabled it to communicate with an unauthorized computer outside the network".

The university used Social Security numbers as a personally identifiable number for students and these SSNs were found in an archived College of Medicine alumni list last used in 2005.

The university put out this information:

"For information about Penn State's efforts to minimize computer security risks, visit the University's Be Safe website at http://its.psu.edu/be-safe. For more detailed information about identity theft risks and prevention, visit http://www.ftc.gov/bcp/edu/microsites/dtheft/"
In March 2014, it has been reported that Chinese hackers broke into the computer networks of the United States government, specifically The Office of Personnel Management, which houses personal information of all federal employees. The hackers appeared to be targeting the files on "tens of thousands of employees who have applied for top-secret security clearance."

"The hackers gained access to some of the databases of the Office of Personnel Management before the federal authorities detected the threat and blocked them from the network, according to the officials. It is not yet clear how far the hackers penetrated the agency's systems, in which applicants for security clearances list their foreign contacts, previous jobs and personal information like past drug use."

This particular hacking is unusual as the US computer systems are constantly being hacked by international hackers, but up until this point, have been stopped before any information was compromised.

Currently, officials are investigating to pinpoint exactly where these attacks came from.

Heartland Automotive (Jiffy Lube) has notified customers of a data breach that has occurred when one of their company owned laptop was stolen with personal information on it.

The information included names, addresses, dates of birth, Social Security numbers.

The company is offering 12 months free of AllClearID. For those affected call 1-877-437-4004.

Secret Service notified The Houstonian Hotel, Club and Spa regarding a breach to their system that houses customer credit card information.

Once the notification happened, the company launched a forensics investigation and discovered that their POS system had been accessed by an unauthorized third party from December 2013 through June 2014, and that the credit card information stored on these systems were compromised.

The company has since stopped the intrusions, but has not communicated how many individuals were affected by the breach. The company is offering 12 months free of credit monitoring services for those affected.

Aecom has notified current and prior employees of a data breach that exposed employee personnel files. Hackers were able to penetrate their corporate network, which included the employee payroll system for the US specifically.

The information exposed included names, addresses, Social Security numbers, personal bank account numbers and routing numbers.

The company has set up 12 months of All ClearID at no cost. For those affected they can call which can be reached at 1-877-615-3770.

The Park Hill School District has informed current and former Park Hill students and employees of a data breach to their
A former employee downloaded files onto a hard drive without authorization. When the employee connected it to a home network, the files went onto the Internet. The information leaked included personnel files and Social Security numbers.

**Information Source:**
Media

**July 7, 2014**
**Legal Sea Foods**
**Boston, Massachusetts**
BSO   
HACK   
Unknown

Legal Sea Foods informed customers of a data breach that occurred on June 5, 2014 that a segment of their mail order web sales and e-commerce environment, that an unauthorized person gained access to a server that contained information from mail order web customer transactions.

After an investigation, transactions made between January 1, 2014 and May 21, 2014 were potentially affected, which included transactions used with credit cards. Names, credit card numbers, card expiration dates, and card verification values may have been breached.

The company has informed their payment processing company of the breach and the processor has been working with the credit card companies to provide them the card numbers of those affected.

**Information Source:**
Vermont Attorney General

**July 4, 2014**
**St. Vincent Breast Center**
**Indianapolis, Indiana**
MED   
DISC   
63,000

St. Vincent Breast Center have announced that patient’s health information may have been breached after the center sent around 63,000 letters to the wrong patients. The letters included patient names, addresses and in certain references to scheduled appointments. Reportedly no Social Security numbers, financial information or clinical information.

“St.Vincent Breast Center entered into an agreement with Indianapolis Breast Center P.C. and Solis Women’s Health Breast Imaging Specialists of Indiana P.C. after they both closed last year.

On May 5, St.Vincent Breast Center mailed letters intended for prior patients of the Indianapolis Breast Center and Solis Women’s Health to inform them that St.Vincent was available to provide care. Some letters also welcomed patients who had previously scheduled healthcare services.

Officials said on May 15, people who had accidentally received another person’s letter began calling St.Vincent”.

For those affected they can call 1-877-216-3862 from Monday through Friday 9:00 a.m. to 7:00 p.m.

**Information Source:**
Media

**July 3, 2014**
**Watermark Retirement Communities**
**Tuscon, Arizona**
BSO   
PORT   
Unknown

Watermark Retirement Communities Inc. informed current and former employees of the facility of a data breach when a laptop was stolen on June 13, 2014. The information on these laptops included names, addresses, telephone numbers, email addresses, dates of birth and Social Security numbers. The laptop was password protected.

For those affected they can call 1-800-597-6618.

**Information Source:**
California Attorney General

**July 3, 2014**
**Blue Shield of California/Department of Managed Healthcare**
**San Francisco, California**
BSF   
DISC   
18,000

The Department of Managed Health Care informed individuals of a breach concerning their personal information. Health plans regulated by the Department of Managed Health Care (DMHC) are required to provide the DMHC periodically with current rosters of the medical providers the health plans contract with.

These plans are not supposed to include confidential or personal information in the rosters because these rosters are generally public documents.

“The DMHC discovered that Blue Shield of California had inadvertently included provider Social Security numbers in the rosters Blue Shield provided to the DMHC in February, March and April, 2013”. Blue Shield neglected to inform the DMHC that the information was confidential or alert the DMHC that a mistake had been made on the documentation.

The information included Social Security numbers, providers’ names, business addresses, business telephone numbers, medical groups, and practice areas.

For those affected Blue Shield is offering you a free-one-year membership in Experian’s ProtectMyID Alert. For those with questions they can call 1-877-371-7902.
Up to 25 students at Milford Schools may have had their personal information stolen due to a data breach with a third party billing service, Multi-State Billing Services, located in Somersworth, New Hampshire, when an employee's laptop was stolen from their locked vehicle in May.

The laptop was password protected but not encrypted, contained information on nearly 3,000 students from 19 school districts in Central and Eastern Massachusetts.

The information on the laptop included names, addresses, Medicaid ID numbers and Social Security numbers.

Multi-State Billing will reimburse costs related to security freezes for the next three years. Information about reimbursement can be obtained by emailing customersupport@msb-services.com or phoning (855) 285-7433.

Because the children aren't actual victims of identity theft, the credit agencies may charge up to $5 each time to place, temporarily lift or permanently remove a security freeze.

---

Multi-State Billing Services LLC has let 19 school districts that they service, that a laptop that was stolen from an employee's locked vehicle contained records on nearly 3,000 students in 19 different school districts in Central and Eastern Massachusetts. The Central districts include Uxbridge, Ashburnham-Westminster Regional, Milford, Northboro, Northboro-Southboro Regional, Southboro and Sutton. Information on which Eastern school districts is currently unknown.

The information on the laptop included names, addresses, Medicaid ID numbers and Social Security numbers.

Multi-State Billing will reimburse costs related to security freezes for the next three years. Information about reimbursement can be obtained by emailing customersupport@msb-services.com or phoning (855) 285-7433.

Because the children aren't actual victims of identity theft, the credit agencies may charge up to $5 each time to place, temporarily lift or permanently remove a security freeze.

---

Students at Uxbridge School District may have had their personal information stolen due to a data breach with a third party billing service, Multi-State Billing Services, located in Somersworth, New Hampshire, when an employee's laptop was stolen from their locked vehicle in May.

The laptop was password protected but not encrypted, contained information on nearly 3,000 students from 19 school districts in Central and Eastern Massachusetts.

The information on the laptop included names, addresses, Medicaid ID numbers and Social Security numbers.

Multi-State Billing will reimburse costs related to security freezes for the next three years. Information about reimbursement can be obtained by emailing customersupport@msb-services.com or phoning (855) 285-7433.

Because the children aren't actual victims of identity theft, the credit agencies may charge up to $5 each time to place, temporarily lift or permanently remove a security freeze.

---

Goldman Sachs Group Inc warned customers of a data breach that occurred when an outside contractor emailed confidential client data to a stranger's Gmail account by mistake. The bank has asked a U.S. judge to order Google Inc to delete the email to avert a "needless and massive" breach of privacy.

"The breach occurred on June 23 and included "highly confidential brokerage account information," Goldman said in a complaint filed last Friday in a New York state court in Manhattan."
Goldman Sachs did not say how many people were affected and are asking Google to assist in tracking down who has access to the data.

The contractor meant to email a report to a gs.com account but inadvertently sent it to a similar email address with a gmail.com account. Goldman Sachs has not been able to retrieve the report and has not received a response back by the individual who owns the gmail account.

Information Source: Media
July 1, 2014 Vermont Health Exchange
Williston, Vermont

A Romanian hacker accessed the Vermont Health Exchange’s development server last December gaining access at least 15 times and going undetected for a month.

“CGI Group, the tech firm hired to build Vermont Health Connect, described the risk as “high” in a report about the attack. It also found possible evidence of sophisticated “counter-forensics activity performed by the attacker to cover his/her tracks.”"

“The report says that no private consumer information was stored on the hacked server, and that CGI Group had “verified that no additional servers [that may store private data] communicated with any of the identified attacker IP addresses.”"

This individual was able to gain access to the server because the default password on that server was never changed (in violation of guidelines laid out in the state’s official policy) along with the fact that the access to the server was never restricted to those users who were known and authorized to be on the server.

Information Source: PHIPrivacy.net
June 30, 2014 Butler University
Indianapolis, Indiana

Butler University in Indianapolis Indiana informed students, staff and alumni of a data breach to their system. Over 160,000 individuals may have been affected when hackers may have accessed their personal information.

The university was contacted by California officials to “inform them that they had arrested an identity theft suspect who had a flash drive with Butler employee’s personal information on it”. In a letter sent to those affected, the university has said that “someone hacked the school’s network sometime between November 2013 and May 2014”.

The school officials have discovered that the information exposed included birthdates, Social Security numbers and bank account information of approximately 163,000 students, faculty and staff, alumni, and prospective students who never enrolle in classes at Butler.

The university is offering a year of free credit monitoring.

Information Source: Media
June 30, 2014 San Antonio Metropolitan Health District
San Antonio, Texas

San Antonio Metropolitan Health District announced a data breach involving vaccination records of 300 children when a laptop containing these records was stolen.

The records included first and the last name of the patient, the patient’s date of birth, an identifier for the patient’s doctor, and the name of the immunizations. The laptop has since been recovered.

Information Source: Media
June 27, 2014 Benjamin F. Edwards & Company
St. Louis, Missouri

On May 27, 2014 Benjamin Franklin Edwards & Company (BFE) discovered an unauthorized access to their database which may have resulted in personal information of it’s customers being compromised. The company did not provide the exact information that was stored on their system, nor have they communicated how many individuals were involved.

For those that have an account and may have been affected the company is offering one year free of AllClearPro. They are asking individuals to contact their financial consultant for more information or go to www.enroll.allclearid.com to enroll.

Information Source: Media
June 26, 2014 Sterne, Agee & Leach
Birmingham, Alabama

Sterne, Agee & Leach has contacted customers regarding a data security incident that occurred between May 29th and
30th, 2014.

An employee of the brokerage firm was unable to locate their firm-issued laptop, which was password protected, but the data stored locally on the laptop was not encrypted. The data stored on the laptop included "account information utilized for mailing to certain Private Client Group customers whose accounts were opened between July 1, 1992 and June 30, 2013".

The information may have included names, addresses, account numbers and Social Security numbers. The information did not include dates of birth, account holdings, account passwords or access codes.

The firm is offering a free one year membership to Experian's ProtectMyID. Those affected must enroll by September 30, 2014, and can visit the website to enroll at www.protecmyide.com/redeem and utilize the activation code in the letter sent by the firm.

Information
Source: California Attorney General

June 26, 2014 Record Assist LLC Houston, Texas BSO HACK Unknown

Record Assist, LLC informed customers of an unauthorized access to their order processing system for ExpressVitals.com. The unauthorized access could have led to obtaining information such as the individuals name, address, credit card number, security code and Social Security number.

Those who are affected can contact the company at P.O Box 19686, Houston Texas 77224-9868 or call 1-844-245-5654.

Information
Source: Media

June 26, 2014 Orange Public School District Orange, New Jersey EDU HACK Unknown

A 16 year old New Jersey teen has been charged with unlawfully accessing the Orange Public School District's database and changing final grades and attendance records.

The Orange High School sophomore is facing multiple counts of second-degree computer theft for unlawfully accessing and altering data an one count of hindering apprehension.

Reportedly, the student accessed the computer system after obtaining the password of a staff member. Authorities do not know how the teen was able to gain the password information. An investigation is still underway.

Information
Source: Media

June 26, 2014 Splash Car Wash Greenwich, Connecticut BSR HACK 120,000

Splash car wash has notified approximately 30,000 customers of a data breach to their system when malwar was found on their point of sale system at several of their locations affecting and potentially breaching credit card data.

The car wash operates 13 locations in New York and Connecticut and was alerted by American Express of the breach. As soon as customers swiped their cards, the information was stolen, not giving the companies system time to encrypt the data. The breach is being investigated by authorities.

Information
Source: Media

June 26, 2014 Salina Family Healthcare Center Salina, Kansas MED DISC 500

"Salina Family Healthcare Center (SFHC) notified more than 500 patients of an unintentional transmission of unsecured personal patient protected health information after discovering the following event:

"On April 8, 2014, a staff member submitted a database to the National Commission for Quality Assurance (NCQA) for our involvement in a care coordination research study. The staff member responsible for our participation in the project inadvertently left a table in that database that included patients' names, dates of birth, chart numbers and CPT codes associated with their care. Upon opening the email, the NCQA staff member who received the database immediately recognized the breach, deleted the database, and notified our staff member".”

Information
Source: PHIPrivacy.net

June 24, 2014 Riverside County Regional Medical Center Moreno Valley, California MED PORT Unknown

The Riverside Regional Medical Center has notified patients of the loss of a laptop computer that contained personal patient information. The laptop went missing from a diagnostic services office in the hospital sometime between June 17,
The information on the missing laptop included names, dates of birth, medical record numbers and results of a nerve conduction study, and the names of the referring doctor and the doctor who performed the study.

The hospital did communicate that no Social Security numbers, health insurance information or home addresses were stored on this particular laptop.

For those who were affected, they have been asked to call Christina Quijada at 1-877-500-1255 or the Riverside County Privacy Office at 951-955-5757.

June 21, 2014  
**NRAD Medical Associates**
*Nassau, New York*

NRAD Associates informed patients of a data breach to their system when a radiologist employed with the facility accesses patient information without authorization.

As disclosed by NRAD the information the Dr. accessed included the following information: names, addresses, dates of birth, Social Security numbers, health insurance information, diagnosis codes and procedure codes.

For those with questions or concerns, call 1-800-926-8180 or go to the link [www.NRAD.com/answers](http://www.NRAD.com/answers)


**UPDATE** (12/4/2014): A physician with NRAD Associates has been arrested for the theft of protected health information of 96,998 patients of the medical facility. James Kessler, a Radiologist with the facility has been charged with Unauthorized Use of a Computer, Unlawful Duplication of Computer Related Material in the 2nd degree and Petit Larceny, all of which are misdemeanors in the state of New York.

As disclosed by NRAD the information the Dr. accessed included the following information: names, addresses, dates of birth, Social Security numbers, health insurance information, diagnosis codes and procedure codes.


June 20, 2014  
**UCDC, Washington Center**
*Washington, District Of Columbia*

The University California, Washington Center received a notification of unsolicited emails being sent to alumni of the university. After an investigation, it was revealed that someone accessed the pre-enrollment system, GoSignMeUp.com, which is a cloud-based provider for the online course registration utilized by UCDC to host its online course registration process.

The information breach included usernames, passwords, addresses, principal e-mails, gender, birth dates and UCDC course information. The university has stated that they do not record or store any Social Security numbers or financial account information on any of its databases.

For those who were affected the university is recommending individuals change their password.

Those with questions are asked to contact techhelp@ucdc.edu

Information  
Source:  
California
Mount Olympus Mortgage Company has notified customers of a data breach when a previous employee downloaded mortgage applications from their system to their private Internet accounts and then sent it to a competitor. The information included names, addresses, Social Security numbers, and other information in connection with mortgages.

**Information**

**Source:**
California Attorney General

**June 19, 2014**

Rady's Children's Hospital
San Diego, California

Rady's Children's Hospital has suffered a data breach when an employee inadvertently sent an email with a file attached to 6 potential job applicants. The applicants were meant to receive approved information for an internal evaluation, instead they received the original file with the information of 14,100 patients. The information included names, dates of birth, primary diagnoses, medical records and insurance carrier claim information. According to the hospital no Social Security numbers, credit card information, addresses or parent/guardian information were included in this file.

The file contained information on patientes admitted to the hospital between July 1, 2012 through June 30, 2013.

**Information**

**Source:**
Media

**June 18, 2014**

The Metropolitan Companies
New York, New York

The Metropolitan Companies, LLC, which is a conglomerate of companies from staffing services to interpreters suffered a data breach as a result of unauthorized access to their computer systems and may have potentially removed documents that included personal information of their customers.

Through an investigation, it has been disclosed that the information that was breached includes names, addresses, phone numbers, email addresses, Social Security numbers, dates of birth, past education, work history, and financial information. The company has not disclosed the number of individuals affected.

For those that may have been affected the company is providing one year of identity theft protection through Kroll. They can be contacted at 1-855-781-0033 to speak with a licensed investigator or visit their website at Visit www.kroll.idMonitoringService.com

**Information**

**Source:**
California Attorney General

**June 17, 2014**

Service Alternatives
Coupeville, Washington

Service Alternatives has informed individuals of a data breach to their payroll system. It appears that an unauthorized third person or persons obtained access to that system between November 2013 and March 2014. The information obtained included full names, addresses, dates of birth (excluding foster parents), Social Security number, Driver's license number or identity card number (excluding foster parents), tax documents, documents provided on form I-9 for anyone hired after Oct. 2010 (excluding foster) parents, bank routing number and account number if direct deposit was ever used.

Those who were affected by the breach may call 1-800-292-6697 or email support@servalt-adm.com

**Information**

**Source:**
Maryland Attorney General

**June 16, 2014**

Riverside Community College
Riverside, California

Riverside Community College has suffered a data breach affecting 35,212 students. On May 30th, a district employee emailed a file containing information about all students who were enrolled in the spring term to a colleague working at home due to illness, for a research report that was on a deadline. The district employee used a personal email account to send the data because the file was too large for the district’s secure email to send. The employee then typed in the incorrect email address.

The information contained in the file included names, addresses, birth dates, Social Security numbers, email addresses, student ID numbers, and telephone numbers.

The district has set up a Call Assistance Center at 1-888-266-9438 for affected students. The center will be open from 6 a.m to 6 p.m Monday through Friday for 90 days.

**Information**

**Source:**

**June 20, 2014**

Mount Olympus Mortgage Company
Irvine, California

BSF INSD Unknown

Mount Olympus Mortgage Company has notified customers of a data breach when a previous employees downloaded mortgage applications from their system to their private Internet accounts and then sent it to a competitor. The information included names, addresses, Social Security numbers, and other information in connection mortgages.
A thumb drive containing 33,702 patient records was stolen from the Redwood Regional Medical Group in Santa Rosa California. An employee placed the thumb drive in a "zipped container in an unlocked locker", where the drive was stolen.

The information contained on the device included patients’ first and last names, gender, medical record numbers, date of birth, date and time of service, area of body X-rayed, the X-ray technologist's name and the radiation level required to produce the X-ray. No other images such as MRI's or mammograms were stored on the device.

The medical center was taken over by St. Joseph Health on April 1st. The records were backed up to the drive as a precaution while they were being moved to Santa Rosa Memorial Hospital’s electronic medical records system.

Information Source: PHIPrivacy.net

PF Chang's is investigating a potential data breach, when credit cards showed up on an underground website that criminals use. Brian Krebs broke the story, when the banks he contacted confirmed that the cards had been used at P.F Chang's restaurants.

P.F Chang's is investigating the allegations currently with authorities.

UPDATE (06/30/2014): PF Chang's has had a class action lawsuit filed against the restaurant chain. The company confirmed on June 12, 2014 that a breach had occured. Some experts believe that the lawsuit is unlikely to succeed because some security experts have said, because proving consumer losses linked to the specific restaurant data breach is difficult to do.

Some believe it was a breach of the restaurant's POS system, most likely infiltrated by malware, similar to the Target and Salley Beauty breaches, the restaurant chain has yet to divulge any details, including the number of cards exposed.

UPDATE (8/4/2014): "P.F Chang's China Bistro Ltd. stated Monday that the data breach that affected customer credit and debit cards affected 33 locations throughout the continental U.S.", the investigatin is still ongoing.

Information Source: Krebs On Security

Stanford Federal Credit Union informed 18,000 members that their personal information was sent to another member accidentally. According to the letter sent to the members, credit union employees recognized the error immediately and the data was destroyed without it being read to the recipient. The data sent was a list of members who were pre-approved for loans. The credit union employee who sent the list inadvertently sent it to a member who had the same first name as the staff member it was meant for.

According to the credit union, the member had not yet read the mail and worked with the staff of the credit union to properly destroy it.

Information Source: California Attorney General

AT&T has informed California regulators of a data breach that occurred with a third party service provider.

"Employees of one of our service providers violated our strict privacy and security guidelines by accessing your account without authorization," the company said in a letter to affected customers. "AT&T believes the employees accessed your account as part of an effort to request codes from AT&T than are used to unlock AT&T mobile phones in the secondary mobile phone market."

Personal information such as Social Security numbers and phone records were accessed. The incident took place between April 9th through April 21st, but the California regulators were just informed this week.

AT&T would not disclose how many customers were affected, but the law requires disclosure if more than 500 people have been affected.
St. Francis Hospital notified patients of a data breach when a mass email to 1,175 patients was sent out where all email addresses were visible vs. having each patient being blind copied on the email.

The hospital is claiming that no medical treatment or other personal information was part of the email.

Those St. Francis patients who have questions about the incident are asked to call the hospital at 1-800-723-4998.

Information Source: Media

June 10, 2014

Access Health CT
Hartford, Connecticut
BSF INSD 413

The Connecticut health insurance exchange has suffered a data breach, when one of the exchanges employees lost a backpack at a local deli that included names, Social Security numbers and birthdates of 413 individuals.

The employee was not authorized to remove these documents from the facility and has since been put on administrative leave.

Information Source: Media

June 9, 2014

College of the Desert
Palm Desert, California
EDU INSD 1,900

The College of the Desert in Palm Dale California informed individuals of a data breach in their system when a college employee sent an unauthorized attachment in an email to approximately 78 college employees, that contained personal information of employees of the college.

The information contained in the attachment included names, Social Security numbers, dates of birth, genders, zip codes, titles of positions held at the university, employment anniversary date, employee identification numbers, insurance information, active or retired employee status.

Those who are affected are asked to call Stan Dupree, HR and Labor Relations Director at 760-674-3777 or sdupree@collegeofthedesert.edu

UPDATE (6/19/2014): According to new reports, The College of the Desert breach affected 1,900 current and former employees. The total individuals affected was not reported when the breach was made public.

Information Source: California Attorney General

June 7, 2014

Walgreens
Atlanta, Georgia
BSR INSD Unknown

Walgreens has notified some patients of a breach when an employee stole some patients information, which included names, dates of birth, and Social Security Numbers in the form of a Medicare ID number and provided the information to a third party. Walgreens is claiming that no credit card, banking or other personal information was involved.

The company has set up a hotling for those affected, 1-866-312-8654 from 7 a.m to 7 p.m Central Standard time, Monday through Friday.

Information Source: Maryland Attorney General

June 6, 2014

Miami-Dade County
, Florida
GOV UNKN Unknown

The county of Miami-Dade informed employees of a data breach where their personal information is being used to file fraudulent unemployment claims, along with credit card fraud. Currently, officials at the county are not clear if this breach happened internally or by external hackers.

They have not released what specific information has been compromised.

Federal officials at the U.S Inspector General's Office are leading the investigation due to false unemployment claims. The Human Resource Department of the agency has put out a statement.

"The recent news report on a “Data Breach” has understandably raised concerns amongst our employees regarding their personal information and whether they are one of the employees impacted by identity theft. Please be advised that when we identify a possible fraudulent unemployment claim, we immediately notify the Departmental Personnel Representative (DPR) for that employee. Our procedures are as follows:

The Human Resources Department receives the Notices of Reemployment Assistance once a claim for unemployment has been filed with the Department of Employment Opportunity (DEO). If a claim is identified as fraudulent (once HR confirms the employee is an active employee) HR contacts the employee’s DPR to provide notice to the Department and notification is immediately sent to the Department of Unemployment indicating that it is a fraudulent claim."
If an employee is notified that a fraudulent claim has been filed on their behalf, the employee should be instructed to do the following:

1. Contact the Unemployment Fraud Hotline to report the fraud at (800) 342-9909. They should report that their identity (SS#, Name) is being used to commit Unemployment Fraud.
2. Make a note of the Master Case File # that has been assigned by the Miami-Dade Police Department: PD130322106429.
4. Notify their banking institutions
5. Make routine checks on their bank accounts
6. Conduct thorough reviews on their bank and credit card statements
7. Visit http://myfloridalegal.com/identitytheft to learn more about Identity Theft

We assure you that fraudulent claims are being taken very seriously and every effort is being made to identify and refer these cases to the proper authorities for appropriate action.

Information
Source: Media

June 6, 2014  Penn State Milton S. Hershey Medical Center
Hershey, Pennsylvania

Penn State Milton S. Hershey Medical Center began alerting patients of a data breach when an employee accessed clinical data on an unauthorized computer and removable storage device. The employee did have permissions to have access to the files, but downloaded the clinical information on a removable storage device and his personal computer, both of which were not properly secured and outside of the medical centers IT department. The employee also used their personal email account to send emails with a test log of the data to two physicians at the medical center.

Information
Source: Media

June 5, 2014  Highmark
Pittsburgh, Pennsylvania

Health Insurer, Highmark Inc. notified customers that are members of either Security Blue or Freedom Blue, that their information may have been mailed to other people. The information mailed was a health risk assessment that included information such as names, addresses, dates of birth and certain medical information. The health insurer is claiming that no Social Security numbers were compromised.

Information
Source: Media

June 4, 2014  National Credit Adjusters
Hutchinson, Kansas

National Credit Adjusters have informed individuals of a breach that has happened when they were notified that some customers were receiving phone calls from unauthorized third party debt collectors. The information that these unauthorized debt collectors may have access to include names, addresses, debt balances, dates of birth and Social Security numbers. The information may also expand beyond the individual on the account to co-signers of the account as well.

The hackers pose as legitimate debt collectors but are actually calling with the attempt to scam individuals out of their money.

For those affected, the company is asking individuals call 1-855-737-9123.

Information
Source: California Attorney General

Midwest Urological Group notified patients of a data breach when a laptop was reported stolen when an employee may have inadvertently forgot to lock the cabinet that housed the laptop. According to authorities the laptop contained patient information that included treatment information on the patients at the facility. No specific details were released as to the type of information involved.


Information
Source: Media
Craftsman Book Company notified customers of a breach that occurred on their site. On Tuesday May 27th the company discovered unauthorized access to their site and recommended a change in their username and password. Since that time they discovered that the breach also included charges on customers credit card. The hackers found another site operated by the company and through the security vulnerabilities in the one site, they were able to get to the Craftsman Book site and ultimately to the customers information.

Since the vulnerability was discovered, the company has shut down the other site and is in the process of securing it.

Arkansas State University was notified by the Arkansas Department of Human Services of a data breach in their College of Education and Behavioral Science's Department of Childhood Services database, potentially exposing personally identifiable information.

According to A-State's Chief Information Officer Henry Torres, “we have confirmed unauthorized access to data, but we have no reports regarding illegal use of the information in these files,” Torres said. “We took immediate measures to address this issue after being notified by DHS. We are cooperating with DHS and working with programmers to assess and resolve the situation.”

The breached involved a database related to the "Traveling Arkansas Professional Pathways (TAP) Registry, which is a professional development system designed to track and facilitate training and continuing education for early childhood practitioners in Arkansas."

To date, the university has stated that Social Security numbers were compromised in the database, no other information as to the specific data was provided by the university.

The Montana Department of Public Health and Human Services announced a data breach that occurred when hackers had access to the server for nearly a year. The server contains names, addresses, dates of birth, Social Security numbers and clinical information of customers along with the Social Security numbers and bank account information of employees.

The agency has set up a help line for those who may have been affected at 1-800-809-2956.

The hospital for Veterans Affairs in Denver had two bio-medical computers stolen from a locked room in the hospital. The computers contained data from tests on approximately 239 VA patients. These computers were used to record data from pulmonary function tests for these patients. The hospital has said that no other data was stored on the computers and the data is encrypted on a password protected application.

The Sharper Future, a mental health facility in Los Angeles has informed clients of a data breach when their offices were burglarized and various electronic equipment that stored patient records which includes names, dates of birth, health and clinical histories, treatment records, CDJR identification numbers and Social Security numbers of their clients.

The facility did report that the information on the stolen equipment was password-protected and did not include financial information. The incident is currently under investigation by authorities.
May 28, 2014    **Precision Planting**  
               **Tremont, Illinois**  
               BSO    HACK    Unknown

Precision Planting customers have been impacted by a security breach affecting one of the company’s data servers. The company has not communicated specifically how their system was compromised, however the information breached included customer names, addresses, tax identification numbers and financial information. The server also contained some employee W-2 forms, Social Security numbers, and driver’s license numbers.

**Information Source:**  
[Media](#)  
records from this breach used in our total: 0

May 28, 2014    **Promedica Bay Park Hospital**  
               **Oregon, Ohio**  
               MED    INSD    500

Promedica Bay Park Hospital notified patients of a data breach when an employee of the facility accessed records of patients not directly under their care from April 1, 2013 to April 1, 2014.

The information breached included each patient’s full name, date of birth, diagnosis, attending physicians, and medications. Patients’ Social Security numbers and financial information are not believed to have been accessed.

The employee was immediately fired once the hospital learned of the privacy breach.

**Information Source:**  
[Media](#)  
records from this breach used in our total: 500

May 27, 2014    **Midwest Women’s Healthcare Specialists**  
               **Kansas City, Missouri**  
               MED    PHYS    1,500

Midwest Women’s Healthcare has informed patients of a data breach when records were mistakenly placed in a dumpster during a construction project at their facility. The records in turn were blown out of the dumpster during a strong wind storm in the area.

The records included names, addresses and Social Security numbers for female patients in 2011 and 2012.


**UPDATE** (12/3/2014): A settlement agreement has been reached with over 1,500 women and the Women’s Healthcare Specialists over the mistaken exposure of their personal information when records were accidentally dumped outside the facility in a dumpster, then blown from the dumpster due to high winds in May 2014. Midwest Healthcare Specialists agreed to set up a victims’ fund of $400,000 to compensate those women whose records were exposed as a result of the physical disclosure of documents.


May 26, 2014    **Power Equipment Direct**  
               **Suwanee, Georgia**  
               BSR    HACK    Unknown

Power Equipment Direct has notified customers of a data breach that occurred when a small piece of malicious computer code was uploaded to a server that handles their check-out process. The malicious code captured and transmitted screen shots of check-out pages. The company reported that the breach most likely occurred from May 4, 2014 until May 5, 2014.

The company is not sure as to what information was captured, it would have been the information on the screen available at the time the malicious code was enabled.

The company is offering AllClear SECURE at no cost for 12 months. For those affected they can call 1-877-676-0382.

**Information Source:**  
[Vermont Attorney General](#)  
records from this breach used in our total: 0

May 26, 2014    **AutoNation Toyota of South Austin**  
               **Austin, Texas**  
               BSO    HACK    Unknown

AutoNation Toyota of South Austin informed customers of a data breach that occurred when a third party vendor, TradeMotion, who operates parts websites for auto dealers nationwide, had their systems hacked potentially exposing credit card information that was stored on their system. The hackers may have also gotten names, addresses, telephone numbers, and email addresses.

The company has arranged for those affected to receive one year of identity theft protection through Experian’s ProtectMyID. Those affected can call 1-866-252-9553 by August 31, 2014 for enrollment.

**Information Source:**  
[Vermont Attorney](#)  
records from this breach used in our total: 0

108
Humana has notified Atlanta customers of a data breach that occurred when a Humana associate's vehicle was broken into and an unencrypted USB drive along with the associate's laptop computer were stolen. The information contained on these devices included medical record information and Social Security Numbers.

Humana said that it "has no reason to believe that the information has been used inappropriately." The company is offering free access to a credit-monitoring service for members who were affected.

"Members enrolled in Medicare plans who have any questions about this may contact Humana at 1-800-457-4708, from 9 a.m. to 5 p.m. Members enrolled in non-Medicare plans should call 1-800-448-6262".

Information Source: PHIPrivacy.net

Placemark Investments, Inc. who is a registered investment adviser providing overlay management services for TD Ameritrade's Unified Managed Account Exchange program, notified 11 Maryland residents of a data breach.

Reportedly, malware placed on one of Placemark's servers, accessed and directed the server to send large batches of spam email. Based on analysis done by the company the malware also had the "potential to expose certain PDF documents tied to account creation that were stored on the server for short intervals".

These documents contained information relating to the eleven individual accounts which included names, addresses, dates of birth, and Social Security numbers.

The company is offering one year free of credit monitoring services from Experian.

Information Source: Maryland Attorney General

San Diego State University discovered a database that was set up and managed by the Pre-College Institute, containing names, Social Security numbers, dates of birth, addresses, and other personal information was mis-configured to enable any computer connected to the SDSU wired network with the program "File Maker". The SDSU wired network consists of offices, some labs and the library.

For those with question or concerns about the incident are asked to contact Felecia Vlahos, the Information Security Officer at iso@sdsu.edu or via phone at toll free 1-855-594-0142 and refer to incident #H05007.

Information Source: California Attorney General

Lowes Corporation had to issue a data breach notice to current and former drivers for the company due to a security breach with one of the third party vendors they use.

Information breached included including names, addresses, birthdays, Social Security numbers, driver's license numbers, and other driving record information with a company called E-DriverFile, an online database provided by SafetyFirst, a driver safety firm headquartered in New Jersey.

The third party vendor unintentionally backed up the data to an unsecure server that was accessible via the Internet. The information may have been exposed from July 2014 through April 2014 before it was discovered.

Lowes is offering their current and former employees one year free of AllClearID. Those affected can call 1-877-322-8228

Information Source: Media

Experian has notified Bluegrass Federal Credit Union of unauthorized access of it's consumer information without proper authorization. The information includes names, addresses, Social Security numbers, dates of birth, and account numbers.
For those affected they can contact Bluegrass Community FCU at 606-324-0888606-324-0888 and ask for Jamie Darling.

Information
Source: New Hampshire Attorney General

May 22, 2014  Alabama Department of Public Health
Montgomery, Alabama  GOV  INSD  7,000

The Alabama Department of Public Health notified individuals of a breach when the U.S Attorney's Office for the Middle District of Alabama and the U.S. Department of Justice's Tax Division informed the health department that they were prosecuting individuals in an ID theft ring involving personal information used to file fraudulent tax returns.

"The indictment indicates that the women ran a large-scale ID theft ring between January 2011 and December 2013 during which time they filed more than 7,000 false tax returns that claimed more than $20 million.

Authorities say the woman stole identities from numerous places. Tracy Mitchell, for example, worked at the hospital at Fort Benning, Georgia, where she had access to military personnel data, including that of soldiers deployed to Iraq and Afghanistan.

Authorities also claim that Tracy Mitchell and her co-indicted daughter, Latasha Mitchell, obtained stolen identities from an Alabama state agency, that Keisha Lanier obtained stolen identities from the Alabama Department of Corrections, that Talarious Paige and Patrice Taylor worked in a call center for a Columbus, Georgia company and stole identities and that Paige, in turn, sold those identities and they were used by Tracy Mitchell, Keisha Lanier, and others to file false tax returns".

Information
Source: Media

May 22, 2014  Ebay
San Jose, California  BSO  HACK  145,000,000

Ebay, the online auction site, was hacked between late February and early March with login credentials obtained from employees. The hackers then accessed a database containing user records of approximately 145 million users which they appeared to have copied.

The information included email addresses, encrypted passwords, birth dates, mailing addresses. The company reports that no financial data or PayPal databases were compromised.

The company is encouraging all who were affected to login into their account and change their passwords.

Ebay has provided the following links for additional information:

http://www.ebayinc.com/
http://www.ebayinc.com/in_the_news/story/faq-ebay-password-change

Information
Source: Media

May 22, 2014  Paytime Inc.
Mechanicsburg, Pennsylvania  BSO  HACK  Unknown

Paytime Inc, a payroll service for corporations, notified customers of a data breach to their payroll system. The hackers obtained usernames and passwords to their system and were able to obtain Social Security numbers, direct deposit account information, dates of birth, hire dates, wage information, home and cell phone numbers, other payroll information and home addresses.

The company is providing one year free of AllClearID. Those affected are asked to call 1-855-398-6436.

Information
Source: California Attorney General

May 21, 2014  Hanover Foods Corporation
Hanover, Pennsylvania  BSO  DISC  5,867

Hanover Foods Inc, who is a Paytime client has learned that over 5,800 of it's employees were part of the over 216,000 individuals affected by the Paytime breach. Hanover's representing law firm has also sent a letter to those affected and has reported the incident to those individuals affected.

The information breached included names, Social Security numbers, direct deposit bank account information, dates of birth, hire dates, wage information, home and cell phone numbers, and other payroll information when hackers obtained usernames and passwords associated with the Paytime system.

Information
Source: Maryland Attorney General
Lowe’s, the home improvement store informed current and former drives of Lowe’s vehicles that one of their third party vendors who provide a computer system “E-DriverFile” that stores compliance documentation and information related to these current and former employees, was unintentionally backed up to an unsecure computer server that was accessible from the Internet.

The information that was compromised included names, addresses, dates of birth, Social Security numbers, driver’s license numbers, Sales IDs and other driving record information.

An investigation was launched and it was discovered that the information may have been exposed between July 2013 and April 2014. The company is providing one year free of AllClear ID services to those affected. For questions from those affected ask to call 1-877-263-7997 within the USA, for those outside the United States or Canada, call 1-512-579-2449.

SafetyFirst has come forward to announce a data breach of their E-DriverFile service. The company is connected to the announcement that Lowe’s current and former employees were involved in a data loss.

“ar new filing with the California Attorney General’s Office obtained today indicates that a server containing a wealth of information about client vehicle operators was unprotected and accessible via the Internet for a period that exceeded six months. SafetyFirst reported that the breach dated back to September 27, 2013. It was not discovered until April 2, 2014 according to those records”.

SafetyFirst unintentionally backed up data to an unsecured computer server that was accessible from the Internet. The information breached included Social Security numbers, and driver license numbers.

On March 26, 2014, the California Information Security Office notified the University California Irvine that three of the computers in the Student Health Center had been infected by a keylogging virus, which captured the keystrokes as information was being entered into the computers, then transmitted the data to unauthorized servers. They believe that hackers gained information from February 14th through March 27th 2014. As a result of the virus personal information of individuals was compromised.

The information included names, unencrypted medical information, potentially including health or dental insurance number, CPT codes, ICD9 codes and/or diagnosis, student ID numbers, non-student patient ID numbers, mailing addresses, telephone numbers, amounts paid to the Student Health Center for services, bank names and check numbers.

UC Irvine has contracted with ID Experts to provide one year of FraudStop credit monitoring and one year of CyberScan Internet monitoring for those affected. To enroll visit www.idexpertscorp.com/protect and use the code provided in the letter sent to those affected or call 1-877-810-8083.
Baylor Regional Medical Center at Plano communicated to patients a data breach that occurred when a "phishing" email went out to affiliated physicians. The physicians may have been unaware that it was a "phishing" scam and inadvertently created unauthorized access to their email accounts.

The email accounts may have included emails that contained patient information, including names, addresses, dates of birth, or telephone numbers, some clinical information such as treating physician, department, diagnosis, treatment received, medical record number, medications, medical service code or health insurance information and Social Security numbers.

Information Source: Media

Boulder Community Health is investigating another data breach of their facility. It has been reported this is the third such incident for this facility since 2008.

Nine people have claimed that they had their records stolen and hard copies mailed to them. Two of these individuals said that there was a letter in theirs that stated their records were mailed “to demonstrate the easy access the hospital and their partners provide to some with bad motives.”

There is an ongoing investigation to understand the extent of the breach. "The hospital — previously known as Boulder Community Hospital until a name change last month — is asking anyone else who thinks their records might have been stolen to call its legal office at 303-440-2342." 

UPDATE (5/12/2014): Seven more patients have claimed that an anonymous source has sent them copies of their medical records in the mail. It is still unclear as to whether the source is taking the medical records from inside of the hospital or from somewhere outside of the hospital. The breach is still under investigation.

Information Source: Media

The office of Brent Green, CPA was burglarized on April 6, 2014 where the burglars took a network server computer and hard drives containing personal information of their clients. Their server was unencrypted and contained Social Security numbers, names, and addresses of both individuals and their independents.

For additional information or questions, those affected are asked to call Brent Green at 831-64-5562.

Information Source: California Attorney General

Gingerbread Shed Corporation notified customers of unauthorized access to their system that compromised the personal data of its customers. The information included names, addresses, phone numbers, email addresses, credit card information, user names and passwords for website accounts.

The company has established a confidential phone line for those affected that have questions 1-866-597-8199 and use reference # 5474042814.

Information Source: California Attorney General

The California Department of Child Support Services has notified individuals of a data breach that resulted in unauthorized disclosure of personal information. On April 7, 2014 letters from the Solano County Department of Child Support Services were misplaced while in the custody of a contracted courier who was transporting mail to the US Post Office.

Those affected are asked to call the Department of Child Support Services at 1-866-901-3212.

Information Source: California Attorney General

Molina Healthcare notified individuals that their personal health information was potentially accessed and shared by an unauthorized person during a technical problem with their information technology systems.

Information Source: California Attorney General
Molina Healthcare has communicated to former members about a data breach that included their Social Security numbers.

Molina said it contracted with a printing company to print postcards that contained information about benefits offered. Unfortunately the postcards did not contain names of the individuals, but addresses and Social Security numbers of the individual.

---

Information
Source: Media

May 5, 2014  
ground (ctrl) 
Sacramento, California

ground(ctrl) operates social networking community websites focused on musicians, informed customers of a data breach to their website. The information breached included e-mail addresses and passwords. The company did inform customers that their credit card information was never stored with them and was not at risk.

For those affected, the company is recommending that usernames and passwords be changed. For questions individuals can call 1-877-463-2875 or via email at security@groundctrl.com.

Information
Source: California Attorney General

May 5, 2014  
UMASS Memorial Medical Center (UMMMC) 
Worcester, Massachusetts

UMass Memorial Medical Center informed patients of a data breach that occurred when a former employee stole personal information from the medical centers files.

The information stolen included names, dates of birth, Social Security numbers and addresses. The former employee had access to this information from May 6, 2002 to March 4, 2014. Investigators believe that this individual stole the information in order to open credit card and cell phone accounts.

Update (1/14/2016): Per HHS the total breach number increased to 14,100 individuals vs. the original 2,300 reported. Our numbers have been amended as such.

More information: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=9BF4AF...
AOL has sent a message to millions of its account holders of a data breach to their system urging them to change their usernames and passwords. AOL won’t confirm an exact number but it appears to be approximately 2 percent of its accounts.

AOL noticed the attack when a significant amount of spam began appearing from spoofed emails from AOL account holders email addresses.

Information Source: Media

April 28, 2014

**Seton Northwest Hospital**
**Austin, Texas**

A computer-like device was stolen from Seton Northwest Hospital that is used in the sleep lab. The device according to the hospital, is a Hewlett Packard desktop device that is used to capture and manipulate data from sleep studies. "It does not function like a normal computer. The operator would need a password and access to Seton systems to get a hold of patient data". Reportedly the data consists of names, dates of birth and Seton account numbers.

The device was stored inside a locked storage area at Seton Northwest Hospital, where the device was stolen.

In response Seton Healthcare sent the following statement:

"But to be safe, Seton already has offered, at no cost to patients, ID protection for a year to all the 180 or so patients whose information we believe is on this data storage device. Seton is sincerely sorry that this incident occurred and plans to work closely with the patients involved to protect them from harm."

Information Source: PHIPrivacy.net

April 25, 2014

**Willis North America Inc.**
**Nashville, Tennessee**

Willis North America Inc. informed customers that on "March 19, 2014 an email was sent internally to a group of current Willis Associates who were enrolled in the medical Plan's Healthy Rewards Program". The original email sent out to customers was as a reminder for a special program through their company, however the individual who sent the email "accidentally attached a spreadsheet to the email that was not meant to be included".

The information on the spreadsheet included names, email addresses, dates of birth, social security numbers, employee ID numbers, and office locations by city/state/zip. Wellness credits, an individuals credit status codes, insurance coverage codes, internal codes for plan geographic region and type of reward applicable, last effective date of medical plan elections, election selections, original and last start dates, and when medical plan coverages began.

The spreadsheet did not include any information that revealed health conditions, health treatments or health claims, or personal health information regarding spouses or dependents.

The company has arranged for two years of identity theft protection at no charge. Those affected can find the information at [www.trustedid.com/enhanced-identity-theft-protection](http://www.trustedid.com/enhanced-identity-theft-protection). To register to to [www.trustedid.com/willis](http://www.trustedid.com/willis) and enter the activation code WNAIDE0314 OR CALL 1-888-880-0761.

Information Source: Vermont Attorney General

April 22, 2014

**NCO Financial Systems Inc.**
**Horsham, Pennsylvania**

NCO Financial Systems Inc. informed customers of a data breach when their third party communication vendor, RevSpring, Inc. sent an email to a number of loan customers that mistakenly included an attachment that contained loan statements. The information on these statements included names, addresses, Social Security numbers, and account numbers.

The company is offering 12 months free of ProtectMyID through Experian. A letter with a code went out to those individuals affected. Those with questions are asked to call 1-866-274-4371.

Information Source: California Attorney General

April 22, 2014

**Snelling Staffing LLC**
**Dallas, Texas**

Snelling Staffing LLC informed current and previous employees of a data breach that exposed personal information to others via the Internet due to an installation error of a cloud based server at the home of a former Snelling employee, on January 24, 2014.

The information exposed included Social Security numbers, driver's license numbers, dates of birth, home addresses, medical information, alleged criminal activity and/or drug test results.
The company did discover that breach and shut down access to the information within the same day.

Iowa State University
Ames, Iowa

Iowa State University has reported a data breach of one of their systems that exposed a large amount of data of individuals who were enrolled in the university over the past 17-year period.

Social Security numbers of approximately 30,000 people who enrolled in certain classes between 1995 and 2012 along with university ID numbers for nearly 19,000 additional people. Authorities believe that the person or persons motivation was apparently to generate enough computing power to create the virtual currency bitcoin.

The university is offering AllClear ID for 12 months free for those whose Social Security numbers were affected. AllClear representatives can be reached at 1-877-403-0281.

Here is the link to the universities information regarding the breach http://www.news.iastate.edu/news/2014/04/22/serverbreach

For those who suspect fraud or question whether a request you receive is legitimate, please contact the ISU Foundation at 515-294-4607, the ISU Alumni Association at 515-294-6525, or Iowa State’s computer security team at serverbreach@iastate.edu.

University Pittsburgh Medical Center
Pittsburgh, Pennsylvania

The University Pittsburgh Medical Center (UPMC) informed employees of a data breach that compromised employee's personal data, including their Social Security number and the potential for fraudulent tax returns being filed in their name.

The number of employees affected was approximately 800. The full extent of the information exposed has not been communicated, however, due to the tax fraud, information such as names, addresses and Social Security numbers were assumed to be involved.

UPMC was aware of the breach in February and thought that the breach included only 27 individuals, but soon became aware that the breach was much larger. An investigation is currently being conducted.

UPDATE (4/21/2014): The extent of the data breach at UPMC thought to be around 800 employees, is much more extensive than originally believed. The current numbers are around 27,000 employees affected. UPMC is offering Lifelock for 12 months for those affected. A letter went out to those individuals with the information. For additional questions, UPMC has provided a toll free hotline (1-855-306-8274) or email JohnHouston@upmc.edu. A class action lawsuit has been filed against UPMC.

UPDATE (5/14/2014): On Friday May 9, 2014 the law firm of Kraemer, Manes & Associates sued University Pittsburgh Medical Center (UPMC) and Ultimate Software Group of Weston, Fla., over the loss of employee data and subsequent identity thefts. They are seeking class-action status in U.S. District Court, and would represent current and former UPMC employees who have been affected by the breach.

Aaron Brothers
Coppell, Texas

Aaron Brothers, a division of Michaels Stores Inc. appears to been a part of the data breach of Michaels Stores Inc. The company confirmed on Thursday April 17, 2014 that the payment system breach also affected its Aaron Brothers chain. Approximately 400,000 cards were potentially breached from June 26, 2013 through February 27, 2014.

Wilshire Mutual Funds
Kansas City, Missouri

Wilshire Mutual Funds informed customers of a data breach that took place on March 13, 2014. It was brought to the company's attention that a copy of individuals 1099-Div tax form was sent by fax to an incorrect shareholders in error.

The information contained on the 1099-Div form included registered owner's names, the registration of the mutual fund account, the addresses of record, the last 4 digits of the Social Security numbers, the fund and account numbers assigned in their recordkeeping system, the taxable amounts, and the Payer's (Wilshire Equity Fund) Federal ID number.

Those affected with questions are asked to call 1-866-591-1568 or to send written correspondence to P.O. Box 219512, Kansas City, MO 64121-9512 or by overnight mail to 430 W. 7th Street, Kansas City, MO 64105.
The office of The Veterans Of Foreign Wars Of The United States notified members that an unauthorized party accessed VFW’s webserver through the use of a trojan and malicious code. The hacker, thought to be in China, was able to download tables containing the names, addresses, Social Security numbers of approximately 55,000 VFW members.

The motivation of the hacker, according to IT experts, was to gain access to information regarding military plans or contracts and not for purposes of identity theft, although they have not ruled that out.

VFW is providing 12 months free of AllClearID. Members can call 1-855-398-6437 with any questions. A security code must be provided and was provided in the letter sent to those affected.

LaCie USA was informed by the FBI that they had found indications that an unauthorized person used malware to gain access to information from customer transactions that were made through LaCie’s website. Reportedly, the transactions that may have been affected happened from March 27, 2013 through March 10, 2014.

The information breached included names, addresses, payment card numbers and card expiration dates. Also included could be an individuals LaCie username and password to access the website.

For those affected they are asked to call Monday through Friday from 9:00 a.m through 7:00 p.m EDT (eastern time).

University Urology P.C of Knoxville Tennessee informed patients of a data breach regarding their personal information. According to the practice, the information was limited to names and addresses and that no Social Security numbers, financial account information or clinical information was exposed.

According to a statement by the facility, an administrative assistant had compiled the data in an effort to sell it to a competing provider, helping them gain patient business. Patients contacted University Urology to let them know that the competing provider had been soliciting their business.

Clinical Reference Laboratory, Inc. notified individuals of a breach regarding their personal information. On or around February 6, 2014 Clinical Reference Laboratory (CRL) sent a packet of invoices via the United States Postal Service to Nationwide Insurance for services performed. The package was damaged when it arrived at the USPS facility and some of the invoice pages were missing.

The information in these missing pages included names, dates of birth, the last 4 digits of individuals Social Security number and the type of lab tests conducted.

The company has arranged a free one year subscription through Equifax Personal Solutions.

For those affected with questions they can call CRL at 1-855-758-7543 or disclosurehelp@crlcorp.com.

The San Francisco based Internet company has informed customers of a potential breach that may have occurred in their system. The company sent notification out to customers noticing suspicious activity on their account and in turn locked their accounts and reset their passwords.

The company reported that the breach included only passwords.
American Express Company informed customers that their credit card information was recovered as part of an investigation by law enforcement agencies and/or American Express. The information reportedly only included the American Express Card account numbers, no Social Security numbers were impacted.

Those individuals who notice suspicious activity on their account are asked to call 1-855-693-2213 to notify the company.

Software developer Deltek Inc. informed approximately 80,000 employees of a breach that occurred in Deltek’s GovWin IQ system.

The company confirmed that on March 13, 2014 they suffered a cyberattack where hackers obtained usernames, passwords and credit card information for individuals who use the GovWin IQ system. Of the 80,000 individuals affected, 25,000 of them may have had credit card information breached.

Those individuals who did have credit card information affected, the company is offering a membership to TransUnion Monitoring services for free.

It has also been reported that authorities have already made an arrest in this case.

Deltek has set up an email address for users to submit questions: protect@deltek.com.

The recruiting site BigMoneyJobs.com has apparently been breached by a hacker that goes by the name of ProbablyOnion by exploiting an SQL Injection vulnerability. The details of over 36,000 users have been leaked online due to the breach.

The information included names, home addresses, phone numbers, emails and passwords of 36,802 users have been published in an Excel file. The information covers both individuals looking for a job and companies looking for talent.

Cole Taylor Mortgage (a division of Cole Taylor Bank) informed customers of a data breach that occurred due to an error by one of their third party vendors. Information was inadvertently made accessible to employees of another federally regulated bank.

The information included names, addresses, Social Security numbers, loan numbers and certain loan information. According to the mortgage company, the breach was caused by a technical error by the vendor that provides them information technology services and solutions to both banks.

The company has established a dedicated toll-free hotline for those who were affected at 1-800-572-9809.

Central City Concern, a non-profit in Portland Oregon, notified individuals of a data breach that was perpetrated by an ex-employee of the agency. Federal law enforcement officers notified the non-profit that this former employee copied files from approximately 15 clients from its Access Center with the intention of filing fraudulent tax returns.

CCC began an investigation and has noted that this former employee may have accessed files from March 23, 2010 through May 24, 2013. The former employee stated to authorities that they had only copied 15 files. The non-profit has set up 12 months free monitoring through Experian’s ProtectMyID alert. Any questions for the agency, those affected are asked to call 1-866-778-1144 Monday through Friday 6:00 a.m to 6:00 p.m.
Kaiser Permanente Northern California Division of Research
Oakland, California

April 2, 2014

Kaiser Permanente’s Northern California Division of Research informed research patients of a data breach to their system. The company discovered that a server was infected by a malicious software that caused a breakdown in the server’s security barriers allowing the hackers to obtain personal information.

The information included first names, last names, dates of birth, ages, genders, addresses, race/ethnicities, medical record numbers, lab results all associated with research provided by individuals as part of research studies.

Currently the company has stated that no Social Security numbers or their Kaiser electronic medical record information used for ongoing medical care was not affected.

Those affected with questions are asked to call 1-877-811-0019 from 8 a.m to 6 p.m PDT Monday through Friday or the Department of Health and Human Services through the Office for Civil Rights at 1-800-368-1019.

Boxee
Ridgefield Park, New Jersey

April 2, 2014

The personal data of over 158,000 Boxee.tv forum accounts were hacked and leaked online to a Tor Internet site and at least one researcher. The information included email addresses, birth dates, IP addresses, message histories, and password changes. It also included message archives and past password changes.

The company was purchased by Samsung last July.

California Correctional Institution
Tehachapi, California

April 2, 2014

On March 9, 2014 an employee roster was discovered within an unsecure desk drawer at one of the correctional facilities.

The roster included full names and the last 6 digits of Social Security numbers.

For those affected they are being directed to call Tim Fites, Information Security Coordinator at 1-661-823-5011.

Palomar Health
Escondido, California

March 28, 2014

Palomar Health in Escondido had a laptop stolen along with two flash drives from an employee’s SUV. Approximately 5,000 patients were affected by the breach.

The flash drives contained patient names, dates of birth, information regarding individual diagnosis, individual treatment and insurance information. The computer was encrypted but the flash drives were not. The information dates back to 2008.

The Oceanside police have recovered the laptop and the missing flash drives, one person was arrested and a possible second suspect arrest may follow.

Those patients who may have been affected can reach the health care system for more information at 1-866-313-7993. The company is offering credit monitoring services for those individuals whose medicare numbers were compromised.

Palomar could face a fine as high as $250,000 from the California Department of Health.

Orlando Health’s Arnold Palmer Medical Center
Orlando, Florida

March 27, 2014

A computer flash drive containing patient information on 586 children treated at Orlando Health’s Arnold Palmer Medical Center is missing or reportedly been "misplaced". The information included last names, assigned medical record numbers, dates of birth, gestational ages, birth weights,
dates of hospitalizations, and in some cases, transfer dates of children who were patients at Arnold Palmer Hospital for Children or Winnie Palmer Hospital for Women and Babies between 2009 and 2013.

Information Source: Media

March 27, 2014 The University of Wisconsin-Parkside
Kenosha, Wisconsin

Students were notified by officials from The University of Wisconsin-Parkside of a data breach that occurred to their system by hackers that installed malware on one university server.

The information that is at risk includes names, addresses, telephone numbers, email addresses and Social Security numbers. The breach affects students who were either admitted or enrolled at the university since the fall of 2010.

The server was shut down and the hacking was reported to local authorities. After launching an investigation it appears the malware was searching for credit card information and they show no evidence that any Social Security numbers were compromised.

The university has set up a website with information for those who may have been affected http://www.uwp.edu/explore/contactus/index.cfm

Information Source: Media

March 27, 2014 Sorenson Communications and CaptionCall
Salt Lake City, Utah

On March 7 it was discovered that there was an unauthorized access to Sorenson Communications employee data via the payroll vendor utilized for both Sorenson Communications and CaptionCall employees. The personal information breached includes both the employee, beneficiaries, dependents, and emergency contacts, or anyone listed in the employees HR account with the company.

The information includes names, dates of birth, addresses, Sorenson income histories, Social Security Numbers, W-2 information, and emergency contact data and appeared to have happened between February 20, 2014 through March 3, 2014.

The FBI has been contacted and is investigating the breach. An email was sent to all those affected on March 11th with instructions on how to enroll in the company-provided credit monitoring services. If an email was not received they are requesting those individuals contact the Human Resources Department at hrsupport@sorenson.com to obtain the information.

Information Source: California Attorney General

March 25, 2014 University of Kentucky HealthCare/Talyst
Lexington, Kentucky

UK Healthcare is notifying 1,079 patients that a laptop with their personal health information was stolen on February 4, 2014 from Talyst, a third party pharmacy billing management company.

The vendor’s laptop included names, dates of birth, medical record numbers, diagnosis, medications, laboratory results, progress notes, allergies, height and weights, dates of service, physician name and clinics, insurance carrier, insurance identification numbers.

Information Source: Media

March 25, 2014 American Express
New York, New York

American Express sent out notification to cardholders regarding unauthorized activity on their cards from unnamed merchants. American Express has stated that names, card account numbers and expiration dates of cards could have been affected. At this time they have stated that no Social Security numbers have been affected.

American Express has placed a fraud alert on their cardholders credit reports. For those affected they are to call 1-800-297-7672 for identity theft assistance or email www.americanexpress.com/idtheftassistance.

Information Source: California Attorney General

March 22, 2014 California DMV
Sacramento, California

The California DMV is investigating a potential data breach of their credit card processing systems. Reportedly several
large financial institutions received private alerts this week from MasterCard about compromised cards used for charges.

As reported by Krebs on Security, "the alert, sent privately by MasterCard to financial institutions this week, did not name the breached entity but said the organization in question experienced a "card-not-present" breach-industry speak for transactin conducted online. The alert further stated that the date range of the potentially compromised transactions extended from August 2, 2013 to January 31, 2014, and that the data stolen included the card number, expiration date, and three-digit security code printed on the back of cards".

Krebs contacted 5 different financial institutions, two mid-sized California banks and "confirmed receipt of the MasterCard notice, and said that all of the cards MasterCard alerted them about as compromised had been used for charges being the notation "STATE OF CALIF DMV INT."

The DMV, who originally stated they would investigate, put out a statement at 6:44 Eastern Time on March 22, 2014, placing blame on the the third party credit card processing company.

The total amount of individuals potentially affected at this time is unknown. KrebsOnSecurity stated that they had received a list of more than 1,000 cards, from one bank, that were potentially exposed that included credit card numbers, expiration dates and three-digit security codes printed on the back.

<table>
<thead>
<tr>
<th>Information Source</th>
<th>records from this breach used in our total: 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 21, 2014 Castle Creek Properties, Inc./Rosenthal Wine Shop Malibu , California</td>
<td>BSR HACK Unknown</td>
</tr>
<tr>
<td>March 21, 2014 San Francisco Department of Public Health/Sutherland Healthcare Solutions San Francisco, California</td>
<td>MED STAT Unknown</td>
</tr>
<tr>
<td>March 20, 2014 Marian Regional Medical Center Santa Maria, California</td>
<td>MED DISC Unknown</td>
</tr>
<tr>
<td>March 20, 2014 Auburn University Auburn, Alabama</td>
<td>EDU HACK Unknown</td>
</tr>
</tbody>
</table>

Information Source:
Krebs On Security
March 21, 2014 Castle Creek Properties, Inc./Rosenthal Wine Shop Malibu, California

Castle Creek Properties Inc/ Rosenthal Malibu Estate notified customers of unauthorized access to computer systems used to process credit card transactions at their Rosenthal wine shop.

The unauthorized access may have compromised payment card data of visitors who used their cards for payment of items at the wine shop tasting room. Information compromised included names, addresses, payment card account numbers, card expiration dates and security codes.

The company is offering a complimentary one year membership of Experian ProtectMyID Alert. For those affected and wish to enroll in the services they are asked to call 1-310-899-8903.

Information Source:
California Attorney General
March 21, 2014 San Francisco Department of Public Health/Sutherland Healthcare Solutions San Francisco, California

San Francisco Health Network/San Francisco Department of Public Health has notified patients that their information may have been compromised as well, due to the recent theft of computers at Sutherland Healthcare Solutions. Sutherland is the third party billing company for the San Francisco Department of Public Health.

The information contained in the stolen computers included names, dates of birth, Social Security numbers, dates and location of services and names of insurance companies or payers.

The agency is providing one year of ID Experts. Anyone who was affected is encouraged to contact ID Experts with any questions and to enroll in the service by calling 1-866-486-4809 or by going to their website www.myidcare.com/idexpertshcareprotection. Documentation was sent to the affected parties that provided steps for enrollment and an access code for entry. Deadline to enroll is July 31, 2014

Information Source:
California Attorney General
March 20, 2014 Marian Regional Medical Center Santa Maria, California

Marian Regional Medical Centers (Santa Maria and Arroyo Grande Campuses) notified patients of a data breach. A secured electronic file containing patients information was sent to a contracted health insurance plan in error. The health insurance plan notified the company immediately that they received the email in error.

The file included names, addresses, types of insurance, dates of birth, dates of service, types of laboratory tests and test results for dates of service between March 1 and March 6, 2014. The company has stated that the Social Security number was not included in the electronic file.

For those affected the company has asked questions or concerns to be directed to a toll free number 1-877-906-1603, 1-877-906-1603.

Information Source:
California Attorney General
March 20, 2014 Auburn University Auburn, Alabama

Auburn University notified individuals of a compromised server within the College of Business network. This incident
could have resulted in unauthorized access to personal information including Social Security numbers and names. The investigation is ongoing and the University has reportedly patched the vulnerability in their system.

They have no evidence as of yet if any information was accessed or misused in any way. The University is offering a one year complimentary membership of Experian's ProtectMyID Alert. For questions or concerns, affected parties should call 1-877-371-7902.

Information
Source: Vermont Attorney General
March 18, 2014 Hickory Grove Gas Station
Vincent, Ohio

A local area gas station in Vincent Ohio off of Ohio 339 has a credit card breach and those affected are customers who recently used either debit or credit cards at the gas station. So far 100 people have reported fraudulent charges on their account that dates back to at least a month ago. Reports are saying that the number could go as high as 300 victims.

It appears hackers infiltrated the network that gas station and grocery store uses. The breach could have also potentially happened through the Kentucky-based credit card processing company they use. They have stopped accepting any credit or debit cards until a full investigation is completed.

Those who think they have been victimized are asked to call the Vincent Ohio Sheriffs Department.

Information
Source: Media
March 18, 2014 Yellowstone Boys and Girls Ranch (YBGR)
Billings, Montana

The Yellowstone Boys and Girls Ranch which treats mental health issues for children and teens reported that a binder was lost or destroyed sometime in 2013. The binder contained information that included names, addresses, dates of birth, parents’ names, programs and treatment professionals’ information. They have stated that no financial or Social Security information was stored in this binder.

Information
Source: Health IT Security
March 18, 2014 The Shelburne Country Store
Shelburne, Vermont

The Shelburne Country Store notified customers of a computer hack to their payment processing system, similar to reported attacks by other national retailers such as Target and Neiman Marcus.

The information compromised included names, addresses, credit or debit card numbers, expiration dates and verification codes. They believe the breach occurred between November 13, 2013 and January 6, 2014. They are unclear as to how many purchases were affected.

The company has set up AllClear ID protect your identity for 12 months at no cost to those affected. They can either email support@allclearid.com or call 1-855-434-8077.

Information
Source: Vermont Attorney General
March 18, 2014 IRS
, Pennsylvania

A former employee of the IRS took home a computer thumb drive that contained personal information on 20,000 current and former employees and contractors. The information included Social Security numbers, names and addresses. The thumb drive was plugged into the employees unsecured network, which could have left the information vulnerable.

This incidence dates back to 2007 before the IRS started using automatic encryption. The IRS will not comment why they did not discover this breach until now, or if the employee who used the thumb drive is still working at the IRS.

Information
Source: Media
March 17, 2014 Service Coordination Inc.
Frederick, Maryland

Hackers infiltrated the computers of a state-licensed provider of services to developmentally disabled individuals. The information stolen included Social Security numbers and medical information for approximately 9,700 clients.

The non-profit learned of breach in late October 2013. The U.S Justice Department asked the non-profit organization to
delay notification of the breach to allow for a federal investigation.

The investigation did lead to the alleged hacker and their equipment and accounts have been seized.

“Service Coordination is one of five private organizations licensed by the state’s Developmental Disabilities Administration, an agency of the Maryland Department of Health and Mental Hygiene.”

Information
Source: Media
records from this breach used in our total: 9,700

March 17, 2014 Arcadia Home Care and Staffing Southfield, Michigan

Arcadia Home Care/Arcadia Health Services, Inc. notified employess of unauthorized access of their files by an independent contractor for Arcadia by the name of Charles E. Symes, II and his new business Alegre. Mr. Symes was previously authorized to use Arcadia’s database, which contained personal information, but only for authorized purposes and access.

The company discovered Mr. Symes gaining unauthorized access to employee’s personal information which included names, Social Security numbers, addresses, bank account information, California driver’s license and other information.

The company believes the information was breached on or around January 2014 through March 1, 2014. For questions the company is asking those affected to call 1-800-733-8427.

Information
Source: California Attorney General
records from this breach used in our total: 0

March 17, 2014 ELightBulbs.com Maple Grove, Minnesota

Elightbulbs.com is in a series of companies who have had security breaches due to exposure of ColdFusion weaknesses. The online company was contacted by Discover card alerting them to a pattern of fraudulent activity on cards that were recently used at their store. This is a similar incident to what happened with Smucker’s. ELightbulbs.com was listed in the ColdFusion botnet panel.

The Vice President of the company, Paul McLellan said “he first learned of the breach on November 7, 2013 from his company’s processor, Heartland Payment Systems”. He also stated that “shortly before we were told by Heartland, we paid $6,000 a year for a company to brutalize our server, for protection and peace of mind. Turns out this flaw had existed for two years and they never saw it.”

The FBI has stated that group responsible for the attack have also compromised much higher-profile targets as well.

Information
Source: Media
records from this breach used in our total: 0

March 17, 2014 Kichlerlightinglights.com New York, New York

KichlerLightingLights is another victim of the ColdFusion botnet. The company’s owner Gary Fitterman stated “It was like being attacked by terrorists. When we learned what had happened, we immediately went into frenzy, spent a ton of money to get forensic experts to take a look.”

The hacking gang used vulnerabilities in Adobe’s ColdFusion to build a botnet of hacked ecommerce sites, designed to bilk the customers credit card data. KichlerLightingLights was just another one of the ecommerce sites affected.

The various companies that have been affected all handled credit card processing on their site. Mr. Fitterman has now outsourced all of his credit card processing transactions to a third party company.

Experts state that if you run your own credit card processing you must be diligent about software updates.

Information
Source: Media
records from this breach used in our total: 0

March 17, 2014 Maryland Department of Health and Mental Hygiene Baltimore, Maryland

“The Department of Health and Mental Hygiene says hackers hit Service Coordination Incorporated of Frederick, which provides case management services to nearly 14,000 Maryland residents.

SCI, in a letter provided to WBAL News, indicates that its computers were hacked between October 20th and October 30th and that access was gained to confidential information.

That potentially includes names, social security numbers, medical assistance numbers, and other vital information, some shared with the Maryland Developmental Disabilities Administration”.

Information
Source: PHI Privacy.net
records from this breach used in our total: 14,000
March 14, 2014  Health Source of Ohio  Milford, Ohio

Health Source of Ohio reported a breach of patients' personal information when a file containing specific data was accidentally made visible online. According to authorities the file was viewed 47 times.

The file included names, account numbers, addresses, phone numbers, Social Security numbers, birthdates, credit card numbers and limited healthcare information. According to the center not all patients information included financial or Social Security numbers. A specific number was not provided of the 8,800, who may have suffered a breach of their financial information or SSN.

Patients who were affected are advised to contact HSO at 1-800-495-7647

Information
Source: Media
records from this breach used in our total: 8,800

March 13, 2014  Silversage Advisors  Irvine, California

On February 20, 2014 Silversage Advisors notified customers of a theft of back-up computer drives from a secure offsite location used as part of the company's disaster recovery plan. The drives contained names, addresses, Social Security numbers, driver's license numbers and account information.

The company is providing one year of Breach Protector credit monitoring and identity theft restoration coverage. For those affected with question they are to call 1-888-969-7500.

Information
Source: California Attorney General
records from this breach used in our total: 0

March 13, 2014  Detroit Medical Center-Harper University Hospital  Detroit, Michigan

A former Detroit Medical Center-Harper University Hospital employee was found with the personal information of 1,087 patients by West Bloomfield police. The documents included patients health information, names, dates of birth, reasons for patient visits and Social Security numbers.

When the hospital learned of the breach they immediately revoked the employee's access to its computer systems and all of the Detroit Medical Center hospitals.

For patients that were affected they can call 1-855-830-9731 with questions.

Information
Source: Media
records from this breach used in our total: 1,087

March 12, 2014  UCSF Family Medicine Center at Lakeshore  San Francisco, California

UCSF Family Medicine Center at Lakeshore notified patients of a theft of desktop computers that were unencrypted on or around January 11, 2014. An immediate analysis of what information the computers obtained. On March 6, 2014 UCSF determined that some of the computers stolen contained Social Security numbers, names, dates of birth and medical record numbers, some only contained names, medical record numbers and health information.

Those who were affected were asked to contact UCSF/ID Experts by calling 1-888-236-0299 1-888-236-0299 Monday through Friday from 6 a.m. to 6 p.m. Pacific time. When calling individuals are asked to used Access Code: 59832

UPDATE (3/20.2014): The University of California at San Francisco is notifying 9,986 individuals who had information on the computers that were stolen from the UCSF Family Medicine Center at Lakeshore. The computers included information such as names, dates of birth, mailing addresses, medical record numbers, health insurance ID numbers and driver's license numbers. Of the 9,986 files, 125 of them also included Social Security Numbers. Credit monitoring is being offered to those whose Social Security numbers were affected.

Information
Source: California Attorney General
records from this breach used in our total: 125

March 12, 2014  NoMoreRack.com  New York, New York

As reported by Krebs On Security, for the second time since August 2013, the “online retailer NoMoreRack.com has hired a computer forensics team after being notified by Discover about a potential breach of customer card data.”
The Director of Business Development with company, Vishal Agarwal, has confirmed that they were approached by Discover Card in August of 2013, communicating that they were seeing fraudulent activity and the online retailer was the point of compromise.

As stated by Mr. Agarwal “they requested then that we go through a forensics audit, and we did that late October by engaging with Trustwave. Trustwave came out with a report at end of October saying there was no clear cut evidence that our systems had been compromised. There were a few minor bugs reported, but not conclusive evidence of anything that caused a leakage in our systems.”

Discover reached out the company again in February to notify them that there was additional evidence of fraud associated with their online store from November 1, 2013 through January 15, 2014.

The company has again engaged Trustwave to complete another forensic audit and to also confirm that they are PCI compliant.

Information Source: Media

March 11, 2014  City of Hope
Duarte, California

The City of Hope was informed by one of their vendors, Sutherland Healthcare Solutions, Inc. regarding a burglary that happened in one of their offices, where the thieves stole eight of their computers. Two of the computers contained City of Hope patient and patient guarantor information. Both computers were password protected. Sutherland Healthcare Solutions provides billing services for the City of Hope, who has since suspended their relationship with Sutherland.

The information on the computers contained Social Security numbers, names, addresses, phone numbers, medical record numbers, account numbers and/or diagnoses. Law enforcement is currently investigating the incident.

The City of Hope has secured the services of Kroll, a risk mitigation company, to provide identity theft protection at no cost for one year for those who may have been affected.

Information Source: California Attorney General

March 11, 2014  Cornerstone Health Care
High Point, North Carolina

Cornerstone Health Care reported a laptop containing information for 548 patients was stolen from Cornerstone Neurology sometime between December 31, 2013 and January 6, 2014.

The laptop contained protected health information such as patient names, dates of birth, physician names and nerve conduction scan summaries. The laptop did not contain any addresses, billing information, or Social Security numbers. The laptop was not connected to their third party billing company or their electronic health records.

Since the theft the medical practice has revised its procedures and policies, retrained the staff on securing patient information and replaced locks on rooms with electronic medical devices.

Information Source: Media

March 11, 2014  Emory Dialysis Center, part of Emory Clinic
Atlanta, Georgia

An employee of Emory Dialysis Center, notified the center that his work laptop had been stolen out of his car on February 7, 2014.

The laptop was protected by a password but was not encrypted. The laptop contained information for 826 patients which included dates of services, blood flow test graphs, first and last names for approximately half of the patients, the rest were the patients initials. The center has stated that the laptop did not contain dates of birth, addresses, billing information or Social Security numbers.

HSM (Health Systems Management) who runs the clinic is now password protecting all laptops and encrypting patient information.

Information Source: Media

March 10, 2014  Statista
New York, New York

Online statistics portal, Statista, notified customers of a data breach that occurred with their system. The breach was noticed when the company internally started receiving spam emails. The company investigated and approximately 50,000 of its customers username and password combination were compromised.

The company has not said whether or not the breach goes beyond access to username and passwords, but at present, this seems to be all that has been affected.
The company notified users almost immediately and assured them that the compromised passwords "cannot be used by third parties due to masking procedures". The company did not encourage customers to change their passwords.

Experts are questioning how secure the passwords are for those that created accounts prior to December 2013 and have stated that "the passwords of those who signed up before this data were stored in the Statista database as MD5 hashes. As many experts will tell you, MD5 passwords can be easily cracked".

The main risk for those affected would be a higher incidence of spam and phishing emails, potentially impersonating Statista.

Information Source: Media

March 7, 2014  John Hopkins University  Baltimore, Maryland

University officials at John Hopkins University announced a data breach of their Department of Biomedical Engineering’s Design Team course web server. A hacker claiming to be part of the group Anonymous claimed credit for the hack.

The hackers made an attempt to extort the university out of server passwords, but the university did not comply with the request.

Officials at the university said that the server did not contain Social Security numbers, birth dates, credit card numbers or any financial data. The data the server did contain included employee data that is publicly available from the department’s website. Those affected include any students from the BME department who were enrolled in the course from 2006 to this past fall. Approximately 1,307 individuals may have been affected.

There was a coding error that left the database vulnerable to attacks and but not prior to the hackers infiltrating the system. The server was primarily used to produce the BME department’s website. Although the breach happened late last year, it was not realized until someone posted on Twitter in January that the server was open to attack.

Information Source: Media

March 6, 2014  North Dakota University  Bismarck, North Dakota

North Dakota University System has notified individuals of a security breach of a computer server that stores personal information on students, staff and faculty.

On February 7, 2014 the server was hacked into and more than 209,000 current and former students and 780 faculty and staff had personal information stored on the server that included names and Social Security numbers according to Larry Skogen, the Interim Chancellor.

The university has notified officials and has set up a website www.ndus.edu/data with information and is organizing a call center for questions from those who were affected.

Authorities have announced that "an entity operating outside the United States apparently used the server as a launching pad to attack other computers, possibly accessing outside accounts to send phishing emails”.

Information Source: Media

March 6, 2014  Los Angeles County Department of Health/Sutherland Healthcare Solutions  Los Angeles, California

On February 5, 2014 Sutherland Healthcare Solutions, which provides patient billing and collection services for Los Angeles County was broken into and computers were stolen. Information that was stored on these computers included first and last names, Social Security numbers, billing information, dates of birth, addresses, diagnoses and other medical information.

Currently the breach is being investigated by authorities and the agency is offering credit monitoring services through ID Experts free for 12 months. To enroll in the free services by calling 1-877-868-9284 or going to www.myidcare.com/securityandprotection.

UPDATE (3/7/2014): The Los Angeles County Department of Health and Human Services (DHS) announced recently that they will be notifying 168,000 patients of a data breach at Sutherland Healthcare Solutions. When originally reported the number of patients was not divulged.

UPDATE (5.27.2014): The Los Angeles County Department of Supervisors voted on Tuesday to tighten and add current requirements for county computers and hard drives. Currently, all laptops are required to be encrypted and the vote on Tuesday now extends that requirement to all county departments’ computer workstation hard drives as well. They also voted to have "all County-contracted agencies that exchange personally identifiable information and protected health information data with the County” be encrypted as a requirement for any contract.
As reported by Krebs on Security, it appears that Sally Beauty Supply may be one of the latest victims of a string of credit card data breaches affecting their payment systems.

"On March 2, a fresh batch of 282,000 stolen credit and debit cards went on sale in a popular underground crime store. Three different banks contacted by KrebsOnSecurity made targeted purchases from this store, buying back cards they had previously issued to customers".

The banks used a "common point of purchase" or "CPP" to determine where the cards were used over the same period of time. "Each bank independently reported that all of the cards (15 in total) had been used within the last ten days at Sally Beauty Supply locations across the United States".

The company had also detected some kind of intrusion into their network at or around the same time that the stolen card mapping or "CPP" dates that the banks found associated with Sally Beauty Supply. The company's initial investigation did not show any evidence that data was compromised at the store level. The company hired Verizon Enterprise Solutions for the initial and continued investigation.

UPDATE (3-17-2014): Sally Beauty has confirmed that the breach they suffered was due to hackers breaking into their network, stealing credit card data from stores. Originally the retailer would not confirm that they suffered a breach as they had no evidence that any credit card data was stolen. The company confirmed that "fewer than 25,000 records containing card present (track 2) payment card data have been illegally accessed on our systems and we believe have been removed." The company also states "As experience has shown in prior data security incidents at other companies, it is difficult to ascertain with certainty the scope of a data security breach/incident prior to the completion of a comprehensive forensic investigation. As a result, we will not speculate as to the scope or nature of the data security breach."

Information Source: Media

OANDA informed customers of an unauthorized breach affecting some of their clients. On Monday March 3, 2014 a historical log of some payments received via PayPal (prior to 2007) was accessed. The company states that the incident did not impact any fxTrade services, client trades or funds.

The information accessed included named and email addresses. The company states that usernames or passwords for their "fxPence" expense reporting tool may have been accessed. These accounts are not related to fxTrade. They are asking customers who registered for this service and use the same username and password on any other external websites, to change those passwords.

Upon learning of the breach, the company shut down access to the system and alerted the FBI, their regulators and relevant privacy offices of the breach.

For additional questions or concerns those who may have been affected can call their respective local office http://www.oanda.com/corp/contact/ or via frontdesk@oanda.com.

Information Source: California Attorney General

On Wednesday March 5, 2014 Point Park University in Pittsburgh Pennsylvania notified employees of a possible data breach that included names, home addresses, Social Security numbers, wage information, birthdates, bank accounts and routing numbers.

The Point Park President stated that as many as 1,800 employees could have been affected by this breach.

"The university was expecting a package from its payroll processing vendor Ceridian, but when the package arrived to campus it was missing all of the accompanying reports, according to an internal email obtained by the Pittsburgh Post-Gazette."

The university is working with authorities and an investigation has been launched. The law firm that represents the university is currently putting a letter together to those who were affected that will include call-center information and other services offered.

Information Source: Media

Smucker's announced a data breach to their Online Store, stealing customer data that could have included customer names, addresses, email addresses, phone numbers, credit card or debit card numbers, expiration dates, and verification numbers.

Information Source: Media

March 4, 2014 Smucker's Orrville, Ohio BSR HACK Unknown

Smucker's announced a data breach to their Online Store, stealing customer data that could have included customer names, addresses, email addresses, phone numbers, credit card or debit card numbers, expiration dates, and verification numbers.
The hackers utilized a sophisticated malware that steals information from Web server applications. This particular malware obtains form data submitted by visitors as customers entered the data for the online checkout process. These particular hackers look for weaknesses in either the end-users computer or weakenss in the Web server. If there is a weakness in either one, that web session then becomes compromised and the hackers “suck down customer data post or pre-encryption (this all depends on whether the data was incoming or outgoing)”. KrebsOnSecurity noted “when a reader first directed my attention to the Smucker’s breach notice, I immediately recalled seeing the company’s name among a list of targets picked last year by a criminal hacking group that plundered sites running outdated, vulnerable versions of ColdFusion, a Web application platform made by Adobe Systems Inc”.

Eureka Internal Medicine has notified patients of a potential security breach. It was discovered from September 25, 2013 until around October 9, 2013 that their janitorial service was mixing paper recycling containing patient information with the regular trash vs. moving it to the locked shredding bin. As a result, the paper containing patient information ended up in the regular trash which was picked up and disposed of by the waste management company vs. being secured in the locked bin for pick up for secure shredding.

Information that may have been in the regular trash bins could have included full names of patients, Social Security numbers, insurance plan information and medical information.

Anyone who is potentially affected by the breach and has questions may call the representing attorney’s office at 1-888-233-2305.

Assisted Living Concepts LLC has notified current and former employees of a potential data breach regarding their payroll records and an unauthorized third party access of this data.

Assisted Living Concepts utilizes an external vendor that provides them with payroll services. On February 14, 2014, the payroll vendor notified the facility of evidence of unauthorized third party access to their payroll information. The company launched an investigation and discovered evidence of this unauthorized access that obtained access to their vendor user credentials and access to the vendor’s systems, which contained payroll files for current and former employees.

The FBI and IRS have advised the company that they believe the personal information accessed may be used by criminals to file fraudulent tax returns. The IRS is encouraging anyone who might have been affected by this unauthorized access file their tax return as soon as possible. Those affected can also call the IRS Identity Protection Specialized Unit at 1-800-908-4490 with any questions.

Capital One has sent notification to customers regarding a possible breach to their personal information. They discovered that a former employee of the company may have improperly accessed customer accounts, which could have been linked to unauthorized transactions.

The information accessed included names, account numbers, Social Security numbers, payment information and other account information. The credit card company has notified law enforcement of the breach.

The company is also offering one year of Equifax’s Credit Watch Gold with 3-in-1 Monitoring by February 28, 2014 for those that may have been affected.
In an unprecedented move, First American Bank made a public announcement regarding fraudulent activity they were seeing on both credit and debit cards of customers with their bank specifically related to cab rides in the city of Chicago.

The bank is urging both residents and tourists to avoid paying for their cab rides with either debit or credit cards. The ongoing breach appears to be related to the card processing systems used by a significant amount of taxis in the city of Chicago.

The bank has reported the breach to MasterCard. They have also reached out to Banc of America Merchant Services and Bank of America, the payment processors for the affected payment systems within the affected taxi cab companies. First American Bank is urging that Banc of America Merchant Services and Bank of America discontinue payment processing for the taxi companies who have been targeted in this breach. So far, neither entity is commenting on the breach or appear to be halting the processing services.

Information
Source: Media
March 3, 2014 City of Detroit
Detroit, Michigan
GOV HACK 1,700

The City of Detroit announced a security breach that affected files of approximately 1,700 city employees. Apparently the breach occurred when an employee clicked on a software link that contained malicious software that released a code that froze access to numerous files.

The files included names, birth dates and Social Security numbers of current and former city employees. A city spokesperson communicated that it didn’t appear that the malicious code gained access to the information in the files, however the city is taking all necessary steps to mitigate any damage.

Information
Source: Media
March 1, 2014 Managed Med, A Psychological Organization
Los Angeles, California
MED UNKN Unknown

Managed Med, A Psychological Corporation has notified the California Attorney Generals office of a data breach with their system. Currently they have not communicated what information was involved in the breach, the dates or how many people were affected.

Information
Source: California Attorney General
February 28, 2014 Sears
Hoffman Estates, Illinois
BSR HACK Unknown

Sears announced that the Secret Service is investigating Sears Holdings Corporation as a target of a similar security breach that hit Target and Neiman Marcus toward the end of 2013.

Sears spokesperson, Howard Riefs in an emailed statement stated “there have been rumors and reports throughout the retail industry of security incidents at various retailers, and we are actively reviewing our systems to determine if we have been a victim of a breach,” additionally, “we have found no information based on our review of our systems to date indicating a breach.” said Riefs.

Information
Source: Media
February 28, 2014 80’s Tees
Mt. Pleasant, Pennsylvania
BSR HACK 3,503

80sTees.com, Inc. announced a data breach that was much larger than originally thought. The online retailer originally reported the breach in April of 2013 to customers whose credit card numbers had been used fraudulently. Since that time, the retailer’s investigation uncovered that the scope of the exposure to customer credit card information was larger than originally believed.

The company has notified any customer who used the site from June 3, 2012 through April 30, 2013 that their credit card may have been used fraudulently.

Originally the company was contacted by Discover Card requesting an investigation due to some unauthorized charges experienced by Discover cards customers. The company completed their own investigation and on February 27, 2013 learned that a small number of Visa customers had also experienced unauthorized charges. On March 6, 2013 Mastercard also contacted the company regarding fraudulent charges against their credit card holders.

The company hired a forensic investigator who discovered that the company had been a victim of a cyber attack that gained access to and installed malware on their website server in early June 2012. Their antivirus and malware scans did not detect the malware.

April 3, 2013 the company notified approximately 3,503 customers of the breach. This is the amount that was reported to the company by the credit card companies.
On April 22, 2013, the company received a report from the forensic investigator that 2,598 credit cards were compromised.

On April 30, 2013 the company received calls from two customers stating that their cards had been compromised. The company investigated those customers’ complaints and reported the issue to the Secret Service. The Secret Service asked the company to not provide any additional notice until their investigation had been completed.

The Secret Service investigation uncovered that the hackers had set up an unauthorized email account that captured the company’s credit card transactions without their knowledge. The Secret Service could not definitely say who the hacker or hackers were. Based on the information the company received, they believed it to be a former high level employee who has since died.

---

Information
Source: California Attorney General
February 27, 2014  L.A Care Health Plan
Los Angeles, California

Los Angeles Care Health Plan notified customers of a data breach to their system. Customers were informed that a processing error occurred in their system that may have involved accidental disclosure of their information. They were made aware of an issue in their payment portal that allowed one member to see another members name, address and member identification number.

Upon learning about the breach, they temporarily disabled the payment portal and reassigned new membership ID’s to those members affected. The disclosures took place from January 22, 2014 through January 24, 2014. The breach is being blamed on a manual processing error which has now been corrected.

They are stating that the information was limited to member name, address and member identification number and did not include any other information, such as Social Security number, Driver’s License number, or financial account numbers.

The company has requested those affected either email L.A Care’s Privacy Office at PrivacyOfficer@lacare.org or by telephone 1-855-270-2327 or a letter to 1055 West 7th Street, 10th Floor, Los Angeles, CA 90017.

---

Information
Source: California Attorney General
February 27, 2014  Oak Associates Funds
Boston, Massachusetts

Boston Financial Data Services notified customers of a data security incident that occurred between January 23 to January 27, 2014 that may have involved customer personal information.

The incident involved the theft of a company electronic device. The device contained a data file that had certain Oak Associates Funds records. This file may have contained names, addresses, email addresses, phone numbers, Social Security numbers, and certain account information, which may have included numbers, shares, balances, set-up dates, and contact instructions.

The company has notified authorities and an investigation is underway. The company is offering one year of Experian’s ProtectMyID Alert. Those affected can enroll in the program by visiting the Experian ProtectMyID website at www.protectmyid.com/redeem or by calling 1-877-371-7902. An activation code was supplied in the notification letter sent by the company.

---

Information
Source: Vermont Attorney General
February 27, 2014  Eastern Alliance Insurance Group
Birmingham, Alabama

Eastern Alliance Insurance Group utilized myMatrix as the pharmacy benefits manager responsible for pharmaceutical claims associated with workers compensation benefits provided through policies issued by Eastern Alliance Insurance Group.

Based on an investigation by the company and federal law enforcement a former employee improperly accessed information on customers of Eastern Alliance Insurance Group. The information stolen included names and Social Security Numbers. They are claiming no credit card numbers were compromised.

The company is offering free credit monitoring and identity protection from First Watch Technologies. Those affected can call Jeffrey P. Lisenby, General Counsel at 1-800-282-6242 or contact myMatrixx toll free at 1-888-770-5571.
Indiana University announced that the personal data of 146,000 students and graduates was breached. The information included their Social Security numbers and addresses and may have affected students and graduates from 2011 to 2014 at seven of its campuses.

According to the university "The information was not downloaded by an authorized individual looking for specific sensitive data, but rather was accessed by three automated computer data-mining applications, called webcrawlers, used to improve Web search capabilities."

The university also announced that the information was stored in an insecure location for the past 11 months. The site has since been locked down.

The university has set up a hotline 1-866-254-1484 for students as well as a website http://bit.ly/1kbX505 with information on how to monitor credit accounts and answers to any additional questions regarding an individuals exposure. The university will also be providing the Social Security numbers of those affected to the three major credit-reporting agencies.

Apple has revealed a security protocol breach of their iOS and OS X systems. The hacker was able to insert him/herself between the initial verification and verification session's destination server. This type of hacking allows the hacker to take over as the trusted user. The destination server sees the hacker as the trusted user and will then allow the hacker to access secured connections such as websites, email messages, applications where you would typically enter a user id and password.

Variable Annuity Life Insurance Company has announced a breach that occurred in 2007. The company just discovered the breach in November of 2013. The discovery led to a previous employee of the company in possession of information relating to some of their customers. The information included customer names and either partial or complete Social Security numbers.

The company has stated that they know of no unusual activity involving the stolen files but have set up identity protection services for one year for the affected parties.

Call 1-713-831-6316 with questions.

McKenna Long & Aldridge (MLA) informed current and former employees of suspicious activity on servers belonging to one of their vendors. Information potentially breached included Federal Wage and Tax Statement Forms W-2, names, addresses, wages, taxes and Social Security numbers, dates of birth, ages, genders, ethnicities, Visa, Passport or Federal Form I9 documents numbers.

The law firm operates 15 offices throughout the United States and one in Korea and the data breach could have affected current and former employees in any of the 14 offices.

As a result of an investigation the information related to the current and former employees was accessed on November 28, 2013, December 11, 2013, and December 12, 2013. The breach was a result of malicious software placed on the vendors servers.

MLA is providing one year of credit monitoring and identity theft protection at no cost. Those affected must enroll by May 31, 2014 by calling 1-877-371-7902 or visit the ProtectID website at http://www.protectmyid.com/redeem.
Tuesday, February 25, 2014 one of the largest Bitcoin exchanges in the world was hacked and 744,408 BTC (bitcoins) went missing, which is equivalent to $350 million dollars at todays trading prices.

MtGox publicly declared that "transaction malleability" was the reason behind the theft and reportedly the hackers went undetected for over 2 years. It has been reported they hackers detected a weakness in the "hot wallet"

This is not the first time Mt. Gox has been hacked. In 2011 the exchange was also infiltrated by hackers. Last year the U.S. authorities seized $5 million of the company’s U.S. assets.

Mt. Gox has suspended all withdrawals and has shutdown its website.

Information Source: Media
February 21, 2014
Discover Financial Services
Salt Lake City, Utah

Discover Financial Services sent a notice to their card holders that they were replacing their current cards in wake of all of the retail data breaches. They stated this was not due to a breach of their own systems.

The card replacement specifically replaces the security codes on the back of the card without changing the card holders current account number.

They have stated to their members this was strictly a security measure on behalf of Discover Financial Services. No information was communicated in the letter that the members card had been compromised.

Information Source: California Attorney General
February 20, 2014
Department of Resources, Recycling and Recovery
Sacramento, California

On January 23, 2014 a Human Resource Officer with the office of Resources, Recycling, Recovery notified individuals that an email went out mistakenly to numerous third parties associated with the agency. These third party specialists were hired by the agency to assist in HR issues and are known to the agency as "Personal Liaisons”. The report that was mistakenly sent contained first initials, middle initials, last names and Social Security numbers.

The agency has contacted these third party liaisons asking them to immediately delete the email and shred any paper reports.

The company is also recommending anyone affected by the breach, place a fraud alert with the credit agency's.

For those affected who have further questions, they should call Romana Herrera at (916) 341-6285.

Information Source: California Attorney General
February 20, 2014
Alaska Communications
Anchorage, Alaska

Alaska Communications informed customers of a potential data breach on January 27, 2014. One of the company desktop computers was infected with a virus and subsequently sent data outside of their network. Possible personal information compromised could have included names, addresses, dates of birth, and Social Security numbers. The company stated they did not see any evidence of dependent, medical, or banking information that was compromised.

The company is offering 1 year of AllClear ID protection at no cost and can be reached at 8-1-866-979-2593 for both AllClear Secure and AllClear PRO services.

Any further questions or concerns about the incident there is more information at the company’s website
http://www.alaskacommunications.com/

Information Source: Vermont Attorney General
February 19, 2014
University of Maryland
College Park, Maryland

The University of Maryland, located in College Town Maryland, had one of their records databases hacked Tuesday January 18, 2014 around 4:00 a.m by an outside source.

This particular database holds information dating back to 1998 and includes names, Social Security numbers, dates of birth and university identification numbers for 309,079 people affiliated with the school at their College Park and Shady Grove campuses.

The hackers did not alter anything in the actual database, but apparently have made a “copy” of the information. The university commented at how
sophisticated the attack was by the hacker or hackers and they must have had a "very significant understanding" of how the database was designed and maintained, including the level of encryption and protection of the database.

According to the university President, school officials are investigating the breach and taking steps to prevent any further system intrusions.

The college has put out the following statements:

"The University is offering one year of free credit monitoring to all affected persons. Additional information will be communicated within the next 24 hours on how to activate this service.

University email communications regarding this incident will not ask you to provide personal information. Please be cautious when sharing personal information.

All updates regarding this matter will be posted to this website. If you have any questions or comments, please call our special hotline at 301-405-4440 or email us at datasecurity@umd.edu".

---

Information
Source: Media
February 15, 2014  Kickstart er
Greenpoint, Brooklyn, New York

The crowd-funding site, Kickstarter, was infiltrated by hackers who made off with user information including usernames, email addresses, mailing addresses, phone number and encrypted passwords.

The company has said that no credit card information was taken.

"Actual passwords were not revealed, however it is possible for a malicious person with enough computing power to guess and crack an encrypted password, particularly a weak or obvious one," the site said in a blog post, adding that "as a precaution, we strongly recommend that you create a new password for your Kickstarter account, and other accounts where you use this password."

The company was made aware of the breach when contacted by law enforcement. The company communicated that they "immediately closed the security breach and began strengthening security measures throughout the Kickstarter system."

The site also said "no credit card data of any kind was accessed by hackers" and that "there is no evidence of unauthorized activity of any kind on all but two Kickstarter user accounts."

---

Information
Source: Media
February 15, 2014  Blue Shield of California
San Francisco, California

On January 15, 2014, Blue Shield of California received information that a transaction confirmation page on their website was displaying Agent ID numbers and in some cases those Agent ID numbers were the agent's Social Security number.

The website page shows billing, payment and other account information associated with an applicant/policyholder's Blue Shield account. Blue Shield uses the agent's name and agent ID number as a means of associating the agent with their client in order to facilitate record keeping and policy administration. The transaction confirmation pages that display and agent's ID/SSN number were visible to those policy holders who applied and/or initiated payment of a current policy through Blue Shield's Website from December 20, 2013 and January 16, 2014.

It is unknown at this time if the exposed SSN's have been misused.

---

Information
Source: Media
February 14, 2014  Forbes.com
New York, New York

Forbes.com announced on their Facebook page February 14th, that they had been a target of a data breach by hackers.

They claim that "the email address for anyone registered with Forbes.com has been exposed Please be wary of emails that purport to come from Forbes, as the list of email addresses may be used in phishing attacks. The passwords were encrypted, but as a precaution, we will strongly encourage Forbes.com readers to change their passwords on our system once we make sign-on available again".

---

Information
Source: Media
February 14, 2014  Experian
Costa Mesa, California

Experian notified customers of a potential security breach of their information. Between January 30, 2014 and January 31, 2014 the nationwide credit agency noticed unauthorized access into consumer information without proper authorization using an Experian client's login information. The consumer information consists of information typically found in a consumer report. This information includes names, addresses, Social Security numbers, dates of birth, and account
Zevin Asset Management LLC has notified customers of a potential security breach of their customers’ data. In mid September 2013 a Zevin employee used an online service provider to host a document listing Zevin’s usernames and passwords for certain custodian accounts. According to the company, two documents, one password protected and an inadvertent “test” version of the document that was neither password protected or deleted.

Both versions were accessible online (one through the use of a password and one without a password) and visible from September 2013 through December 30, 2013.

Possible information compromised included names, Social Security numbers, financial account numbers, and account holdings.

The company is offering 1 year free of credit monitoring services and asked to contact Benjamin Lovell, President if they want the enroll in the service.

Las Vegas Sands recently launched an investigation into a security breach of several of their casino websites. Both the Venetian and the Palazzo had the homepage of their websites hacked and there could be others.

Currently it is unknown if credit card information and/or customer data was compromised.

The hackers responsible for the breach posted employee information including email addresses and Social Security numbers, on the website for the Sands Casino Resort in Bethlehem. The hackers also posted an image of Sands Chairman and CEO Sheldon Adelson posing with the Israeli Prime Minister, Benjamin Netanyahu.

In addition to Las Vegas and Bethlehem, websites for casinos in Macau and Singapore were also hacked.

UPDATE (2/28/2014): Las Vegas Sands Casino released a statement that the attackers who breached the company website did compromise customer and employee data, which included Social Security numbers, driver’s license numbers and a mailing database. The data breach affected customers at their location in Bethlehem Pennsylvania. They are currently investigating their additional locations to see if similar data was affected. Originally the company had communicated that customer data was not affected.

Bank of the West notified individuals regarding a recent data breach that may have involved stolen personal information such as Social Security and driver’s-license numbers.

The company sent letters and e-mails to anyone who applied for a job with the company before Dec. 19, the date the breach was discovered.

Currently they are not releasing any information as to the type of information breached or the timeframes the information may have been exposed.

“It could’ve been user name and pass code; it could’ve been more personal information like Social Security numbers, driver’s license, date of birth,” said Debra Jack, Bank of the West spokeswoman. “We don’t have conclusive evidence that personal information was taken, but we sent those letters as a precaution.”

The target of the breach was an online application system that had been retired earlier in 2013, the company disabled the affected servers and is now investigating with help from the FBI.

The company, Freeman, announced a data breach regarding employee W2 forms. Some employees may have received a
W2 form that belonged to another employee. The company announced that one of their vendors, ADP, who works with a large national vendor that mails all of ADP's W2's, has experienced an error in their technology.

A glitch in the mail vendors' technology caused the barcode to input the incorrect barcode on the envelopes. The US Postal Service and delivered based on the barcode, not the name or address shown on the envelope.

**Information Source:**
California Attorney General

**February 10, 2014**

 Nielsen New York, New York

Nielsen company announced that an undisclosed number of Nielsen Audio employees are being notified that their personal information including names and Social Security numbers may be at risk after an employee with their Human Resources department mistakenly sent out a mass email containing the data.

It is currently unknown how many employees were affected.

The Nielsen Audio employee mistakenly emailed a file containing the information to other Nielsen Audio employees, who then forwarded the email containing the file to others within the Nielsen environment. These employees were unaware of the contents of the file.

**Information Source:**
Media

**February 10, 2014**

 University of Miami Health System Miami, Florida

The University of Miami Health System (UHealth) notified patients of a data breach when an offsite storage vendor communicated that the records could not be located. The Health System, which is one of the largest health providers in Southern Florida, discovered the breach on June 27, 2013. They have just recently begun notifying patients of the breach.

The information in the missing files included patient names, dates of birth, physician names, insurance company names, medical record names, facility visited, procedures, diagnostic codes, and Social Security numbers.


**UPDATE** (8/26/2014): The University of Miami Health System has agreed to a class-action settlement for the data breach that occurred in 2013 when records went missing from an offsite storage facility the medical system used.

Under the settlement agreement, the UHealth will be required to conduct various risk assessments, remediate any identified problems, and ensure vendors have adequate security controls in place. The agreement states that the university will pay $100,000 in individual claims, $90,000 in attorneys’ fees, and $1,500 to the named plaintiff that initiated the lawsuit. Both parties have asked the federal district court to approve the recently-filed proposed settlement agreement. [http://www.phiprivacy.net/wp-content/uploads/Carsten_proposedsettlement.pdf](http://www.phiprivacy.net/wp-content/uploads/Carsten_proposedsettlement.pdf)

**Information Source:**
Media

**February 8, 2014**

 Medtronic Minneapolis, Minnesota

It has been reported that Medtronic, the world's largest medical device maker's computer network has been hacked sometime in the first half of 2013. It is not clear what type of information the hackers were targeting. Federal laws meant to safeguard medical information require companies to disclose any breach involving patient information, so far Medtronics has not made these disclosures.

The attacks point to Chinese hackers and the medical device company was not aware of the intrusions until federal authorities contacted them and they have now formed a task force to investigate the breach. A spokeswoman for the medical device maker would not comment on any specific attacks.

**Information Source:**
Media

**February 8, 2014**

 Boston Scientific Natick, Massachusetts

It has been reported that Boston Scientific, a medical device maker's computer network has been hacked sometime in the first half of 2013. It is not clear what type of information the hackers were targeting. Federal laws meant to safeguard medical information require companies to disclose any breach involving patient information, so far Boston Scientific has not made these disclosures.

Denise Kaigler, a Senior Vice President of Corporate Affairs with Boston Scientific stated "like many companies, Boston Scientific experiences attempts to penetrate our networks and systems and we take such attempts seriously. We have a dedicated team to detect and mitigate attacks when they occur as well as to implement solutions to prevent future attacks." Ms. Kaigler would not comment on the specifics of any attack, but described the media reporting as "inaccurate."
The attacks point to Chinese hackers and the medical device company was not aware of the intrusions until federal authorities contacted them and they have now formed a task force to investigate the breach.

Information
Source: Dataloss DB

February 7, 2014 Easter Seals of Superior California
Suwanee, Georgia

On December 10, 2013, an Easter Seal Society of Superior California employee's company vehicle were broken into, and a company laptop containing health record information belonging to minors may have been breached.

The laptop contained emails that may have had specific information such as children's names, dates of birth, health care provider information, health care billing information, patient identification numbers, and occupational therapy notes.

The company is investigating any potential fraud that may have been associated with this information.

Information
Source: California Attorney General

February 7, 2014 San Francisco Airport-South San Francisco Embassy Suites Hotel
South San Francisco, California

South San Francisco Embassy Suites hotel informed customers who stayed at the hotel that they may have been affected by unauthorized access to two of their computer systems. The hotel learned that in 2013 an unauthorized third party obtained information relating to some payment cards used at the hotel.

The information breached involved credit and/or debit card numbers, expiration dates, cardholder names, and the CVV2 code on the back of the cards. The data was captured with a manual device and the hotel is claiming that their computer systems were not breached, so no other personal information about their customers was obtained.

Law enforcement was contacted regarding the breach. The company stated they have no reason to believe that this situation has impacted any other Embassy Suites hotel or any other hotel in their chain.

Information
Source: Vermont Attorney General

February 6, 2014 The Home Depot
Atlanta, Georgia

Three Home Depot employees were arrested for allegedly stealing personal information of some 300 employees, and were initially detected last fall and those employees whose files were notified of the breach. One of the three employees was caught using her Home Depot email to send the stolen information.

Security investigators fear that this breach may have affected as many as 20,000 individuals. Information stolen included Social Security numbers and birthdates. Allegedly the employees opened numerous fraudulent accounts with the stolen personal information.

UPDATE (5/30/2014): Originally it was reported that up to 20,000 individuals may have been affected by this security breach. The number has now been increased to 30,000 individuals may have been affected. The first report that came out reported three Home Depot employees were involved, but according to the disclosure document sent on behalf of The Home Depot Corporation, one individual was arrested and The Home Depot will seek prosecution of the individual to the fullest extent of the law.

Information
Source: Media

February 5, 2014 St. Joseph Health System
Suwanee, Georgia

St. Joseph Health System in Texas has reported a data breach of a server that stored information for numerous facilities.

Information was accessed through a single server by hackers from China and other locations. The server contained employee and patient data for St. Joseph Regional Health Center in Bryan, Burleson St. Joseph Center, Madison St. Joseph Health Center, Grimes St. Joseph Health Center and St. Joseph Rehabilitation Center. The affected server was taken offline once the breach was discovered.

The breach supposedly occurred between December 16 through the 18th, 2013.

The data included patient names, birth dates, Social Security numbers, and possibly addresses. Medical information for patients was accessible, as well as bank information for current and former employees. Both adult and minor information may have been compromised.

Currently, investigators could not determine if any information had been extracted or used.
Dr. K. Min Yi informed patients of a burglary that occurred at the surgeon’s facility on May 28, 2013, in which the burglars stole a desktop hard drive and an external hard drive that had over 4,000 patients records on them.

The information included patients medical history, including lab and radiology reports, surgical information, names, addresses, telephone numbers, dates of birth and insurance information of the primary insured individual. They do not believe that patient Social Security numbers were compromised, however the SSN of the primary insured may have been exposed.

White Lodging, a company that maintains hotel franchises under nationwide brands such as Hilton, Marriott, Sheraton and Westin may have been the victim of a data breach potentially exposing credit and debit card information. The company has not released the number of potential cards that may have been affected.

The breach was first noticed by various banking sources, who were sharing data indicating that they were seeing a pattern of fraud on hundreds of cards that were all used at Marriott hotels around March 23, 2013 through the end of last year. The breach seemed to only occur at those Marriott locations that were managed by White Lodging Services Corporation.

Reportedly the breach appears to have affected mainly restaurants, gift shops and other establishments within hotels managed by White Lodging.

UC Davis Health Center has informed patients of a potential data breach to their system. They recently learned that one of their medical provider’s email accounts was impacted by an email “phishing” scam, which malicious software is used to access records. In this case this malware targeted the medical provider’s email account.

They are currently investigating the breach and are unclear as of now if direct access to the information contained in this provider’s emails was breached. Potential records breached include names, medical record numbers and dates of clinical visits to this provider.

BringItToMe.com informed certain customers that a data breach occurred at one of their vendors that may have compromised personal or payment card information. No details have been released as to the specific personal or payment card information that may have been breached.

The company was recently informed that the online ordering software provider, Big Tree Solutions, discovered unauthorized modifications in their software that could potentially allow new payment card information entered between October 14, 2013 and January 13, 2014 to have been obtained by an unauthorized user.

According to the company the unauthorized modification has been corrected and other security measures have been put into place.
genders, dates of birth, phone numbers, employee ID's, and dates of hire.

The company has launched an investigation as to the unauthorized access and hired a computer security firm to analyze their computer network. In the initial investigation, it appears that the unauthorized person or persons did so for the purpose of filing fake tax returns.

The company is asking any affected employees to complete the IRS Identity Theft Affidavit or to contact the IRS Identity Protection Specialized Unit at 1-800-908-4490 with questions.

The company has also offered free one-year membership to Experian's ProtectMyID Alert.

**Information Source:**
Vermont Attorney General

**January 25, 2014 Michaels Stores Inc.**
 Irving, Texas

On January 25, 2014, Michaels Stores Inc. communicated with customers as to the possibility of a security breach regarding customers payment cards. They have not confirmed as of yet, that a breach did occur, however based on a preliminary investigation and in light of the recent Target and Neiman Marcus breaches, the company felt it was important to warn customers of the possibility of a breach.

Michaels is currently working with investigators as to the potential of this breach. No additional detailed information has been supplied by the company.

**UPDATE (2/11/2014):** A class action lawsuit has been filed against Michaels by an individual. The suit claims that "the arts and crafts supplier failed to secure and safeguard customers’ private financial information". The suit also alleges that "Michaels failed to adequately monitor its payment systems in such a manner that would enable the retailer to detect fraud or other signs of tampering so that the breach of security and diversion of customer information was able to continue unnoticed for a period of time".

It has also been reported that Michaels failed to disclose a data breach that occurred in May of 2011. A lawsuit was filed for the 2011 breach, but was settled.

The company has not yet released the total number of individuals affected by the breach or when the breach might have taken place.

**UPDATE (7/22/2014):** "A federal court in Illinois held July 14 that an elevated risk of identity theft from a Michaels Stores Inc. breach provides standing, but without evidence of specific monetary damages that risk is insufficient to support statutory or common law claims ([Moyer v. Michaels Stores, Inc.](http://www.pennrecord.com/news/15093-class-action-filed-against-coca-cola-fo...), N.D. Ill., No. 1:14-cv-00561, dismissed 7/14/14).

Judge Elaine E. Bucklo of the U.S. District Court for the Northern District of Illinois dismissed the case against the arts and crafts retailer, finding that the plaintiffs failed to plead monetary damages".

**Information Source:**
Media

**January 24, 2014 Coca-Cola Company**
 Atlanta, Georgia

The Coca-Cola Company announced the theft of several computers from one of their locations that contained personal information on employees and other individuals. The company did not detail the specific information that was stored on the stolen computers. The theft was discovered on December 19, 2013.

**UPDATE (11/13/2014):** "A class action lawsuit has been filed against the Coca-Cola company and its regional distribution subsidiaries on behalf of 70,000 people whose information and identities have been allegedly compromised by the theft of 55 laptops from the company’s Atlanta headquarters over a six year period."

The company did not notice the theft of these laptops until November of 2013 prompting the company to send notices to those affected in January 2014. According to the company, 18,000 individuals had Social Security numbers affected, and an additional 56,000 individuals that may have had their drivers license information compromised. The laptops were not encrypted and along with the above information, the laptops may have also included names, addresses, ethnicity and other personal information.

The class action suit alleges that the company failed to protect personal data, but failed in adequately notifying victims of the breach.


**UPDATE** (October 13, 2015): A Coca-Cola employee who showed he suffered harm after company laptops were stolen is pursuing a class action lawsuit against the company according to a Pennsylvania federal court.


**Information Source:**
California Attorney General

**St. Francis Hospital and Medical Centers**

January 24, 2014  
St. Francis Hospital and Medical Centers  
Hartford, Connecticut  

MED  PHYS  Unknown

St. Francis Hospital announced a breach of 858 patient records when physical patient files were stolen from a contracted emergency room physicians car. The files included patient names, patient medical record numbers and dates of birth. No Social Security numbers or financial records were compromised.

Information  
Source:  
Dataloss DB

January 23, 2014  
W.J Bradley  
Centennial, Colorado  

BSF  INSD  Unknown

W.J Bradley Mortgage Capital, LLC announced in a letter to customers that information disclosed to the Emery Team at W.J Bradley Mortgage Capital, LLC in connection with numerous loan transactions had been breached. According to the company, information on specific loan transactions had been taken from their computer systems and copied by several former loan officers of the company. This information was then shared with another mortgage company not associated with W.J Bradley.

The company communicated that the information taken included income, marital status, and loan information. There is no evidence that the information was released to the public at large.

A court order was obtained by W.J Bradley requiring the return of all private customer information to the company, prohibiting the defendants from sending that information to others, and requiring that the defendants destroy all copies of the information in their possession.

Information  
Source:  
California Attorney General

January 20, 2014  
Dartmouth-Hitchcock  
Lebanon, New Hampshire  

BSO  HACK  Unknown

Dartmouth-Hitchcock informed patients of a security breach involving their personal information that is maintained by the company.

On or around December 3, 2013, the company discovered that, as a result of a phishing incident, certain employee user accounts had unauthorized activity in the Employee Self Service Direct Deposit Payroll system.

The company launched an investigation and found further unauthorized access to this same system from October 6, 2013 through December 2, 2013. The information accessed included full names, bank account information (routtng and checking account numbers), Social Security numbers along with other information the employee supplied to the self service system.

Employees are asked to call IS Security Manager, Charles Goff at 1-603-653-1380 or email IS-Security@hitchcock.org.

Information  
Source:  
Vermont Attorney General

January 17, 2014  
Easton-Bell Sports Inc.  
Van Nuys, California  

BSR  HACK  Unknown

Easton Bell Sports Inc., out of Van Nuys California informed customers of a data breach in December. The company has stated that one of their vendors servers was the attack of vicious malware and was breached on or around December 1, 2013.

The breach may have impacted online purchases made from December 1, 2013 to December 31, 2013. The customer information breached may have included names, addresses, phone numbers, email addresses, credit card numbers, along with the 3 or 4 digit security code on the back of cards.

Once the breach was discovered, the company immediately shut the server down and took steps to stop any further infiltration of the system. The company has hired a computer forensics expert to conduct an investigation.

The amount of customers affected is currently unknown.

Information  
Source:  
California Attorney General

January 17, 2014  
E-Benefits Department of Veteran Affairs  
District Of Columbia  

GOV  UNKN  Unknown

As reported by a local T.V station in Moore County North Carolina, a Navy veteran reported to have been utilizing the E-Benefits portal through the Department of Veteran Affairs to check his own benefits. He was on the VA’s E-Benefits website trying to track down his own history for a bank loan. Instead, windows kept popping up displaying other veterans’ medical and financial information. He has since reported the issue to the Department of Defense, the VA and Senator Kay Hagan’s office.

The VA has responded with a statement to ABC11 on Friday January 17, 2014 with the following:
“The Department of Veterans Affairs (VA) takes seriously our obligation to properly safeguard personal information. Wednesday evening, during a process to improve software supporting the joint VA and Department of Defense benefits web portal eBenefits, VA discovered a software defect. During that limited timeframe, some Veterans and Servicemembers who had registered and logged into eBenefits were able to see a combination of their own information as well as data from other eBenefits users. VA took immediate action upon discovering the software defect and shut the eBenefits system down in order to limit any problems. VA is conducting a full review to be certain the underlying technological issues have been resolved before the system is returned to operation.

VA’s independent Data Breach Core Team (DBCT) is reviewing this issue and believes a relatively limited number of Veterans have been affected. Once the DBCT determines the number of users impacted, their identities and other pertinent facts, VA will take the appropriate response, which may include free credit monitoring for the affected individuals, consistent with VA’s standard practice.”

Information Source:  
Media 

January 15, 2014  
South Carolina Department of Employment and Workforce  
Columbia, South Carolina  
GOV  INSD  4,658

A South Carolina Department of Employment and Workforce human resources employee allegedly downloaded the personal information of 4,658 current and former DEW employees to a personal device, according to authorities.

The data downloaded may have included payroll information, Social Security numbers and bank account information. The employee has since been fired. The incident allegedly occurred on December 18, 2013.

Information Source:  
Media 

January 15, 2014  
City of Burlington  
Burlington, Vermont  
GOV  DISC  Unknown

The Office of The Clerk/Treasurer for the City of Burlington informed individuals that their names and Social Security numbers were inadvertently left unredacted as part of the individuals request for a tax abatement that was provided to the Burlington Board of Tax Abatement (which is made up of the City Council, Mayor and City Assessor).

The information was part of a clickable agenda item that was posted on the City Council’s website on January 9, 2014, the information was redacted on January 13, 2014.

Those affected with questions can call Bob Rusten, Chief Administrative Officer at 1-802-865-7000.

Information Source:  
Media 

January 14, 2014  
Southwest General Health Center  
Middleburg Heights, Ohio  
MED  PHYS  480

Southwest General Hospital notified approximately 480 patients who were part of an obstetrics study that some of their private information was recently lost, including names, data on births, clinical information and medical record numbers. The data was included in one binder and the binder was discovered missing early in December 2013. The binder did not include Social Security numbers or financial information.

Information Source:  
Media 

January 14, 2014  
NORCOM-North East King County Regional Public Safety Communication Agency  
Bellevue, Washington  
GOV  HACK  6,000

The North East King County Regional Public Safety Communication Agency (NORCOM) has announced a security breach of a server that stored records of an estimated 6,000 medical responses for Duvall Fire District 45, Skykomish Fire Department and Snoqualmie Pass Fire & Rescue. Currently, the investigation has revealed that the medical response records breached included names, addresses, dates of birth, nature of emergency call and initial medical condition.

The breach also included personnel data for 231 full-time and volunteer firefighters who work or have worked for the three agencies. This information could include driver's license information, date of birth, Social Security numbers, emergency contact and limited medical information.

Information Source:  
Media 

January 13, 2014  
Update Legal  
San Francisco, California  
BSO  INSD  Unknown

On or around September 9, 2013, Update Legal was informed by San Francisco Police that a suspect in custody had digital photographs of I-9 forms on the smartphone in this person’s possession. This individual potentially obtained Social Security numbers, date of birth, driver's license numbers, email addresses, passport identification, state ID cards, military dependent's ID cards, US Citizen's ID cards, Certification of Birth Abroad, Birth Certificates and addresses.
Neiman Marcus confirmed that its database of customer information was hacked last month, around mid-December, the same time that Target stores were targeted. The case is similar to the Target case in that only retail shoppers were affected, no online shoppers were affected.

The cause, size and duration of the attack are not yet known and should start to be revealed once a third party investigation is completed. The company is also working with the Secret Service, which is customary in these types of attacks.

**UPDATE (1/16/2014):** It has been reported that the breach at Neiman Marcus could as far back as July 2013 and that the breach was not fully contained until Sunday January 12, 2014. Neiman Marcus is still not communicating the total amount of individuals affected, but did comment that "some of their customers" payment cards were used fraudulently and have taken steps to notify those customers. They still do not believe that Social Security numbers or birth dates were affected.

**UPDATE (1/25/2014):** Neiman Marcus released a statement that approximately 1.1 million individuals have been affected by the recent data breach to their system.

**UPDATE (7/21/105):** A lawsuit filed against Neiman Marcus for the data breach it suffered in 2014 and may have started as far back as 2013, has been ruled to have standing.

"The United States Court of Appeals for the Seventh Circuit held that data breach victims suffer injury for purposes of Article III standing and can thus have their day in court against companies who fail to protect their personal information from hackers.

The class action against Neiman Marcus alleged that the data breach plaintiffs suffered injuries even if they have not yet been victims of identity theft or other fraud. These injuries include an increased risk of future fraudulent charges and greater susceptibility to identity theft. Chief Judge Wood noted that "the Neiman Marcus customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an 'objective reasonable likelihood' that such an injury will occur."


---

Rakecia Matrese Brame, a former social worker for the Alamance County Department of Social Services in North Carolina, pled guilty to identity theft, tax, and fraud charges. According to court documents, Brame was employed as a social worker from 2009 to 2011 and was responsible for investigating claims of abuse and neglect against minors and disabled adults. She had authorized access to their system which included names, dates of birth and Social Security numbers of Alamance DSS clients.

Brame used her access to identifying information contained in Alamance DSS records to illegally obtain the personal identifying information of clients and others. She would then sell that information to two tax preparers at the Greensboro branch of Nothing But Taxes, a tax return preparation firm. They used the stolen identities to claim false dependents on tax returns they prepared for Nothing But Taxes clients, inflating tax refunds on their clients' behalf.

---

Barry University informed individuals of a security incident that may have affected personal information maintained by the university.

On May 14, 2013, Barry University detected malware which infected a laptop owned and used by Barry University. The files infected included full names, dates of birth, Social Security numbers, driver's license numbers, bank account numbers.

The university is offering a free one-year credit monitoring service. They've supplied a phone number to those affected at 1-800-981-7571 and to reference number 47911.
Loudoun County school officials have responded to a data breach that made publicly available personal information about students and staff members, along with detailed emergency response plans for each school.

More than 1,300 links could be accessed through a Google search, thought to be password protected, unveiled thousands of detailed documents as to how each school in the district will respond to a long list of emergencies, which included the staging areas for response teams as well as where the students and staff would be located during an emergency.

Additional documents that could be accessed included students’ course schedules, locker combinations, home addresses, phone numbers and birthdates along with the address and cell phone numbers for many school administrators.

The contractor Risk Solution International acknowledged that the breach was caused by “human error” on their part, which is said to be the cause of the data breach.

UPDATE: Loudoun County Public Schools administrators released a more detailed statement about the information made publicly available on the Internet due to errors committed by the contractor Risk Solutions International (RSI).

According to school officials, the investigation is continuing as to how the webpage, which was made accessible through online search engines without any password protection happened. The page included 1,286 links detailing information on 84 Loudoun schools. It is unknown how long the information was exposed or how many links were opened by unauthorized individuals.

Locker combinations were revealed for one school and only one parent contact information was revealed for fewer than 10 schools according to the spokesperson for the district. The statement also made clear that RSI’s website was not hacked and that it never lost its password security. Instead, the breach occurred when RSI employees were doing technical testing on November 4th, December 19th and December 24th 2013. (1/9/2014)

Information Source: 
January 3, 2014  
Agency of Human Services  
Williston, Vermont  
Beverly Franklin  
GOV  DISC  Unknown

Vermont Agency of Human Services notified individuals of a data breach containing names and Social Security numbers of individuals. The email distribution list inadvertently included all AHS employees and some contractors. According to the agency, the email was opened by numerous AHS employees, a subsequent email was promptly sent that instructed recipients of the email to “hard delete” it so it did not remain in their email delete box.

For those with questions or concerns can call Joanne Dunster, Benefit Programs Assistant Administrator/ESD HIPAA Liaison at 1-802-769-6155.

Information Source: 
January 2, 2014  
Straight Dope Message Board  
Chicago, Illinois  
BSO  HACK  Unknown

The security team at The Straight Dope discovered hackers broke into their online message board forum. This resulted in unauthorized access of members usernames, emails and passwords. The message board does not store Social Security numbers or credit card information. The company is suggesting all users change their password in their system.

Information Source: 
January 2, 2014  
Eye Surgery Education Council  
Fairfax, Virginia  
MED  HACK  4,748

Reportedly, the Eye Surgery Education Council’s system was hacked and user accounts with partial email addresses, user names and clear text passwords were dumped onto the Internet.

Information Source: 
January 1, 2014  
Snapchat  
Venice, California  
BSO  HACK  Unknown

The hacker or group known as "Lightcontact" is claiming to have hacked Snapchat.com. Reportedly, the group published a database containing Snapchat user names and phone numbers and posted it to several public forums such as Reddit.com.

UPDATE: Snapchat has announced a security update to their mobile image sharing services to include an opt out option to the Find Friends system. This update is said to prevent others from looking up their account information through address books. This update will allow a person to no longer appear if this type of search is initiated. According to security vendor AdaptivMobile, the compromised accounts are concentrated mostly in California and New York, with the two states accounting for nearly 2.3 million accounts. Other regions affected include Illinois, Colorado and Florida(1/4/2014)
January 1, 2014  **Skype breach**  
*Redmond, Washington*  

On January 1st, the Syrian Electronic Army is reportedly taking credit for hacking into user accounts on Skype. The amount of users affected is unknown. Reportedly, the hackers infiltrated a user's account and monitors the activity and sells the data.

**Information Source:** Media  

December 30, 2013  **T-Mobile Supplier**  
*Unknown,*  

A supplier for T-Mobile reported a breach of files stored on their servers. This breach included the breach of names, addresses, Social Security numbers and/or Driver's License numbers. This access was discovered in late November 2013. They believe that the primary goal of the hackers was to obtain credit card data, but credit card information was not included in these files.

**Information Source:** California Attorney General  

December 30, 2013  **Wichcraft Operating LLC**  
*New York, New York*  

An unauthorized third party accessed their systems compromising payment card information of certain customers in possibly two of their locations, New York and San Francisco. The breach occurred from approximately August 11, 2013 to October 2, 2013.

Based on their investigation, the information accessed by the unauthorized party may have included names, payment card numbers, security codes and expiration dates. They are claiming that not all of these data elements were accessed for each customer.

**Information Source:** California Attorney General  

December 29, 2013  **American Express Company**  
*New York, New York*  

American Express announced, as part of an investigation by law enforcement and/or American Express, the company discovered a data breach that involved customer information. The data recovered included American Express cardholder account numbers, names and other card information such as the expiration date. They have stated that Social Security numbers were not impacted and their systems did not detect any unauthorized activity on card holders accounts as related to this incident.

**UPDATE:** (1/16/2014): American Express has sent out a new letter addressed to customers affected by the data breach. This new communication entailed information that one of the merchants that they purchased goods with was affected by the breach. The information breached did not change, in that card holder account numbers, names and other card information such as expiration date were compromised. No Social Security numbers were impacted.

**Information Source:** California Attorney General  

December 29, 2013  **Riverside Health System**  
*Newport News, Virginia*  

Riverside Health System has announced an electronic records health breach discovered in November. The breach involved one employee who accessed 919 medical records over a four-year period. The system wide breach included patients Social Security numbers, patient history and other information that appears in the system's electronic medical record.

**Information Source:** Media  

December 27, 2013  **Briar Group**  
*Brighton, Massachusetts*  

Briar Group confirms it was the source behind a Seaport data breach. After an investigation by the Briar Group, who runs eight restaurants and bars in the city, confirmed that their systems were compromised causing the data breach that affected hundreds of individuals who visited the Seaport area of Boston sometime in November.
Currently, a number has not been released as the investigation regarding the breach is ongoing. The breach included unauthorized access to card data at their restaurants sometime between October and November 2013.

Information
Source: Media
December 27, 2013
Colorado Community Health Alliance (CCHA)
Denver, Colorado
MED INSD Unknown

1,918 Medicaid patients data was breached after a temporary employee from an outside contractor Colorado Community Health Alliance (CCHA) sent the information to his/her own personal email address according to media reports. The Colorado Department of Health Care Policy and Financing believes this information may have been intended for the employee’s use in another business.

The information included patient names, date of birth, addresses, telephone numbers, health conditions and Medicaid identification numbers. Social Security numbers were not involved.

Information
Source: Media
December 25, 2013
Inspira Medical Center Vineland
Vineland, New Jersey
MED STAT Unknown

The December 23 theft of a computer from the radiology department of Inspira Medical Center Vineland may have resulted in the exposure of patient information. The computer was kept in an unsecured filing room.

Information
Source: PHIprivacy.net
December 24, 2013
Lakes Liquor
Detroit Lakes, Minnesota
BSR UNKN Unknown

Hundreds of debit and credit cards were compromised after customers used them at Lakes Liquor between October 27 and November 25. Customer names, payment card numbers, expiration dates, and security codes may have been accessed for fraudulent purposes. It is unclear how the information was obtained from Lakes Liquor.

Information
Source: Media
December 22, 2013
Office of Dr. Rob Meaglia, DDS
Rocklin, California
MED STAT Unknown

The December 15 office burglary of a computer resulted in the exposure of patient information. Medical records, dental insurance information, and Social Security numbers may have been exposed. The computer was encrypted and password-protected.

Information
Source: California Attorney General
December 21, 2013
Affinity Gaming
Las Vegas, Nevada
BSO HACK Unknown

Facilities owned by Affinity Gaming may have been exposed to a cyber attack between March 14 and October 16. Customer information associated with credit and debit cards may have been taken. Affinity Gaming owns Silver Sevens Hotel & Casino, Rail City Casino, Buffalo Bill’s Resort & Casino, Primm Valley Resort & Casino, Whiskey Pete’s Hotel & Casino, Golden Mardi Gras Casino, Golden Gates Casino, Golden Gulch Casino, Mark Twain Casino & RV Park, Lakeside Hotel & Casino, and St. Jo Frontier Casino.

Information
Source: Media
December 21, 2013
DeLoach & Williamson, South Carolina Health Insurance Pool
Columbia, South Carolina
MED PORT Unknown

The October 16, 2013 theft of a laptop from a DeLoach & Williamson employee’s car may have resulted in the exposure of an unspecified number of South Carolina Health Insurance Pool patients’ information. Full names with middle initials, Social Security numbers, dates of service, and provider identification numbers may have been exposed.

Information
Source: Media
December 20, 2013
Tennova Cardiology
Nashville, Tennessee
MED PORT 2,777

Those with questions may call (866) 369-0422.
The October 22 theft of a laptop from a transcription contractor working with Tennova Cardiology resulted in the exposure of patient information. The laptop was not encrypted and included names, dates of birth, physician names, and health information (No Social Security numbers or financial information reported).

**Information Source:** Media  
December 20, 2013  
**Discover Financial Services**  
Riverwoods, Illinois  
BSF UNKN Unknown

An unspecified number of Discover customers had their account numbers changed and were issued a new card. It is unclear what type of security breach prompted the notification and when it may have occurred. Several customers in California received the notification letter; residents of other states may have been notified as well.

**Information Source:** California Attorney General  
December 20, 2013  
**Techmedia Network**  
Ogden, Utah  
BSO HACK Unknown

An unauthorized person or persons gained access to Techmedia Network's systems. Customer names, credit card numbers, expiration dates, CVV security codes, mailing addresses, email addresses, and phone numbers may have been exposed. The breach was discovered on November 28.

**Information Source:** California Attorney General  
December 20, 2013  
**W.J. Bradley Mortgage Capital, LLC**  
Centennial, Colorado  
BSF INSD Unknown

A former loan officer took files from WJB’s computer systems while she was still employed. The loan officer then left WJB and another mortgage company ended up with the information in late July and early August of 2013. Client names, Social Security numbers, credit reports, bank account information, tax information, and other sensitive information related to loan applications was taken. The information was eventually retrieved and removed from the systems of the unnamed mortgage company.

**Information Source:** California Attorney General  
December 20, 2013  
**Walgreens**  
Baltimore, Maryland  
BSR INSD Unknown (eight people confirmed to have been affected)

Walgreens became aware of a breach involving an employee on November 4, 2013. The employee was fired and prosecuted. The incident was reported to the Maryland Attorney General’s office on November 27 and credit card numbers were affected.

**Information Source:** PHIPrivacy.net  
December 20, 2013  
**Washington Department of Social and Health Services (DSHS)**  
Tacoma, Washington  
MED DISC 2,600

The personal information of between 2,600 and 7,000 households receiving assistance from the Washington DSHS was accidentally mailed to old or incorrect addresses between August 19 and October 26. The information included names, Social Security numbers, dates of birth, phone number and other contact information, medical diagnosis information, chemical dependency or treatment information, income, and any public-assistance services that the household received. The issue was discovered on October 22.

**UPDATE:** Acting Medicaid Director releases information on the incorrect mailing of Medicaid cards by NCDHHS: The Director states; “After a review of the incident, it has been determined that some Medicaid cards were incorrectly sent because of human error in computer programming and the quality assurance process in printing the new Medicaid identification cards. These new cards were printed for children switched from NC Health Choice to Medicaid because of new eligibility rules and requirements under the Affordable Care Act (Obamacare). A program was developed to extract the information from the eligibility database to generate the mailing, but utilized the incorrect name and address for the parent or responsible adult.

The incorrect card shows the child’s name, Medicaid identification number, date of birth and primary care physician’s name and physician’s address. No Social Security numbers were released.

The parent or responsible adult who received an incorrect card is being advised to immediately destroy it by shredding or cutting it into small pieces. They are also being advised that they can turn in the card to their
county department of social services if they prefer. A directory of the county social services offices can be
found here: http://www.ncdhhs.gov/dss/local/.” (1-06-2014)

Information
Source: PHIPrivacy.net

December 20, 2013  StakerLaw Tax and Estate Planning Law
Camarillo, California

On Friday December 20, 2013 the owner of the firm had his home burglarized in which the firm’s back-up hard drive was
stolen which contained the firm’s customer files containing sensitive personal information.

Information
Source: California Attorney General

December 18, 2013  Washington Post
Washington, District Of Columbia

Hackers were able to access Washington Post employee usernames and passwords through an attack on the paper’s
servers. The attack began through access to a server used by the Washington Post’s foreign staff and then spread to
more Washington Post servers. The Washington Post and several other national papers were attacked in 2011 as well.

Information
Source: Media

December 18, 2013  CITGO Petroleum Corporation
Houston, Texas

A folder with personal information was discovered in a location that made it accessible on CITGO’s intranet to
unauthorized employees. The issue was discovered on October 9. Social Security numbers, financial information, and
other personal information could have been accessed.

Information
Source: California Attorney General

December 17, 2013  Colorado Governor’s Office of Information Technology
Denver, Colorado

A Colorado state employee lost a flash drive that contained the information of current and former Colorado state
employees. It contained names, Social Security numbers, and a limited number of home addresses. The flash drive was
discovered missing in late November and is believed to have been lost while the employee traveled between work sites.
Approximately 8,000 of those who were affected were current employees while 10,800 were former employees.

Information
Source: Media

December 17, 2013  U.S. Federal Election Commission (FEC)
Washington, District Of Columbia

The U.S. Federal Election Commission’s computer system was accessed by unauthorized parties sometime in October of
2013 during the government shutdown. The system appears to have been infiltrated by hackers located in China. The
attack occurred at a time when no staff members were on duty to identify the issue.

Information
Source: Media

December 17, 2013  Jonathan M. Wainwright Memorial VA Medical Center
Walla Walla, Washington

Some veterans may have had their information accidentally emailed to an external source on November 1. An email sent
to an external education partner contained an attachment with veteran information that included names and Social
Security numbers. The issue was contained within 10 minutes of the email being sent.

Information
Source: Media

December 17, 2013  Radnor School District
Radnor, Pennsylvania
An employee performing a transfer of personnel data accidentally left the data accessible and a middle school student viewed it. The student also shared the information. Current and former employees may have had their names, addresses, phone numbers, dates of birth, and Social Security numbers accessed as early as June and as late as the end of the 2012-2013 school year. The breach was discovered in November.

Information
Source: Media
records from this breach used in our total: 2,000

December 17, 2013
Comprehensive Psychological Services LLC
Columbia, South Carolina
MED PORT

The October 28 office theft of a laptop resulted in the exposure of patient information. The laptop was password-protected and the patient files on it were not encrypted. Neuropsychological testing, educational testing, custody evaluations, and other assessments and evaluations may have been exposed.

Information
Source: Media
records from this breach used in our total: 0

December 17, 2013
UHS-Pruitt Corporation
Norcross, Georgia
MED PORT 1,300

Those with questions may call (678) 533-6437 or 1-800-222-0321.

Current and former residents of Heritage Healthcare of Ashburn, UniHealth Post-Acute Care Augusta Hills, Heritage Healthcare of Fitzgerald, Heritage Healthcare at Osceola, Palmyra Nursing Home and Sylvester Healthcare may have been affected by the September 26 theft of a laptop from an employee's car. The laptop contained patient names, Social Security numbers, Medicare numbers, dates of birth, and resident ID numbers.

Information
Source: Media
records from this breach used in our total: 1,300

December 17, 2013
UniHealth SOURCE
Austell, Georgia
MED PORT 2,500 (No Social Security numbers or financial information reported)

The October 8 theft of an employee's laptop resulted in the exposure of current and former client information. The laptop was taken from the employee's car while it was parked at home. Full names and potential diagnoses may have been exposed.

Information
Source: Media
records from this breach used in our total: 0

December 16, 2013
Tennessee Department of Treasury
Nashville, Tennessee
GOV INSD 6,300

An employee downloaded the information of 6,300 Nashville teachers in order to work from a personal computer and account at home. A Tennessee Consolidated Retirement System file that contained teacher names, Social Security numbers, and dates of birth was uploaded by the employee around the time that he resigned from his position. His personal computer and other electronic devices were seized by investigators.

Information
Source: Media
records from this breach used in our total: 0

December 16, 2013
Massachusetts Mutual Life Insurance Company
Springfield, Massachusetts
BSF DISC Unknown

A MassMutual account manager accidentally included information about retirement plans in an email that was sent to an individual at a MassMutual retirement services client. The client representative confirmed that the email was deleted. It contained an unspecified number of client information that included names, Social Security numbers, addresses, dates of birth, retirement plan names, and group numbers. The incident occurred on December 3.

Information
Source: California Attorney General
records from this breach used in our total: 0

651 (No Social Security numbers or financial information reported)
Those with questions may call 1 (719)-576-2225.

A former doctor took patient information after ending his practice at Colorado Health & Wellness, Inc. The breach was discovered on September 4, 2013 and involved patient names, addresses, telephone numbers, and email addresses. A notice was sent by Colorado Health & Wellness in November.

Information
Source: HHS via PHIPrivacy.net

December 16, 2013  Dr. Martin Luther King Jr. Health Center, Bahoo.net, Professional Transcription Company  Bronx, New York  MED DISC  37,000 (No Social Security numbers or financial information exposed)

Those with questions may call 1-(877)-451-9361.

Dr. Martin Luther King Jr. Health Center learned that a transcription vendor named Professional Transcription Company hired a subcontractor named Bahoo.net to work on data transcription. Bahoo.net inadvertently made patient information viewable through public internet search engines. The breach occurred in 2009. Patient names, treatments, procedures, diagnosis information, and dates of services may have been accessed. Bahoo closed its website and destroyed the hard drive so that the public could no longer view the personal information. It is unclear what types of data were on the hard drive and when it was posted because the hard drive was destroyed.

Information
Source: HHS via PHIPrivacy.net

December 16, 2013  Greater Dallas Orthopaedics, PLLC  Dallas, Texas  MED STAT  5,840 (No Social Security numbers or financial information reported)

Patients of Dr. Allaaddin Mollabashy and Dr. Nathan F. Gilbert may have had their information exposed by the September 1 office theft of two computers. Patient names and medical information were on the password-protected laptops.

Information
Source: HHS via PHIPrivacy.net

December 14, 2013  Bailey’s Health Center  Falls Church, Virginia  MED DISC  1,499

Patient information was kept on an unsecured computer server. Names, Social Security numbers, addresses, pharmacy identification numbers, medication dosages, payment information, and names and addresses of prescribers may have been accessed by unauthorized parties. The pharmaceutical records were discovered online on October 18 through a routine forensic audit.

Information
Source: Media

December 14, 2013  Lanap and Implant Center of Pennsylvania  Collegeville, Pennsylvania  MED DISC  11,000

Those who want to know if they were affected may call 1-(570)-704-5854.

The Lanap and Implant Center learned of a breach on September 17, 2012. Patient information had been uploaded to websites in February of 2010 where it could be downloaded by anyone. Names, Social Security numbers, addresses, dates of birth, phone numbers, dates of appointments, types of services provided, dental insurance information, and other patient records were available. At least 5,000 patients were informed of the breach sometime around November 1, 2012. The information appears to still be available for download.

Information
Source: PHIPrivacy.net
An employee accessed patient information without cause. The employee's actions did not appear to be malicious and the employee was placed on administrative leave. The incident or incidents were discovered on November 4.

Information Source: Media

December 13, 2013

The University of Connecticut (UConn) Health Center
Storrs, Connecticut

MED INSD

164 (No Social Security numbers or financial information exposed)

Electronic files that contained names, Social Security numbers, tax identification numbers, addresses, and dates of birth were discovered online on November 11. The information was taken down on November 23 and appears to have accidentally ended up online after maintenance work on a University computer disabled a privacy feature during the summer.

UPDATE (12/17/2013): Over 6,500 individuals were affected. The breach affected current and former staff as well as fewer than 200 students. The data affected may date back as far as 1999.

Information Source: Media

December 13, 2013

University of North Carolina - Chapel Hill
Chapel Hill, North Carolina

EDU DISC

6,500

A notice from Target Corp. can be found here: Target’s CEO with a message to consumers

Customers with questions may call Target at 866-852-8680 or visit Target’s main website.

Target discovered that hackers may have accessed customer debit and credit card information during the Thanksgiving and Christmas shopping season. Customers who used a payment card at any of Target’s stores nationwide between November 27, 2013 and December 15, 2013 may have had their payment card information copied for fraudulent purposes. Credit card companies and banks have been notifying customers of the issue and advising them to watch for suspicious charges. Customer names, credit or debit card numbers, card expiration dates, and card security codes were taken and have appeared on the black market.

UPDATE (12/24/2013): Target now faces at least three class-action lawsuits as a result of the breach. A wave of scam artists are attempting to profit from the breach by posing as Target or bank representatives addressing the breach. People who shopped at Target are being warned not to give their information out over the phone. Target is working with the U.S. Department of Justice and the Secret Service to investigate the breach.

UPDATE (12/27/2013): Target customers are also being warned to be suspicious of emails claiming to be from Target or banks that request personal information. It is estimated that the breach may cost Target up to $3.6 billion. It appears that online customers were not affected.

UPDATE (12/28/2013): Target confirmed that PINs associated with payment cards were also exposed.

UPDATE (1/2/2014): East-West bank has issued a letter to their card holders warning that some of their accounts may have been compromised due to the Target data breach. East-West bank has issued new credit cards to their customers who shopped at any Target stores to reduce any potential unauthorized use of a card. (Source CA Attorney Generals’ Office)

UPDATE (1/10/2014): Target Corp. says that up to 70 million people were affected by the data breach, significantly more than was originally suspected. Experts predict the numbers could climb even higher than 70 million once the company completes its investigation.

UPDATE (1/13/2014): Target Corp. has confirmed that malware was found on the Point of Sale devices. The malware has been removed. The number of individuals affected are now said to be 110 million individuals, 70 million more than originally thought.

UPDATE (1/13/2014): Security experts are stating that Target may not be alone in the data breach. Neiman Marcus and at least 3 other unnamed retailers (these retailers are thought to be located in Eastern Europe) may also have been compromised as federal investigators track what they believe to be an international crime ring.

UPDATE (1/14/2014): Companies that help Target process payments could be facing millions of dollars in fines and costs as a result of the data breach.

UPDATE (1/16/2014): The malware that infected in the Target POS systems has been found and is known as the Trojan.POSRAM, according to new report by investigators. “The malware is a memory-scraping tool that grabs card data directly from point-of-sale terminals and then stores it on the victims system for later retrieval”. The malware was originally thought to have been developed in Russia, known as BlackPOS. This new version is considered to be highly customized so that current antivirus programs would not have detected it as reported by investigative agencies.

UPDATE (1/20/2014): "A 17 year-old Russian national from St. Petersburg is thought to be responsible for the malicious programming that allowed for data from Target and Neiman Marcus to be compromised," according to a California based security firm.
UPDATE (12/1/2014): Two Mexican citizens were arrested at the border in South Texas for the purchase of thousands of dollars worth of merchandise with information stolen during the Target security breach, as reported by a South Texas police chief.

A spokesman with the Secret Service announced that the investigation is ongoing into the possibility of a link between the Target breach and the two arrested in Texas.

UPDATE (12/2/2014): A Target Corp. investor filed suit in Minnesota federal court Wednesday, against the retailers Executives holding them liable for damage caused by the holiday season data breach that saw hackers steal personal and financial information from tens of millions of customers.

Shareholder Maureen Collier filed the suit with a complaint alleging that Target's board and top executives harmed the company financially by failing to take adequate steps to prevent the cyberattack then by subsequently providing customers with incomplete and misleading information about the extent of the data theft.

"The suit brings claims of breach of fiduciary duty, gross mismanagement, waste of corporate assets and abuse of control, and seeks monetary damages on behalf of the company from the 14 named officers and directors".

UPDATE (2/5/2014): Hackers who broke into Target's computer network and stole customers' financial and personal data used credentials allegedly were stolen from a heating and air conditioning subcontractor in Pennsylvania, according to digital security journalist Brian Krebs.

It appears as though the air conditioning company was given access to Target's computer network in order for the vendor to make remote changes to the system to cut heating and cooling costs. Target has not confirmed the accuracy of this report.

UPDATE (2/6/2014): Target Corporation announced they are fast tracking new credit card security technology in their stores, 6 months earlier than originally planned. Target's CFO announced it is moving up its goal to utilize chip-enabled smart cards, and now plans to have them in stores by early 2015. These cards encrypt point of sale data, rendering the credit card number less useful if stolen. Currently this technology is more prevalent outside of the US, but have resulted in lower card number thefts in other countries, notably Canada and the United Kingdom.

UPDATE (2/15/2014): The breach at the Target Corp. that exposed credit card and personal data on more than 110 million consumers appears to have begun with a malware-laced email phishing attack sent to employees at the HVAC contractor Fazio Mechanical in Sharpsburg Pennsylvania. According to Krebs on Security, "multiple sources close to the investigation now tell this reporter that those credentials were stolen in an email malware attack at Fazio that began at least two months before thieves started stealing card data from thousands of Target cash registers."

UPDATE (5/5/2014): Target's CEO has resigned in the wake of the data breach over the holiday season. He is claiming the breach was his fault. He is the second major executive to resign. Earlier in the year the company's Chief Technology Office resigned as well. The CFO of the company will take over as the interim CEO.

UPDATE (8/7/2014): Target has announced that the data breach will cost it's shareholders $148 million.

UPDATE (12/9/2014): A Minnesota ruled that a lawsuit put forth by several banks could proceed as the court stated that Target failed to adequately defend against the massive data breach they suffered. This is the first time a data breach case of this size has moved forward based on a companies failure to respond to warnings from security software/experts.


UPDATE (12/2/2015): Target will pay $39.4 million dollar settlement with banks and credit unions who filed a lawsuit against the retailer after the massive hacking event.


<table>
<thead>
<tr>
<th>Date</th>
<th>Information Source</th>
<th>Number of Records Exposed</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 12, 2013</td>
<td>inSync, Cottage Hospital, Cottage Health System Santa Barbara, California</td>
<td>MED DISC 32,755 (No Social Security numbers or financial information exposed)</td>
</tr>
</tbody>
</table>

A Cottage Hospital vendor removed an electronic security device without notifying Cottage Hospital. The removal may have exposed patient information. Patients treated at centers in Goleta, Santa Ynez, and Santa Barbara between September 29, 2009 and December 2, 2013 may have had their lab results, procedures performed, and other medical details relating to diagnosis exposed.

UPDATE (12/13/2013): Patient names, dates of birth, addresses, and health information may have been exposed.

UPDATE (12/15/2013): Cottage Hospital’s vendor was inSync.
At least seven employees of Boston Convention and Exhibition Center and 300 people who attended conventions during the fall may have been affected by a credit card breach. It is unclear how the credit card information may have been accessed and the exact dates when customers would have been vulnerable.

Information Source: Media

December 11, 2013
University of Iowa
Iowa City, Iowa

An employee called the University of Iowa's help desk after clicking a suspicious link in an email. It was discovered that the personal information and direct deposit information of over a dozen University of Iowa employees may have been exposed through compromised employee computers and accounts. At least two employees had an unspecified, but large amount of money stolen from their November paychecks. Two sets of phishing emails were sent to nearly 2,000 University of Iowa employees and the scam has been contained.

Information Source: Media

December 11, 2013
Los Angeles Gay & Lesbian Center
Los Angeles, California

A cyber attack caused the information of clients associated with the L.A. Gay and Lesbian Center to be affected between September 17, 2013 and November 8, 2013. Names, Social Security numbers, credit card information, dates of birth, contact information, medical information, and health insurance account numbers may have been exposed.

Information Source: California Attorney General

December 10, 2013
Office of Dr. Stephen Imrie
San Jose, California
MED PORT 8,900

Those with questions may call 1-888-407-4736.

The September 23 home burglary of a password-protected laptop and other items may have exposed patient information. The laptop contained patient first and last names, Social Security numbers, dates of birth, telephone numbers, surgical information, medical history, and other information related to patient records.

Information Source: California Attorney General

December 9, 2013
Southern Illinois University (SIU) HealthCare
Springfield, Illinois
MED PORT 1,891 (No Social Security numbers or financial information reported)

The loss or theft of a former SIU orthopedic surgeon's computer resulted in the exposure of patient information. The loss or theft was discovered on October 15. Information included patient names, dates of birth, admission dates, medical record numbers, diagnoses, procedural codes, and other health information from patients treated by Dr. Mark P. McAndrew.

Information Source: Media

December 6, 2013
B&G Foods North America, Inc., Maple Grove Farms
St. Johnsbury, Vermont
BSR HACK Unknown

Those with questions may call 1-888-887-3268 between 8:00 a.m. and 4:30 p.m., Eastern Time, Monday through Friday.

On November, 16, B&G Foods North America, Inc. discovered that an unauthorized party accessed Maple Grove Farms' website. Customers who made online purchases may have had their names, addresses, telephone numbers, and payment card numbers exposed.

Information Source: California Attorney General

December 6, 2013
Horizon Healthcare Services, Inc. (Horizon Blue Cross Blue Shield)
Sometime between November 1 and 3, two unencrypted laptops were stolen from employee workstations. The laptops were password-protected and cable-locked to the workstations. Names, Social Security numbers, addresses, dates of birth, Horizon Blue Cross Blue Shield New Jersey identification numbers, and demographic information may have been exposed. Almost 840,000 Horizon Blue Cross Blue Shield members were affected.

UPDATE (04/06/2015): A class action lawsuit was filed against Blue Cross Blue Shield of New Jersey of more than 830,000 members arguing that they were at risk of identity theft due to the data breach when stolen laptops were discovered that contained personal information, including Social Security numbers. The judge in the case dismissed the class action lawsuit claiming that since there was no evidence that the information on the laptops was used to create harm, the judge claimed there was no standing.

She also "dismissed a claim of economic injury brought by three of the plaintiffs who argued that their premiums should have provided for the security of their personal information. Citing precedent, Cecchi dismissed that claim as well, writing that the plaintiffs failed to demonstrate actual economic harm as a result of the breach."


---

A breach that involved keylogging software affected at least 93,000 websites. The virus may have originated on a server located in the Netherlands. It first started collecting passwords and usernames on October 21. Approximately 860 computers in the United States were affected. More than 99% of the computers that were affected were outside of the United States.

---

A breach at the Chicago Public Schools affected 2,000 people nationwide. Each state has a different number of residents who were affected.
The vision exam dates, diagnoses, dates of birth, genders, identification numbers, and school names of students were accidentally made available to the public online between June 18 and July 31, 2013. The breach was discovered on October 7 and the Chicago vision exam program information was removed. The information was viewed by 14 people during that time. All cached and archived versions of the information were also removed from the Internet.

Information Source: Databreaches.net

December 3, 2013 MadelynOregon Portland, Oregon BSR HACK 1,700

MadelynOregon’s website may have been accessed by unauthorized parties. The credit card transaction information of customers may have been accessed between mid-October and mid-November. Seven customers confirmed that they were affected by fraudulent credit card activity after making purchases on MadelynOregon’s website.

Information Source: Media

December 2, 2013 Board of Barbering and Cosmetology Sacramento, California GOV STAT Unknown

Those with questions may call 1-(866)-968-7797.

The August 23 office burglary of a desktop computer resulted in the exposure of sensitive information. Individuals who participated as models during cosmetology, barbering, manicure, esthetician, or electrology exams may have had their names, dates of birth, and California drivers’ license or identification card numbers exposed.

Information Source: California Attorney General


On December 2, 2013 the United States Fund for UNICEF discovered unauthorized access to one of the U.S Fund’s servers on or around November 4, 2013. The initial investigation by the agency showed only one server affected, however the personal information exposed included names, credit card numbers, credit card security codes, expiration dates of the cards, bank account numbers, phone numbers, and email addresses.

Information Source: Vermont Attorney General

November 29, 2013 University of Washington Medicine Seattle, Washington MED HACK 90,000

An employee at UW Medicine opened an email attachment that contained malicious software in early October. The malware affected the employee's computer and any information on the computer may have been compromised. Patient names, Social Security numbers, phone numbers, addresses, and medical record numbers may have been affected. Patients who were seen at UW Medicine dating back to at least 2008 could have had their information exposed. Notifications of the breach were sent at the end of November.

Information Source: Media

November 28, 2013 Florida Digestive Health Specialists Bradenton, Florida MED INSD 4,400

An employee was found to have improperly accessed and photographed patient records. The issue was discovered when the employee had the images printed at a store and a store employee reported the incident. Patient names, Social Security numbers, dates of birth, and phone numbers were exposed. The employee was fired and a criminal investigation has begun.

Information Source: Media

November 28, 2013 The Flamingo Resort and Spa Santa Rosa, California BSO HACK Unknown

Employees with questions may call 1-(800)-848-8300.
A virus was discovered on The Flamingo Resort and Spa payroll computer. Employee names, Social Security numbers, bank routing numbers for those who used direct deposit, dates of birth, phone numbers, and home addresses may have been exposed.

**Information**

**Source:**

**Media**

**November 28, 2013**  
**Orange County Anaheim Medical Center, Kaiser Foundation Hospital  
Anaheim, California**  
MED  PORT  Unknown

Patients with questions may contact Kaiser Permanente at 1(800)-443-0815.

A flash drive that contained patient information was discovered missing on September 25, 2013. It contained names, dates of birth, and medical record numbers.

**Information**

**Source:**

**PHIPrivacy.net**

**November 28, 2013**  
**Amos Medical Services  
Laurel, Maryland**  
MED  PHYS  Unknown

Amos Medical Services was charged with improper disposal of records after leaving patient records in a dumpster. The records were left behind when the office of Amos Medical Services moved within Laurel, Maryland. Amos Medical Services and their associated doctor agreed to pay $20,000.

**Information**

**Source:**

**PHIPrivacy.net**

**November 28, 2013**  
**CVS Pharmacy, Inc., Maryland CVS Pharmacy, LLC  
Gaithersburg, Maryland**  
MED  PHYS  Unknown

The Maryland Attorney General charged CVS Pharmacy, Inc. and Maryland CVS Pharmacy, LLC with failing to protect sensitive financial and medical information. CVS disposed of patient records in publicly accessible places. CVS agreed to pay $250,000 in a settlement with the Maryland Attorney General.

**Information**

**Source:**

**PHIPrivacy.net**

**November 27, 2013**  
**Maricopa County Community College District  
Phoenix, Arizona**  
EDU  UNKN  2.49 million

An unspecified data breach may have exposed the information of current and former students, employees, and vendors. Names, Social Security numbers, bank account information, and dates of birth may have been viewed by unauthorized parties.

**UPDATE** (12/02/2013): Student academic information may have also been exposed. The Maricopa County Community College District’s governing board will spend as much as $7 million to notify and offer credit monitoring to those who may have been affected.

**UPDATE** (12/07/2013): Estimations for the cost of the breach are as high as $14 million.

**UPDATE** (4/22/2014): Maricopa County Community College District waited seven months to inform 2.5 millions individuals (students, staff, graduates) of the security breach. The District is now in a class action lawsuit. The lawsuit claims that the “FBI warned the Maricopa County Community College District in January of 2011 that a number of its databases had been breached and made available for sale on the Internet”. It was also reported that “the district’s Information Technology Services employee also became aware of the security breach in January 2011, and repeatedly reported their findings to Vice Chancellor George Kahkedjian”.

**Information**

**Source:**

**Media**

**November 27, 2013**  
**University of Pittsburgh Medical Center  
Pittsburgh, Pennsylvania**  
MED  INSD  1,300

An employee was found to have accessed patient records without legitimate cause. The employee worked in a unit coordinator position for about a year and her supervisor was aware of the issue. Patient names, Social Security numbers, medical records, dates of birth, contact information, treatment information, and diagnosis information were accessed. The employee was fired.

**Information**

**Source:**

**Media**

**November 27, 2013**  
**California Employment Development Department**
Unemployment claim filing notices were sent to employers that contained information of people who had never been employed with them. An undisclosed number of people had their names and Social Security numbers mistakenly exposed. The issue was discovered when several employers notified EDD that some of the names and Social Security numbers did not match their records.

**UPDATE (11/22/2013):** The erroneous mailings occurred between September 14, 2013 and October 9, 2013.

**URM Stores**

**Spokane, Washington**

URM Stores is the wholesaler that processes electronic payments made by customers of Yoke’s Fresh Market, Rosauers, Super 1 Foods, Family Foods, Harvest Foods, CenterPlace Market, and Trading Co. Stores.

Customers with questions may call URM’s call center at 877-237-7408.

Washington banks and credit unions noticed fraudulent activity on the debit and credit cards of grocery store customers. The breach was traced to Yoke’s Fresh Markets, Rosauers stores, and other grocery stores associated with URM stores. The hacking incident occurred sometime between September and October. Customers were encouraged to use cash, check, or an alternative form of payment card processing to pay in stores until the breach was resolved.

**UPDATE (12/03/2013):** Over 24 stores in Montana and an unspecified number of stores in Oregon were also affected. URM believes the breach that allowed fraudulent copies of customer payment cards to be created has been contained. Customers were encouraged to check their bank statements after URM allowed normal payment card purchases to resume.

**Anthem Blue Cross**

**California**

The breach affected doctors across California.

The Social Security numbers and tax identification numbers of around 24,500 California doctors were accidentally posted in Anthem’s online provider directory. The information was available online at the end of October for about 24 hours.

**University of California, San Francisco (UCSF)**

**San Francisco, California**

The September 25 car theft of a physician’s laptop may have resulted in the exposure of patient information. The laptop may or may not have been encrypted and the physician is based in the Division of Gastroenterology at UCSF’s School of Medicine. Patient names, Social Security numbers, dates of birth, and medical record numbers were on the laptop.

**Crown Castle International Corp**

**Canonsburg, Pennsylvania**

Crown Castle determined on October 31 that their payroll information may have been accessed by hackers. Employee names, Social Security numbers, and compensation may have been exposed.

**Redwood Memorial Hospital**

**Fortuna, California**

An unencrypted flash drive from Redwood Memorial Hospital’s Cardiopulmonary Services Department was discovered missing on November 8. The flash drive had been missing since at least November 6 and contained patient names, report ID numbers, test indications, ages, heights, weights, test recording and analysis dates and times, facility and address where services were rendered, and clinical summaries of test findings. Some patients who were seen at Redwood Memorial Hospital between 2001 and 2013 may have had their information exposed.
The October 12 theft of a laptop resulted in the exposure of current and former employee information. Current and former employees of Clarity Media Group’s subsidiaries and of Freedom Communications were also affected. Names, Social Security numbers, mailing addresses, email addresses, phone numbers, dates of birth, salaries, and 401(k) balances were on the laptop. The dependents of employees may have also had their information exposed.

A hacker or hackers compromised some of the user accounts of GitHub. The hackers used a brute force attack to expose passwords. GitHub reset the passwords of users who were affected.

Sometime around April 11, 2013, Dr. Whisman learned of a breach that involved patient information on a computer recovered during an identity theft ring investigation. The patient information included full names, Social Security numbers, addresses, telephone numbers, dates of birth, and insurance plan information for patients who were seen in 1998 and 1999. The information likely came from a stolen computer and Dr. Whisman was encouraged to delay notification until the investigation was completed.

Two breaches in the summer of 2013 and November of 2013 resulted in the exposure of student information. The sensitive information that was exposed in July may have been accidentally exposed through an administrative error.

A second breach was discovered on November 8 when the Superintendent learned that student information had been posted on a publicly accessible webpage. The investigation of the November breach is ongoing. Student names and ID numbers were the primary types of data that were exposed in both incidents.

UPDATE (11/23/2013): A student of Sachem North High School pleaded not guilty to computer trespass and was released without bail. The student may have also accessed information in 2012. A list of 15,000 students’ information that dated back to the early 2000s was discovered online. A list of 130 students who received instructional services in an alternative setting in the 2010-2011 school year was also discovered online.
A July cyberattack resulted in the exposure of customer information. Customers were required to change their login credentials. It is unclear what kind of customer information was exposed.

**Information Source:**
Media

A group of hackers claimed responsibility for compromising usernames, emails, and passwords associated with MacRumors and vBulletin Forum. The hackers used a Zero Day exploit. A total of 860,000 MacRumors users were affected. It is unclear how many vBulletin Forum users were affected.

**Information Source:**
Media

Greencastle Community School Corporation notified parents of a security issue involving improper access by students. Several students from Greencastle High School found a list of student network passwords and were able to access a limited amount of confidential student files on the school network. Students in grades three through 12 may have had breakfast or lunch expenses falsely charged to their names and students with unauthorized access may have been able to access the network under other students’ accounts.

**Information Source:**
Media

A Dynacare Laboratory employee’s car was stolen on October 22. The car held a flash drive with employee names, Social Security numbers, addresses, dates of birth, and genders. Dynacare Laboratory is one of Froedtert Health Workforce’s contractors and Froedtert Health Workforce was handling health information for the City of Milwaukee Wellness Program. The City of Milwaukee Department of Employee Relations learned of the incident on November 15.

**UPDATE** (11/18/2013): A Dynacare laptop that contained no personal information was also in the employee’s car. The car and laptop were recovered; the flash drive remains missing.

**UPDATE** (11/21/2013): The City of Milwaukee filed a complaint against Dynacare with the Federal Office of Civil Rights.

**UPDATE** (11/29/2013): A total of 9,414 people were affected including about 6,000 city employees and 3,000 city employee dependents. The Milwaukee Professional Firefighters Association Local 215 was also affected and a lawsuit against Dynacare Laboratory and Froedtert Health was filed.

**Information Source:**
Media

The October 1 theft of a laptop resulted in the exposure of patient information.

**Information Source:**
HHS via PHIprivacy.net

The October 1 theft of a laptop resulted in the exposure of patient information.

**Information Source:**
HHS via PHIprivacy.net
A March 19 breach may have resulted in the exposure of patient information. The breach may have involved the theft of computer equipment, the unauthorized access of information on a computer, and/or paper records.

**UPDATE (12/20/2013):** A dishonest employee accessed names, Social Security numbers, addresses, dates of birth, driver's license numbers, passport numbers, physician names, diagnosis information, medical billing codes, bank account and routing numbers, and payment party names and payment information. Hospital for Special Surgery learned of the breach on May 31 and the dishonest employee was arrested in August.

### Information

**Source:**
HHS via PHIPrivacy.net

**November 15, 2013**

**Mount Sinai Medical Center**  
**New York, New York**

*GOV PORT*  
610 (No Social Security numbers or financial information reported)

The August 1 theft or loss of a portable electronic device resulted in the exposure of patient information.

### Information

**Source:**
HHS via PHIPrivacy.net

**November 15, 2013**

**Mount Sinai Medical Center**  
**New York, New York**

*MED PHYS*  
1,586 (No Social Security numbers or financial information reported)

Patient records were improperly disposed of on August 6.

### Information

**Source:**
HHS via PHIPrivacy.net

**November 15, 2013**

**Superior HealthPlan, Inc.**  
**Austin, Texas**

*MED DISC*  
6,284 (No Social Security numbers or financial information reported)

New Health and Human Services Commission ID numbers were sent on Superior ID cards to CHIP members on October 4. It was discovered that a computer error caused some Superior CHIP ID cards to be sent to incorrect addresses. Names, CHIP ID numbers, and doctors' names and phone numbers were exposed. All members who were affected were notified.

### Information

**Source:**
HHS via PHIPrivacy.net

**November 15, 2013**

**Group Health Cooperative**  
**Seattle, Washington**

*NGO DISC*  
1,015 (No Social Security numbers or financial information reported)

Group Health member identification numbers and chronic conditions were accidentally printed on the outside of letters that were mailed on September 16. The issue was discovered on September 23.

### Information

**Source:**
HHS via PHIPrivacy.net

**November 15, 2013**

**Rose Medical Center**  
**Denver, Colorado**

*MED PHYS*  
606 (No Social Security numbers or financial information reported)
Patient records were improperly disposed of sometime between June 28 of 2013 and July 16 of 2013.

**Information**  
**Source:** HHS via PHIPrivacy.net  
**November 15, 2013**  
**Lincoln Credit Center, National Debt Defense, SmartPath**  
**San Diego, California**  
BSF UNKN Unknown

Personal information related to client accounts may have been compromised at a physical location. The breach occurred sometime between October 20 and November 15. Lincoln Credit Center is monitoring client accounts for suspicious activity.

**Information**  
**Source:** California Attorney General  
**November 14, 2013**  
**Alta Bates Summit Medical Center, AverMedia Technologies**  
**Berkeley, California**  
MED INSD 115

Two women are accused of misusing the information of over 115 people in the Bay Area for identity theft purposes. At least 15 Alta Bates Summit Medical Center patients had their information misused and at least 35 had their information collected. The two women were arrested on November 5 and also had a payroll sheet from AverMedia Technologies in their possession.

**Information**  
**Source:** California Attorney General  
**November 13, 2013**  
**USI Insurance Services LLC**  
**Columbus, Ohio**  
BSF HACK Unknown

Malicious software was installed on the USI website on or around October 2, 2013. A hacker may have been able to view information stored in the USI system. Client names, usernames, passwords, and mailing addresses were exposed.

**Information**  
**Source:** California Attorney General  
**November 12, 2013**  
**Rotech Healthcare**  
**Orlando, Florida**  
MED PORT 10,680

On August 30, 2013 Rotech discovered that a former employee had taken employee files when her employment ended on November 26 of 2010. Rotech employees and their dependents may have had their names, Social Security numbers, addresses, and certain medical insurance information exposed. This medical information may have included the carrier that administered health care coverage, pharmacy services received, and other medical services received. The information was not removed with malicious intent and there has been no evidence of misuse.

**UPDATE** (12/16/2013): A total of 10,680 employees and their dependents were affected.

**Information**  
**Source:** PHIPrivacy.net  
**November 11, 2013**  
**City Jeffersonville**  
**Jeffersonville, Indiana**  
GOV DISC 311

City vendors and other businesses were alerted to a breach of information that dates back to 2001. Names, addresses, and in some cases Social Security numbers, were sent to city employees in a monthly email about vendor payments. The issue was noticed when a recent software change made the information easier to spot. Jeffersonville’s information technology staff deleted the emails from city employee inboxes.

**Information**  
**Source:** Media  
**November 11, 2013**  
**North Country Hospital and Health Center**  
**Newport, Vermont**  
MED INSD

550 (No Social Security numbers or financial information reported)

Patients with questions may call (802) 334-3253.
A former employee refused to return a laptop that contained unspecified patient health information. North County Hospital first learned of the issue on September 18. The Newport Police Department was contacted and all administrator-level computer system user codes and passwords that the employee had access to were changed. The laptop was also password-protected and will be remotely locked out if someone attempts to use it to access the Hospital systems.

Information Source: HHS via PHIPrivacy.net

November 11, 2013, New York City Police Department, New York City, New York

A former police detective pleaded guilty to paying hackers to steal passwords associated with the email accounts of other officers. The dishonest detective also misused the National Crime Information Center database to search for the information of at least two other NYPD officers. The breaches occurred between April of 2010 and October of 2012. The dishonest detective was charged with one count of conspiracy to commit hacking and one count of unauthorized access. The 30 or more people who were affected included 20 current and former NYPD officers. At least 43 email accounts and one cellular phone account were hacked.

Information Source: Media

November 11, 2013, St. Mary's Janesville Hospital, SSM Health Care, Janesville, Wisconsin

The August 27 car theft of an SSM Health Care employee's unencrypted laptop resulted in the exposure of patient information. Patients who were treated in St. Mary's Janesville Hospital's emergency room between January 1 and August 26 of 2013 were affected. Names, dates of birth, medical record numbers, account numbers, providers, departments of service, bed numbers, room numbers, dates and times of service, history of visits, complaints, diagnoses, procedures, test results, vaccines, and medications were exposed.

Information Source: PHIPrivacy.net

November 11, 2013, Discover Financial Services, Riverwoods, Illinois

An unspecified number of Discover customers had their account numbers changed and were issued a new card. It is unclear what type of security breach prompted the notification and when it may have occurred. Several customers in California received the notification letter; residents of other states may have been notified as well.

Information Source: California Attorney General

November 8, 2013, Standard Insurance Company, Portland, Oregon

One of Standard Insurance Company's vendors accessed a file that was inadvertently disclosed on the vendor's system. Names, Social Security numbers, addresses, and dates of birth could have been accessed between October 7 and October 18. The issue was discovered when an insurance policyholder noticed they had access to the information and contacted Standard Insurance Company.

Information Source: Media

November 8, 2013, Baltimore County, Baltimore, Maryland

A contractor who worked for Baltimore County between December of 2011 and July of 2012 was found to have saved the personal information of 12,000 county employees to computers for reasons unrelated to work. The information was discovered during an investigation in Florida and came from payroll files dated between January and March of 2007. Employees who had their paychecks direct deposited were affected and the bank account information of 6,633 employees was exposed. Baltimore county employees are no longer allowed to download personal information to county computers and more than 5,000 county hard drives will be cleared of related data.
Over 1,300 people who received payment from state hospitals had their information exposed online. Names, addresses, payment dates, name of facilities that made the payments, and dollar amounts paid were posted on North Carolina Department of Health and Human Services' transparency website "NC OpenBook." The error was discovered when an individual complained. The information had been available for years.

University of Chicago Physicians Group's former contractor ICS Collection Services discovered that website users were able to view sensitive information of other users. At least one user was able to view the names, addresses, dates of birth, insurance payments and dates, insurance company names, insurance policy numbers, procedures, diagnosis codes and descriptions, dates of service, treating physician names, and sometimes even Social Security numbers associated with University of Chicago Physicians Group patients. ICS Collection Services learned of the issue on July 9.

Those with questions may call (419) 222-5077.

The August 8 office theft of several computers resulted in the exposure of patient information. The computers contained names, Social Security numbers, addresses, and dates of birth that were encrypted. They also contained letters, reports, evaluations, and session notes that were not encrypted.

Good Samaritan Hospital learned that a laptop was missing on July 8. An investigation revealed on September 23 that the laptop contained data files related to patient pacemakers. Names, dates of birth, addresses, telephone numbers, and health insurance company names may have been exposed. Five patients had their Social Security numbers on the laptop. Only a fraction of patients who had their pacemakers checked between 1996 and July of 2013 were affected.

UPDATE (12/5/2014): "Rensselaer County has paid $25,000 in a court award and set aside $90,000 for expected legal fees in a flurry of lawsuits brought by jail officers and others whose medical information was viewed for years by employees using a computer in the jail nurses' office.

Seven parties, including four current or former correction officers, a jail employee, the family of a correction officer on behalf of a minor child, and a private individual have sued the county.

More suits are anticipated, officials have said.

Two cases have been settled."

More Information: http://www.timesunion.com/local/article/Cost-grows-for-medical-access-la...
The August 22 office theft of a computer resulted in the exposure of patient information. Names, dates of birth, age, gender, radiology images, radiation therapy dose planning, diagnoses, and Texas Health Presbyterian medical record numbers were on the computer.

Information
Source:
HHS via PHIPrivacy.net

November 8, 2013
Ferris State University - Michigan College of Optometry
Big Rapids, Michigan

Michigan College of Optometry learned on July 23, 2013 that their network had been compromised in December of 2011. A malware program could have accessed the names, Social Security numbers, demographic information, and a limited amount of clinical information of patients that were on the server. Former and current patients were mailed letters on September 24.

Information
Source:
HHS via PHIPrivacy.net

November 8, 2013
Comprehensive Podiatry LLC
Independence, Ohio

The August 3 theft of a laptop resulted in the exposure of patient information.

Information
Source:
HHS via PHIPrivacy.net

November 8, 2013
Access Counseling, LLC
Los Angeles, California

A briefcase was stolen from an employee’s car sometime between the evening of August 22 and the morning of August 23. The case files of seven clients were inside of the briefcase. Additionally, the briefcase contained a computer with files that included names, partial Social Security numbers, dates of birth, addresses, and clinical notes related to all clients.

Information
Source:
HHS via PHIPrivacy.net

November 8, 2013
BriovaRx
Chicago, Illinois

A breach of patient records occurred between July 3 and July 11 of 2013. In a breach that may be related, a former employee was sued for stealing confidential health information and trade secrets in October.

Information
Source:
HHS via PHIPrivacy.net

November 8, 2013
Region Ten Community Services Board
Charlottesville, Virginia

A hacker obtained the passwords to several employees’ emails on July 29. The email accounts may have contained the health information of patients.
November 8, 2013, Schuylkill Health System
Pottsville, Pennsylvania

The August 7 theft of a laptop resulted in the exposure of patient information.

November 8, 2013, Littleton Podiatry
Littleton, Colorado

The August 27 theft of a laptop resulted in the exposure of patient information.

November 8, 2013, Sierra View District Hospital
Porterville, California

A routine security audit at Sierra View District Hospital revealed that an employee had inappropriately accessed protected health information. An investigation revealed that the information was not disclosed externally. The breach occurred between July 1 and August 2.

November 7, 2013, DaVita
Denver, Colorado

The theft of an unencrypted laptop resulted in the exposure of patient and employee information. The laptop was stolen from an employee's vehicle and contained names, insurance information, diagnoses, and dialysis treatment information. Approximately 375 patients also had their Social Security numbers exposed.

November 7, 2013, Department of Economic Opportunity
Tallahassee, Florida

A glitch in the Department of Economic Opportunity's website caused Social Security numbers of people who registered for unemployment to be exposed. The information was mistakenly sent to businesses and the Department of Economic Opportunity alerted businesses to the issue. Those who were affected were sent letters.

November 7, 2013, Washington State University
Pullman, Washington

The October 11 theft of two external hard drives may have exposed the information of students, current employees, and former employees. Administrative and financial information such as Social Security numbers may have been exposed.
A dishonest employee accessed and misused patient information sometime between January of 2009 and March of 2012. Social Security numbers and dates of birth were taken to file fraudulent tax returns. The former employee pleaded guilty to one count of theft of government property and one count of aggravated identity theft.

A patient discovered a stack of unshredded medical documents in a publicly accessible dumpster near the medical offices on Samaritan Drive. Prescriptions, diagnoses, and other sensitive medical information could have been accessed. The breach occurred in July and an employee removed the information soon after the incident.

The Oregon Department of Consumer and Business Services fined Samaritan $1,000 for the breach. Samaritan will pay a full fine of $5,000 if it fails to comply with Oregon's confidential records laws during the next five years.

An unnamed contractor misplaced a University Hospitals hard drive after taking it for a computer system upgrade. The hard drive was stolen from the car of an employee of the contractor on August 8. It contained patient information such as names, birth dates, addresses, medical record numbers, insurance provider information, and health information.

Hackers stole and stored information online related to customers who used limousine and other ground transportation. The online information included plain text archives of credit card numbers, expiration dates, names, and addresses. Many of the customers were wealthy and used credit cards that would be attractive to identity thieves.

An employee was found to have accessed Social Security numbers, dates of birth, medical diagnoses, prescribed treatments, and other health information without cause. A patient contacted Boone Hospital Center on September 16 and said that her personal health information had been accessed. An investigation revealed the breach and the employee's access was terminated on September 19.

An employee's USB drive was discovered missing on September 3, 2013. It contained the names, Social Security numbers, and addresses or email addresses of current employees, applicants, and agency employees. A total of 33 people were affected.

UPDATE (12/04/2013): A second USB drive was also lost on August 30. A total of 739 Lebanon Center and Wheelock Terrace patients in New Hampshire were affected. Patient information included names, dates of birth, diagnoses, dates of admission or service, medical insurance identification information, and other medical information. At least 71 patients had their Social Security numbers on the USB drive.

UPDATE (12/16/2013): A total of 1,167 individuals were affected.
Information Source: Databreaches.net  
October 31, 2013  Milwaukee Public School District, Express Scripts  
Milwaukee, Wisconsin  
EDU DISC  6,000

Social Security numbers were printed on the outside of letters that were sent to a third party vendor. As many as 6,000 letters were sent to MPS Medicare D recipients.

Information Source: Media  
October 31, 2013  Paragon Benefits Inc, TSYS Employee Health Plan  
Columbus, Georgia  
BSO INSD  5,232

An employee of a temporary staffing agency who was working at Paragon Benefits Inc. emailed personal information to his own Gmail account for fraudulent purposes. The information came from TSYS employees. The dishonest employee was arrested and charged with felony identity theft. Two spreadsheets that contained names, Social Security numbers, dates of birth, and home addresses were sent. At least 1,000 TSYS former employees and 11 family members had their information exposed.

Information Source: Databreaches.net  
October 30, 2013  Ektron  
Nashua, New Hampshire  
BSO HACK  22

The June 15 hack of Ektron resulted in the exposure of current and former employee information. Names, Social Security numbers, immigration visas, passport numbers, and employee authorization cards were exposed. Ektron learned of the breach in July and hired a third party firm to investigate the scope of the breach in August.

Information Source: PHIPrivacy.net  
October 30, 2013  Florida Department of Health  
Orlando, Florida  
MED INSD  3,500

Patients who suspect fraudulent activity may call the Orange County Sheriff’s Office at (407) 253-7000. Patients with general questions may call the Department of Health at (407) 858-1490.

Two employees accessed a database of patient names, Social Security numbers, and dates of birth for the purpose of misusing the information to file tax returns. Police found a hand written list of 148 names and personal information when they searched the home of the alleged ring leader. Patients who were 17 and 18 years of age were targeted.

UPDATE (12/21/2013): The two women each pleaded guilty to one federal fraud charge related to accessing names, Social Security numbers, and dates of birth.

Information Source: PHIPrivacy.net  
October 30, 2013  Children’s Healthcare of Atlanta  
Atlanta, Georgia  
MED INSD  500 (No Social Security numbers or financial information exposed)

Children’s Healthcare of Atlanta fired and sued an executive for allegedly taking proprietary information that included patient health information, state license numbers for more than 500 health care providers, and other health care provider information. The executive announced her resignation on October 16 and on October 18 the Hospital discovered that she had emailed sensitive information to her personal email account. The executive had planned to leave on December 20 but was fired for exposing the Hospital’s sensitive information.

Information Source: PHIPrivacy.net  
October 30, 2013  Florida Department of Health  
Orlando, Florida  
MED INSD  2,300

Those with questions may call (407) 858-1490.

Two former employees used patient records to make lists of names, Social Security numbers, and dates of birth. The information was created for tax fraud purposes.
An investigation uncovered sensitive information from Emerald Garden and Tampa General Hospital patients. A dishonest Emerald Garden employee was arrested in May and sentenced to 37 months in prison for conspiring to misuse the information to file tax refunds. A contact at Tampa General Hospital also supplied patient information.

**Information Source:**

PHIPrivacy.net

---

**MongoHQ**  
**Mountain View, California**

MongoHQ's internal system was compromised. The system allowed certain administrative users to appear as other users. MongoHQ reset all employee accounts and will enable devices, email, and internal applications after a credential reset and audit.

**Information Source:**

Media

---

**Allina Health**  
**Minneapolis, Minnesota**

Roughly 3,800 patients were affected by a breach that involved a former employee at the Inver Grove Heights clinic. The employee worked as a certified medical assistant and viewed patient records without permission between February of 2010 and September of 2013. Patients who were seen at any location within Allina Health's system may have had their demographic, clinical, and health insurance information viewed. The employee also had access to the last four digits of patients' Social Security numbers.

**Information Source:**

Media

---

**HealthFitness, Gerdau**  
**Minneapolis, Minnesota**

Those who may have been affected may call (877) 371-7902.

HealthFitness informed Gerdau of a laptop theft that exposed the information of Gerdau employees and employee dependents. HealthFitness administers Gerdau's health management and wellness program. The laptop contained Social Security numbers, employee names, spouse names, dates of birth, and health plan elections.

**Information Source:**

PHIPrivacy.net

---

**Dun & Bradstreet**  
**Suwanee, Georgia**

A cyber attack occurred during the period between March and April 2013. Dun & Bradstreet hold information for business marketing and other businesses may have been affected.

**Information Source:**

California Attorney General

---

**NBC Sports Group**  
**Stamford, Connecticut**

Those with questions may call (203) 356-2720.

The August 24 theft of two laptops resulted in the exposure of personal information. The laptops were stolen in Northern California and it is unclear whether employees, clients, or general consumers were affected. Names, Social Security numbers, driver's licence numbers, and dates of birth were exposed.

**Information Source:**

Databreaches.net

---

**Michigan State University**  
**East Lansing, Michigan**

Michigan State University provided a notification here: [http://police.msu.edu/crimealert10202013.asp](http://police.msu.edu/crimealert10202013.asp)

An unauthorized user was able to modify employee banking information. The breach was discovered on October 18 when
two employees reported receiving email confirmations of changes to their direct-deposit designations. The unauthorized user may have obtained valid payroll credentials by using a phishing attack. The HR/Payroll systems were taken offline on Friday, October 18 and were expected to become active again on October 21.

Information Source: Media

October 25, 2013 Yusen Logistics (Americas) Inc.
Secaucus, New Jersey

An unencrypted laptop was stolen from an employee’s vehicle sometime around September 23. It contained a spreadsheet with payroll deduction information for former and current Yusen Logistics Americas employees. It contained names, Social Security numbers, addresses, and payroll benefit deduction amounts from the period of July 2013 to September 2013.

Information Source: California Attorney General

October 25, 2013 Mount Sinai Medical Center
Miami Beach, Florida

An employee who was working at Mt. Sinai Medical Center through a temp agency was found with patient information during a traffic stop. Police uncovered a bag that contained over 100 printouts with patient names, Social Security numbers, addresses, and dates of birth. Photocopies of checks that had been written to Mt. Sinai Medical Center and corresponding billing statements were also found during the February 27, 2013 traffic stop. Additional information that could be used for fraud was also found at the temporary employee’s residence.

The dishonest employee was convicted for involvement in the identity theft and tax refund scheme. It was later discovered that the temp agency gave Mt. Sinai Medical Center false background information about the temporary employee. Mt. Sinai Medical Center no longer does business with the staffing agency.

Information Source: PHIprivacy.net

October 23, 2013 University of Southern Maine
Portland, Maine

Someone broke into a University van and stole campus keys. The keys could give them access to nearly 50 Portland and Gorham campus buildings. The University is in the process of replacing locks of the affected buildings. Student, personnel, and other records may be accessible. Faculty, staff, and students were notified of the incident and encouraged to shut electronic devices down when leaving them unattended. They were also advised to not leave sensitive information or belongings in campus buildings without additional locks.

Information Source: Media

October 23, 2013 The Fisherman’s Restaurant, Radiant Systems
Fort Worth, Texas

Radiant Systems accidentally transmitted Fisherman’s Restaurant employee information to another Radiant Systems restaurant customer. The error occurred from May 3, 2013 through September 24, 2013. Radiant Systems learned of the issue on September 23 and notifications were sent in early October. Full names, Social Security numbers, dates of birth, gender, marital status and number of dependents, addresses, telephone numbers, and personnel information were exposed.

Information Source: California Attorney General

October 22, 2013 AHMC Healthcare, Inc.
Alhambra, California


The October 12 office theft of two laptops resulted in the exposure of patient information from a number of facilities. Authorities believe a well-known transient was responsible for the thefts. San Gabriel Valley Medical Center, Garfield Medical Center, Moneterey Park Hospital, Whittier Hospital Medical Center, Greater El Monte Community Hospital, and Anaheim Regional Medical Center patients were affected. Names, Social Security numbers, diagnosis and procedure codes, insurance identification numbers, and insurance payments were exposed.

Information Source: Media

October 22, 2013 AHMC Healthcare, Inc.
Alhambra, California

729,000 (about 73,000 Social Security numbers exposed)
The US Federal Trade Commission filed a complaint against Aaron’s over their practice of monitoring customer activity through software called Detective Mode. It was determined that customers who rented computers were put at risk for identity theft by Aaron’s practice of recording customer keystroke activity, screen shots, and images taken from webcams. Aaron’s may only use tracking technology with the consent of the renter and may not use technology that captures keystrokes, screenshots, images, or sounds on the devices it rents.

Information
Source: Media
records from this breach used in our total: 0

October 22, 2013
Aaron's
Atlanta, Georgia
BSR  DISC  Unknown

The clinic theft of a laptop on October 4 resulted in the exposure of patient information. The stolen laptop contained names, Social Security numbers, addresses, phone numbers, dates of birth, Seton medical record numbers, patient account numbers, diagnosis information, immunization information, and insurance information of patients who visited the Seton Total Health Partners program, Seton McCarthy, Seton Topfer, and Seton Kozmetsky community health centers.

Information
Source: Media
records from this breach used in our total: 5,500

October 22, 2013
Seton McCarthy Clinic, Seton Healthcare Family
Austin, Texas
MED  PORT  5,500

Between October 2010 and December 2012, Court Ventures, a public records aggregator, provided access to US Info Search data to a foreign criminal posing as a legitimate private investigator.

Court Ventures had a contract with US Info Search where customers of Court Ventures had access to US Info Search data which included records on more than 200 million Americans, including individuals' Social Security numbers, dates of birth, and other records.

Experian purchased the assets of Court Ventures in March 2012, and the criminal's access to the US Info Search data was shut down in December 2012. Experian has publicly stated that no Experian databases were breached in this situation.

UPDATE (3/10/2014): According to Krebs on Security, in March 2014, Hieu Minh Ngo pled guilty to running an identity theft business called Superget.info out of his home in Vietnam. Ngo posed as a private investigator when he contracted with Court Ventures to gain access to consumer records. Ngo was then able to provide access to the US Info Search database to his clients.

Krebs on Security states, "The government alleges that the service's customers used the information for a variety of fraud schemes, including filing fraudulent tax returns on Americans, and opening new lines of credit and racking up huge bills in the names of unsuspecting victims. The transcript shows government investigators found that over an 18-month period ending Feb.2013, Ngo's customers made approximately 3.1 million queries on Americans."

Krebs adds, "That means that if Ngo's clients conducted 3.1 million individual queries, the sheer number of records exposed by Ngo's service is likely to have been many times that number - potentially as many as 30 million records."


UPDATE (2/23/2015): The total number of records indicated here has been changed to 3.1 million by PRC to reflect the approximate number of records queried by Ngo's customers according to the court transcript. [This 3/10/14 UPDATE was amended on 2/23/15 to include additional content from the Krebs on Security blog post of March 10, 2014, related to the Court Ventures breach.]

UPDATE (7/15/2015): Hieu Minh Ngo, the Vietnamese man who perpetrated an online identity theft service and had access to personal information on more than 200 million Americans was sentenced to 13 years in a U.S prison

UPDATE (7/21/2015): A class action lawsuit has been filed against Experian as a result of their subsidiary, Court Ventures, allowed access to personal information of individuals by one individual who posed as a private investigator.

"The suit alleges that Experian negligently violated consumer protection laws when it failed to detect for nearly 10 months that a customer of its data broker subsidiary was a scammer who ran a criminal service that resold consumer data to identity thieves."

Read more regarding the suite here: http://krebsonsecurity.com/wp-content/uploads/2015/07/Experian-Ngo-Compl...

More Information: http://krebsonsecurity.com/2015/07/experian-hit-with-class-action-over-i...

Information
Source: Media
records from this breach used in our total: 3,100,000

October 21, 2013
RGV DME (Durable Medical Equipment)
McAllen, Texas
MED  INSD  Unknown

Three people were sentenced to prison for their roles in a scheme to defraud Medicare and Medicaid. Two of the people...
owned RGV DME and a third worked for them. Between early 2004 and late 2011, the three submitted fraudulent claims to Medicare and Texas Medicaid for DME supplies.

Information
Source: PHIPrivacy.net

October 19, 2013 Hospice of the Chesapeake
Pasadena, Maryland

An employee emailed spreadsheets with sensitive patient information to a personal account in order to work from home. Names, ages, dates of service, diagnoses, and medical record numbers were in the spreadsheets. The breach was discovered on August 8 and initially suspected to have been caused by a computer intrusion. Hospice of the Chesapeake investigated the breach for two months before revealing it to patients.

UPDATE (11/08/2013): Hospice of the Chesapeake notified HHS and stated that 7,035 patients were affected.

Information
Source: Media

October 18, 2013 Broward Health Medical Center
Fort Lauderdale, Florida

Federal and local officials discovered a breach that involved the records of 960 patients treated at Broward Health between October of 2012 and December of 2012. The patients were treated at 1600 S. Andrews Ave. Their names, addresses, dates of birth, insurance policy numbers, and reasons for visits were exposed when an employee took patient documents out of the medical facility. The last four digits of patients’ Social Security numbers are recorded at Broward Health for insurance purposes and were also exposed.

Information
Source: Media

October 18, 2013 BW Arthritis and Rheumatology, Good Samaritan Hospital, MedStar Health Inc,
Padder Health Service, LLC
Glen Burnie, Maryland

Four people face charges related to misusing patient information to make more than $750,000 of fraudulent purchases. At least two of the people worked at medical offices and at least one had direct access to a health care database. One of the dishonest employees worked at Paddar Health Service between June of 2010 and February of 2012 and at BW Arthritis and Rheumatology between February of 2012 and February of 2013. Another dishonest employee worked at Good Samaritan Hospital from July of 2008 to July of 2010.

Information
Source: Media

October 18, 2013 Long Island Rail Road
Long Island, New York

Ticket vending machines associated with Long Island Rail Road were discovered to have been compromised. Customers who used their debit and credit cards at the machines may have had their information recorded and used to create fraudulent payment cards. Tiny cameras were placed on the machines and hidden in thin black strips. A total of seven machines in Bayside, Garden City, Great Neck, Greenvale, and Merillon Avenue were compromised.

Information
Source: Media

October 17, 2013 California State University Sacramento (Sacramento State University)
Sacramento, California

In August, Sacramento State University was notified that a computer server had been hacked. It contained the Social Security numbers, driver’s license numbers, and other personal information of staff members. The cause and extent of the breach were determined in late September and staff members were notified in mid-October.

Information
Source: Media

October 17, 2013 Datapak Services Corporation
Howell, Michigan

Those with questions may call (855) 398-6434
Datapak Services discovered that its online systems had been infected by malware since March 5, 2013. Customer names, addresses, payment card numbers, expiration dates, and CVV codes may have been accessed by an unauthorized party.

<table>
<thead>
<tr>
<th>Date</th>
<th>Source</th>
<th>Information</th>
</tr>
</thead>
</table>
| October 17, 2013 | Databreaches.net | **University of Arizona**  
**Tucson, Arizona**  
EDU HACK 9,080  
A July 29 breach of the University of Arizona’s College of Law website allowed intruders to access class rosters and applicant lists. University of Arizona law students and applicants may have had their names, Social Security numbers, usernames, and passwords exposed. |
| October 17, 2013 | Media           | **Ouidad**  
**Danbury, Connecticut**  
BSR HACK Unknown  
Hackers were able to access Ouidad’s customer database between June 30 and July 4 of 2013. Ouidad account information, names, credit card numbers, credit card security codes and expiration dates, billing addresses, email addresses, and phone numbers were exposed. |
| October 17, 2013 | Media           | **Eagleton School, Castro School, Munroe School**  
**Morrison, Colorado**  
MED PORT 100 (No Social Security numbers or financial information reported)  
The theft of a nurse’s suitcase resulted in the exposure of student medical information. The suitcase contained a thumb drive. The theft occurred on October 5 and about 100 parents received notification of the breach. Medications and other health-related information were on the thumb drive. Addresses and Social Security numbers were not included in the compromised data. |
| October 16, 2013 | PHIprivacy.net  | **Memorial Hospital of Lafayette County, Healthcare Management System**  
**Darlington, Wisconsin**  
MED DISC 6,000 (No Social Security numbers or financial information exposed)  
Memorial Hospital of Lafayette learned on August 6 that some patients had their financial statements sent to other people. The mistake was caused by an error in the settings of an unnamed third-party billing vendor’s system. Patients who were seen at the hospital as far back as 2001 may have had their information sent to the wrong address. Patient names, addresses, identification numbers, account numbers, dates of services, and the charges associated with services received were exposed. UPDATE (11/08/2013): The billing vendor was Healthcare Management System. |
| October 13, 2013 | PHIprivacy.net  | **PR Newswire**  
**New York, New York**  
BSO HACK Unknown  
Customer usernames and encrypted passwords were accessed and taken by hackers on or after March 8, 2013. Hackers may have had access to the news release services of companies that use PR Newswire. The breach is related to the Adobe hack that was revealed in early October of 2013. |
| October 12, 2013 | Media           | **Gordon Supply Company**  
**Glenside, Pennsylvania**  
BSF HACK 400  
A woman found two bags of personnel records in her backyard in mid-August. The woman called the cops after
discovering the sensitive information. Social Security numbers, driver’s license photos, addresses, phone numbers, medical information, dates of birth, emergency contacts, payroll history, and tax documents were exposed. The breach occurred after the building was abandoned and the files were not checked before being discarded. An estimated 400 people were affected.

Information
Source: Media
October 11, 2013 Google Chrome Mountain View, California

A data management firm discovered that Chrome browser users may have had their personal information stored on the hard drives of their computers without their knowledge or consent. Google Chrome regularly stores names, street addresses, email addresses, phone numbers, bank account numbers, credit card numbers, and Social Security numbers in web browsers for later use. It was not known that Chrome’s cache also stores the information in plain text.

Information
Source: Media
October 11, 2013 Hope Family Health Westmoreland, Tennessee

The August 4 theft of an unencrypted laptop from an employee’s home may have resulted in the exposure of patient information. Current and former patients may have had their names, Social Security numbers, dates of birth, and billing addresses exposed. The information came from financial records, patient account information, and billing records dating back to 2005.

Information
Source: Media
October 11, 2013 Monterey County Department of Social Services Salinas, California

A Monterey County computer was compromised during the evening of March 17. It was connected to the California State Network and contained the information of individuals who received public assistance benefits through Monterey County Department of Social Services between 2002 and 2009. First and last names, Social Security numbers, addresses, phone numbers, and dates of birth were exposed.

Information
Source: Media
October 11, 2013 Sentara Healthcare, Sentara Virginia Beach General Hospital Virginia Beach, Virginia

Two dishonest nurse aides gathered information from at least 12 patients in order to file fraudulent tax returns. The breach occurred between September of 2011 and April of 2013. Some of the patients were from Sentara Virginia Beach General Hospital. The nurses’ aides were indicted on charges of conspiracy to defraud the government.

Information
Source: PHIprivacy.net
October 10, 2013 Nordstrom Aventura, Florida

Six skimmers were found on registers in one Nordstrom store in Aventura. Six people were seen tending to the devices on the afternoon of October 5. They came in groups of three and distracted sales people while tampering with the registers, twice. Skimmers and tiny cameras were installed to collect credit card information. The information can be used to make fraudulent credit cards.

Information
Source: Media
October 10, 2013 Petrochem Insulation, ASRC Energy Services San Francisco, California

The July 18 theft of a laptop from an employee’s car resulted in the exposure of employee information. The laptop contained personnel spreadsheets with employee names, Social Security numbers, and employee identification numbers.

Information
Source: Media
October 10, 2013 NHC Healthcare Oak Ridge, Tennessee

Those with questions may call (888) 568-8578.
An unencrypted backup tape was discovered missing. It contained the names, Social Security numbers, dates of birth, home addresses, and medical information of patients.

### Information Source: Databreaches.net

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Type</th>
<th>Records from this breach used in our total:</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 10</td>
<td><strong>City of Wichita - Electronic Procurement Website</strong> Wichita, Kansas</td>
<td>GOV</td>
<td>29,000</td>
</tr>
<tr>
<td></td>
<td>Hackers accessed the city of Wichita's electronic procurement website.</td>
<td>HACK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Current and former vendors who had worked with the city and employees who</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>had been reimbursed for expenses since 1997 were affected. Social</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security numbers, taxpayer ID numbers, and bank account information may</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>have been exposed.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**UPDATE** (11/22/2013): This breach was a result of the Dun & Bradstreet Credibility Corp. breach. Nearly 29,000 local vendors and employers were affected by the hacking incident that occurred during the weekend of October 5.

### Information Source: Media

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Type</th>
<th>Records from this breach used in our total:</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 10</td>
<td><strong>Legal Aid Society of San Mateo County</strong> Redwood City, California</td>
<td>NGO</td>
<td>Unknown</td>
</tr>
<tr>
<td></td>
<td>The August 12 office burglary of 10 laptops resulted in the exposure of</td>
<td>PORT</td>
<td></td>
</tr>
<tr>
<td></td>
<td>client information. The laptops were used by Legal Aid Society attorneys</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>to assist individuals in getting services. Names, Social Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>numbers, dates of birth, medical information, and health information</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>may have been exposed.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Information Source: California Attorney General

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Type</th>
<th>Records from this breach used in our total:</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 9</td>
<td><strong>Minnesota Counties Insurance Trust</strong> St. Paul, Minnesota</td>
<td>BSF</td>
<td>3,000</td>
</tr>
<tr>
<td></td>
<td>An employee working as a child support officer is accused of making</td>
<td>INSD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>more than 4,000 queries without legitimate cause in a driver and vehicle</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>services database between 2010 and 2011. Photographs, addresses, and</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>driving records may have been exposed.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**UPDATE** (10/04/2013): A $2 million settlement has been proposed to end a class action lawsuit. An insurance trust representing Minnesota counties will pay $500 to the named plaintiffs who initially brought the suit and those who had their information viewed for illegitimate purposes will receive a share of the money "based on the number of times they were illegitimately searched."

### Information Source: Media

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Type</th>
<th>Records from this breach used in our total:</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 9</td>
<td><strong>University of California San Francisco Medical Center (UCSF)</strong> San</td>
<td>MED</td>
<td>3,541</td>
</tr>
<tr>
<td></td>
<td>Francisco, California</td>
<td>PORT</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A total of 3,541 patients were affected by the September 10 theft of an</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>unencrypted laptop from an employee's vehicle. A subset of the 3,541</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>patients who were affected had their Social Security numbers exposed.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**UPDATE** (10/08/2013): Paper documents with patient names, Social Security numbers, dates of birth, and medical information were also stolen.

### Information Source: Media

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Type</th>
<th>Records from this breach used in our total:</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 9</td>
<td><strong>Holy Cross Hospital</strong> Fort Lauderdale, Florida</td>
<td>MED</td>
<td>9,900</td>
</tr>
<tr>
<td></td>
<td>Nearly 9,900 former Holy Cross Hospital patients were affected by a</td>
<td>INSD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>breach that involved a dishonest employee filing fraudulent tax returns.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Names, Social Security numbers, dates of birth, and addresses were</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>exposed between November 2011 and August 2013.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Information Source: Media

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Type</th>
<th>Records from this breach used in our total:</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 9</td>
<td><strong>All Source Medical Management, Scottsdale Dermatology Clinic</strong></td>
<td>MED</td>
<td>1,456</td>
</tr>
</tbody>
</table>

171
An employee of All Source Medical Management was arrested on suspicion of stealing the credit card information of multiple patients. The dishonest former employee later admitted to using patient address and credit card numbers to make fraudulent purchases with a co-conspirator. It is unclear if other clinics and hospitals were affected.

**UPDATE** (12/16/2013): A total of 1,456 patients were affected. The data was stolen sometime between January 1, 2013 and October 4.

**Information**

**Source:** PHIPrivacy.net

---

A former employee removed paper copies of daily patient schedules from Rothman Institute on August 11. The paper copies were taken without permission and were not used for malicious purposes. Patients who were seen between March 18 and May 10 may have had their names, telephone numbers, dates of birth, locations, staff or physician seen, codes for insurance companies, copay amounts, dates and times of appointments, reasons for visits, and internal-use chart, and code numbers exposed. Social Security numbers and credit card information were not exposed. The information was not shared with unauthorized parties.

**UPDATE** (11/08/2013): A total of 2,350 patients were affected.

**Information**

**Source:** Media

---

On August 8, Saint Louis University learned that about 10 employees had their direct deposit information changed after several malicious phishing emails were sent to employees on July 25. About 20 phishing emails were sent and several employees provided their account information. No unauthorized transactions have occurred because of the email scam. Additionally, patients who were treated or reviewed at facilities owned by the Tenet Healthcare Corporation or SSM Health Care may have had their information exposed.

**Information**

**Source:** Media

---

A number of sales agents were affected when a data backup of PayJunction's internal business system was inappropriately accessed. The unauthorized access occurred in July and was discovered in late September.

**Information**

**Source:** Databreaches.net

---

A breach at a Walgreens in Anaheim resulted in the exposure of customer information. Thieves stole a computer and paper records in December of 2012. The theft was discovered on December 31 and occurred on December 28. The burglary occurred in Crescent's billing center. Names, Social Security numbers, addresses, phone numbers, health insurance information, dates of birth, and medical information were exposed.

**Information**

**Source:** Media

---

An email with patient information was sent to an unauthorized person. Names, dates of birth, addresses, diagnoses, and medications were exposed.
Hackers obtained the customer information of nearly 3 million Adobe customers who used Photoshop, InDesign, Premiere, and other Adobe software products. Customer IDs, encrypted passwords, names, encrypted credit or debit card numbers, expiration dates, and other information related to customer orders were exposed. Anyone who bought software directly from Adobe’s website is advised to change their Adobe account passwords.

UPDATE (10/11/2013): Hackers kept the source code on a hidden, but unencrypted server.

UPDATE (10/21/2013): A second breach related to the initial one in early October caused Adobe to reset client passwords.

UPDATE (11/20/2013): Around 42 million passwords for the Australian-based online dating service Cupid Media were also found on the same server that contained stolen Adobe, PR Newswire, and National White Collar Crime Center information.

UPDATE (11/25/2013): Some estimate that 152 million Adobe ID accounts were in a file that began circulating the internet in late October. Adobe Systems Inc has encountered delays in trying to notify all customers of the issue since it was discovered 10 weeks ago.

The June 27 car theft of a laptop resulted in the exposure of customer information. Names, Social Security numbers, addresses, and bank account information were exposed.

An unencrypted backup tape was discovered missing. It contained patient names, Social Security numbers, dates of birth, home addresses, and medical information.

A programming error that occurred on July 11, 2013 allowed 34 visitors to PLS Financial Services’ website to view the names, Social Security numbers, addresses, and email addresses of PLS Financial Services customers. The error was discovered on July 26 and quickly fixed.

On July 3, Bell Helicopter learned that some people who attended Bell Helicopter Training Academy were receiving phishing emails from a source claiming to be Bell. It appears that Bell’s database of attendee information was accessed by a cyber intruder. Attendees may have had their email addresses and credit card numbers exposed.
The California Public Utilities Commission launched an investigation into the unauthorized disclosure and publication of Comcast subscribers' unlisted names, telephone numbers and addresses to determine whether Comcast violated the laws, rules, and regulations of California.

**UPDATE (8/25/2014):** An evidentiary hearing has been scheduled in this case for September 2014 to investigate whether or not Comcast broke the law.

<table>
<thead>
<tr>
<th>Information Source</th>
<th>October 3, 2013</th>
<th>Windhaven Investment Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government Agency</td>
<td>Boston, Massachusetts</td>
<td>BSF Hack 419</td>
</tr>
<tr>
<td>Windhaven Investment discovered a breach of their server in August of 2013. Client names, account numbers, custodians, investment positions, and other account information may have been accessed by an unauthorized party. The breach may have occurred earlier than August. At least 419 New Hampshire residents were affected. The total number of people affected nationwide was not revealed.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Information Source</th>
<th>October 3, 2013</th>
<th>Mercy Health Systems, Allscripts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Databreaches.net</td>
<td>Baltimore, Maryland</td>
<td>MED STAT 25 (No Social Security numbers or financial information reported)</td>
</tr>
<tr>
<td>Mercy Health Systems discovered a breach of their server in August of 2013. Client names, account numbers, custodians, investment positions, and other account information may have been accessed by an unauthorized party. The breach may have occurred earlier than August. At least 419 New Hampshire residents were affected. The total number of people affected nationwide was not revealed.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Information Source</th>
<th>October 3, 2013</th>
<th>Tri-State Surgical Associates</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHIPrivacy.net</td>
<td>Elkton, Maryland</td>
<td>MED INSD 433</td>
</tr>
<tr>
<td>An unauthorized staff member provided a physician with the information of 433 patients on July 18. The information included names, Social Security numbers, addresses, phone numbers for home and work, dates of birth, sex, languages spoken, employers, emergency contacts, emergency phone numbers, emergency contact relationship, guarantor information, and insurance information.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Information Source</th>
<th>October 2, 2013</th>
<th>Santa Clara Valley Medical Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media</td>
<td>San Jose, California</td>
<td>MED PORT 571 (No Social Security numbers were exposed)</td>
</tr>
<tr>
<td>The theft of an unencrypted laptop from the audiology department of Santa Clara Valley Medical Center resulted in the exposure of patient names, medical record numbers, dates of birth, ages, sex, dates of service, and brainwave tests. The theft was discovered on September 16.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Information Source</th>
<th>October 2, 2013</th>
<th>UnityPoint Health</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media</td>
<td>West Des Moines, Iowa</td>
<td>MED INSD 1,800 (less than 180 Social Security numbers exposed)</td>
</tr>
<tr>
<td>Those with questions may call (877) 223-3817.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A breach was discovered on August 8 during the course of a routine audit. It was discovered that a contractor accessed UnityPoint's EMR system without a legitimate reason. An employee gave computer passwords to an employee of another
company that provides care to patients. Names, medical insurance account numbers, home addresses, dates of birth and other health information was accessed between February of 2013 and August of 2013.

Information
Source: PHIPrivacy.net
Records from this breach used in our total: 180

October 1, 2013  **R.T. Jones Capital Equities Management Inc.**
St. Louis, Missouri
BSF  HACK  800

R.T. Jones learned of a cyber attack that occurred on July 22, 2013. On August 7, 2013, it was discovered that an unauthorized party was able to access a database that contained names, Social Security numbers, and dates of birth. At least 800 people were affected in Maryland. It is unclear how many were affected nationwide.

Information
Source: Media
Records from this breach used in our total: 800

October 1, 2013  **McHenry County College, Ellucian**
Crystal Lake, Illinois
EDU  DISC  Unknown

McHenry County College's software vendor Ellucian accidentally sent the personal information of current and former McHenry County College students and staff to three other junior colleges. Social Security numbers and other information were sent to Morton, Prairie State, and Triton.

Information
Source: Media
Records from this breach used in our total: 0

October 1, 2013  **JP Morgan Chase**
New York, New York
BSF  DISC  Unknown

JP Morgan Chase customers received a privacy notification in early September. A labeling error caused the Social Security numbers of customers to be printed on the outside of the notification letter. A lawsuit was filed against JP Morgan Chase on behalf of affected customers. The lawsuit claims that JP Morgan did not immediately notify its customers and should have prevented the breach from happening. The case is Alexander Furman et al v JP Morgan Chase & Co et al, No. 13-cv-06749, U.S. District Court, Northern District of Illinois.

Information
Source: Media
Records from this breach used in our total: 0

October 1, 2013  **Atlanta Center for Reproductive Medicine**
Atlanta, Georgia
MED  DISC  654 (No Social Security numbers or financial information reported)

Atlanta Center for Reproductive Medicine became aware of a breach on July 12. The breach involved email and it is not clear exactly how patient information was exposed or what type of information was involved.

Information
Source: HHS via PHIPrivacy.net
Records from this breach used in our total: 0

October 1, 2013  **Accountable Care Organization of Puerto Rico, Inc. (ACO of Puerto Rico), PHM Healthcare Solutions**
San Juan, Puerto Rico
MED  UNKN  5,000 (No Social Security numbers or financial information reported)

A breach that involved either unauthorized access to ACO of Puerto Rico's network or an unintentional disclosure of patient information online occurred between March 5 and July 16 of 2013.

Information
Source: HHS via PHIPrivacy.net
Records from this breach used in our total: 0

October 1, 2013  **Dermatology Associates of Tallahassee**
Tallahassee, Florida
MED  UNKN  916

A breach caused the exposure of patient information: Dermatology Associates of Tallahassee notified patients on September 4. Patient names, Social Security numbers, addresses, and dates of birth were compromised. It is unclear how the breach occurred.

Information
Source:
September 30, 2013  The New Teacher Project  
Brooklyn, New York  

NGO  PORT  Unknown

The July 27 or 28 office theft of an unencrypted laptop resulted in the exposure of current and former employee information. Names, Social Security numbers, dates of birth, and employee ID numbers were exposed.

Information Source: Databreaches.net

September 30, 2013  Sentry Life Insurance, Department of Labor  
Stevens Point, Wisconsin  

BSF  DISC  Unknown

Sentry Life Insurance discovered that several forms sent to the Department of Labor contained an attachments with names, Social Security numbers, and in a few cases, 401k account balances. The Department of Labor uploaded the forms to a public website before Sentry’s discovery. The discovery was made on July 2 and a letter was sent on July 11 to the Maryland Attorney General’s Office on behalf of Sentry.

Information Source: Databreaches.net

September 30, 2013  Denny’s  
Phoenix, Arizona  

BSR  PHYS  200

Job applications from a Denny’s in Phoenix were found in a dumpster behind the Denny’s. The paperwork dated back to August of 2012. The information included addresses, Social Security numbers, and other information normally found on job applications. The manager said there was a mistake and that similar paperwork is usually shredded.

Information Source: Databreaches.net

September 28, 2013  Virginia Polytechnic Institute and State University (Virginia Tech)  
Blacksburg, Virginia  

EDU  HACK  144,963 (No Social Security numbers or financial information reported)

The University’s statement can be found here: http://www.vtnews.vt.edu/articles/2013/09/092413-hr-hrserver.html

The computer server of Virginia Tech’s Department of Human Resources was accessed on August 28. The information of people who applied online to Virginia Tech between 2003 and 2013 may have been accessed. No Social Security numbers or financial information was exposed. A total of 16,642 job applicants had their driver’s license numbers exposed. The remaining job applicants had not submitted this information.

Information Source: Media

September 28, 2013  State Farm  
Bloomington, Illinois  

BSF  INSD  687 (11 customers confirmed affected)

State Farm became aware of fraudulent charges on a customer’s credit card a few days after the card was used to pay for insurance policies. A former employee at an after-hours call center was found to have misused the credit card information of at least 11 customers. The dishonest employee had also worked with 687 other customers.

Information Source: Media

September 28, 2013  ICG America (Amazing Clubs, Games2U, Flying Noodle, Monster Brew, Texas Irons, California Reds)  
Austin, Texas  

BSO  HACK  Unknown

ICG America learned that its payment processing system was the target of a cyber attack. The attack began on January 2, 2013 and continued until August 2, 2013. Customers who made purchases from companies operated by ICG America may have had their names, credit card and debit card numbers, expiration dates, CVV codes, addresses, and email addresses exposed.

Information Source: Media

September 28, 2013  Unique Vintage  
Burbank, California  

BSR  HACK  Unknown
A breach letter can be found here: https://oag.ca.gov/system/files/Customer%20Notification%20Letter%20%2892312rv%292_0.pdf

Unique Vintage's website was accessed by malware between January of 2012 and September 14, 2013. Customer names, emails, credit card numbers, and phone numbers may have been accessed.

Information
Source: California Attorney General
September 26, 2013
LexisNexis, Dun & Bradstreet, Kroll Background America
Short Hills, New Jersey
BSO HACK Unknown

Hackers were able to access an underground database of stolen consumer information. It was discovered that the network was set up to receive information from internal systems at several large data brokers. LexisNexis was one of the data brokers that was affected and discovered that their networks may have been compromised for at least five months. Dun & Bradstreet discovered that their systems had been compromised as far back as March 27, 2013. The breach of Kroll Background America, Inc. had began as far back as June 2013.

UPDATE (11/26/2013): Kroll Background America informed California that 548 California residents were affected by the breach.

Information
Source: Media
September 23, 2013
Columbia University Medical Center (CUMC)
New York, New York
MED DISC 407

An Excel file with the names and Social Security numbers of 407 medical students was accidentally attached to an email that was sent to medical students interested in a residency match list. The Excel column that contained the Social Security numbers was hidden and still accessible. The issue was discovered in March for the 2013 list and it was later discovered that the same issue had occurred in 2008 and 2009.

Information
Source: Databreaches.net
September 23, 2013
Stanford University
Stanford, California
EDU HACK Unknown

Stanford University ID holders (SUNet) users had their account passwords and other information exposed. The breach occurred sometime during the summer of 2013 and continued into the fall. The full extent of the breach was not revealed. SUNet users were instructed to change their passwords before accessing the system again.

Information
Source: Media
September 23, 2013
Summit Community Care Clinic
Frisco, Colorado
MED DISC 921 (No Social Security numbers or financial information reported)

An administrative error led to the exposure of patient email addresses. Email addresses were placed in the visible "TO:" field instead of the blind "BCC:" field. The email was an invitation to a monthly patient advisory meeting and was sent on July 22.

Information
Source: HHS via PHIprivacy.net
September 20, 2013
Murphy USA
Little Rock, Arkansas
BSR CARD Unknown

Murphy USA stations in Conway Arkansas and Durant, Oklahoma were also affected. It is unclear if this is related to the breach that occurred at Murphy USA gas stations in 2011 in Virginia.

Two men pleaded guilty to one count each of conspiracy to commit wire fraud. They placed skimming devices on gas pumps at Murphy USA station in Conway and Little Rock, Arkansas as well as Durant, Oklahoma. This allowed them to collect credit card information and create fraudulent credit cards. The breach occurred between April 2012 and January 2013 and led to fraudulent charges of about $400,000. It's estimated that between 50 and 500 people were affected.

Information
Source: Media

Customers who placed an order online or by phone between March 1, 2013 and July 15, 2013 may have had their information exposed. Customer names, debit and credit card numbers, addresses, phone numbers, expiration dates and CVV codes may have been accessed by hackers.

Information Source: Media

September 19, 2013  DiscountMugs.com (BEL USA LLC)
Medley, Florida  BSR  HACK  Unknown

A curious resident entered an abandoned building that used to be Edgewater Hospital and found a room filled with thousands of patient records. A local news team investigated and found that photos had been taken of the situation four years earlier in 2009 by the Illinois State Health Department. The records included patient names, Social Security numbers, dates of birth, and addresses. Edgewater Hospital had been abandoned for more than a decade.

Information Source: PHIPrivacy.net

September 18, 2013  Logan Community Resources, Inc.
South Bend, Indiana  MED  UNKN  2,900 (No SSNs or financial information reported)

An August 24, 2012 breach resulted in the exposure of patient information.

Information Source: HHS via PHIPrivacy.net

September 18, 2013  Minne-Tohe Health Center/Elbowoods Memorial Health Center
New Town, North Dakota  MED  UNKN  10,000 (No SSNs or financial information reported)

An October 1, 2011 breach resulted in the exposure of protected health information.

Information Source: HHS via PHIPrivacy.net

September 18, 2013  St. Francis Health Network, Advantage Health Solutions
Indianapolis, Indiana  MED  UNKN  2,575 (No SSNs or financial information reported)

Advantage Health Solutions and St. Francis Health Network (Franciscan Alliance ACO) were affected by a breach.

Information Source: HHS via PHIPrivacy.net

September 15, 2013  International SOS Assistance, Inc.
Philadelphia, Pennsylvania  GOV  HACK  Unknown

An unauthorized user or users accessed at least one U.S. system that hosts traveler information. The type of information that may have been accessed was not reported and International SOS is still investigating the incident.

UPDATE (10/23/2013): The breach occurred on August 24 and was confirmed on August 28. Names and passport numbers were exposed. Some travelers also had their Social Security numbers exposed.

Information Source: Media

September 13, 2013  MNsure
St. Paul, Minnesota  MED  DISC  2,400

An agency employee accidentally sent the information of 2,400 insurance agents to two other MNsure employees via email. MNsure instructed the employees to delete the information. Names, Social Security numbers, and addresses were part of the breach.

UPDATE (12/12/2013): It was also discovered that the health insurance exchange has vulnerabilities that may allow
hackers to see information travelling between a user's computer to the MNsure website.

Information
Source: Argotec
Media
September 13, 2013
Argotec
Greenfield, Massachusetts
BSR UNKN Unknown

An unspecified incident occurred on or around July 26 that may have exposed the confidential information of current and former employees. Names, Social Security numbers, and bank account information may have been exposed. Current employees were sent notification on August 6.

Information
Source: Media
September 11, 2013
Edgewood Partners Insurance Center (EPIC)
San Mateo, California
BSF PORT Unknown

Five laptops were stolen during a July 16 office burglary. The laptops contained confidential information and were password-protected but unencrypted. Current and former employees and their beneficiaries and dependents, contractors, and job applicants were affected. Names, Social Security numbers, addresses, dates of birth, drivers' license numbers, benefits information, bank account information, and health information were exposed.

Information
Source: Media
September 11, 2013
Kaiser Permanente
Oakland, California
MED DISC Unknown

Participants in a Wellness Screening competition pilot may have had their information exposed. A Kaiser Permanente employee accidentally included confidential information in an email sent to a member of the pilot planning team. In addition to a summary of the competition, it included names, Kaiser Permanente medical record numbers, phone numbers, email addresses, names of employers, department names, and dates and times of health screenings. The pilot planning team member was not authorized to receive the confidential information.

Information
Source: California
Attorney General
September 11, 2013
FSV Payment Systems, Paymast'r Services
Boulder, Colorado
BSF HACK Unknown

Between July 22 and July 28, an unauthorized party accessed a website that contained sensitive information. Names, Social Security numbers, addresses, drivers' license numbers, and Payroll Card numbers may have been accessed. The website was shutdown once the breach was discovered. Paymast'r Services, PaycheckPLUS! Payroll cards issued by MetaBank were affected.

Information
Source: California
Attorney General
September 10, 2013
Pierce County Housing Authority
Tacoma, Washington
BSO DISC 979

A human error resulted in the exposure of client information. A client found a file with Social Security numbers on the website. The site was shut down while the file was removed. It is unclear how long the information was available and the error was caused by a former employee. Those with questions may call (888) 829-6550.

A website breach exposed an unspecified number of customer names, addresses, credit card numbers, credit card expiration dates, and CVV codes. Hackers put malware on Outdoor Network’s Boats.net and Partzilla.com websites and were able to access information from credit card transactions between December 2012 and July 2013.

Information
Source: Media
September 10, 2013
Outdoor Network, LLC, Boats.net, Partzilla.com
Lake Placid, Florida
BSR HACK Unknown

Those with questions may call (888) 829-6550.

A website breach exposed an unspecified number of customer names, addresses, credit card numbers, credit card expiration dates, and CVV codes. Hackers put malware on Outdoor Network’s Boats.net and Partzilla.com websites and were able to access information from credit card transactions between December 2012 and July 2013.

Information
Source: Media
September 10, 2013
University of South Florida (USF) Health
Tampa, Florida
EDU INSD 140
Police searched the car of a University custodial employee and found USF Physicians Group patient billing information. Names, Social Security numbers, and dates of birth had been exposed. The employee no longer works for the University and patients were sent a notification letter in late July.

Information Source: Media

September 10, 2013
TrendNet
Torrance, California
BSR HACK

The FTC case can be found here: http://www.ftc.gov/os/caselist/1223090/130903trendnetorder.pdf

FTC fined TrendNet for having inadequate security practices and marketing their products to consumers as secure. TrendNet’s website was breached by a hacker or hackers. This allowed them to bypass users’ login credentials and access wireless camera feeds. At least 700 people who purchased TrendNet security cameras had their live camera feeds hacked. Some of their feeds were published online by hackers.

Information Source: Media

September 7, 2013
Rockland Federal Credit Union
Rockland, Massachusetts
BSF HACK Unknown

Those with questions may call 781-878-0232.

Rockland Federal Credit Union is sending customers new debit cards with new PINs as a result of a merchant who discovered a breach in their computer system. All old debit cards will be deactivated on September 26.

Information Source: Media

September 6, 2013
Georgia Department of Labor
Marietta, Georgia
GOV DISC 4,457

An employee accidentally emailed a document with the names and Social Security numbers of 4,457 Cobb-Cherokee Career Center customers to 1,000 people. Recipients were notified and instructed to delete the email immediately without reading it.

UPDATE (09/06/2013): The employee who accidentally sent the email attachment was suspended. The Georgia Department of Labor is also reviewing its internal policies for handling sensitive information.

Information Source: Media

September 6, 2013
Office of Dr. Hankyu Chung
San Jose, California
MED PORT 2,182 (No Social Security numbers or financial information reported)

A June 17 office burglary resulted in the theft of two laptops. One of the laptops contained names, telephone numbers, dates of birth, visit dates, health complaints, physical examination notes, diagnoses, testing information, medication information, and other medical record information. The thief or thieves were able to get into the office by opening an unlocked door. No identity theft protection services are being offered to affected patients.

UPDATE (11/08/2013): HHS received a report stating that 2,182 patients were affected by the breach.

Information Source: California Attorney General

September 6, 2013
Conexis, State of Virginia
Blacksburg, Virginia
EDU DISC 13,000

Employees of the state of Virginia who are enrolled in the Commonwealth's 2014 Flexible Spending Account had their information exposed. Conexis erroneously sent summary reports of Blue Cross/Blue Shield Flexible Spending Account Services to 11 state human resources and payroll employees. The reports included participants from across the state rather than from specific locations related to the human resources and payroll employees’ work. The human resources and payroll employees who received information that was not intended for them signed a certification confirmation that they had deleted or destroyed the information.
Information Source: Media
September 6, 2013  James A. Haley Veterans Hospital
Tampa, Florida

A volunteer allegedly stole the names and Social Security numbers of 106 patients and used the information to file $550,000 worth of fraudulent tax returns. The volunteer had a co-conspirator and the breach began in late January of 2012.

Information Source: Media
September 6, 2013  Illinois Department of Healthcare and Family Services
Springfield, Illinois

A contractor sent Family Health Network ID cards to the wrong addresses in July of 2013. A total of 3,100 clients had their names, Medicaid numbers, and dates of birth exposed.

Information Source: Media
September 5, 2013  Medical University of South Carolina (MUSC), Dreyer Medical Clinic, Blackhawk Consulting Group
Charleston, South Carolina

A hacker from outside of the United States accessed customer information from Blackhawk Consulting Group, a credit card processing vendor. The information included financial information from customers who paid the Medical University of Southern Carolina with a credit card online or over the phone between June 30 and August 21. No patient information was accessed. Some of Blackhawk Consulting Group’s other customers were affected and a total of 10,000 people may have had their information exposed.

UPDATE (09/09/2013): Specifically, names, billing addresses, email addresses, payment card numbers, expiration dates, and CCV2 numbers were exposed by a Blackhawk Consulting Group hack in August.

Information Source: Media
September 5, 2013  Boston Public School (BPS), Plastic Card Systems
Boston, Massachusetts

Boston Public School students across 36 schools may have had their information compromised by the loss of a flash drive. The flash drive was misplaced sometime around August 9 by BPS’s ID card vendor Plastic Card Systems.

Information Source: Media
September 5, 2013  North Texas Comprehensive Spine and Pain Center
Sherman, Texas

A former employee stole an external hard drive that contained the medical information of patients. There has been no evidence that the information on the hard drive was improperly used.

UPDATE (09/15/2013): Close to 3,000 patients were notified of the potential breach. Names, Social Security numbers, dates of birth, addresses, and diagnoses were exposed.

Information Source: Media
September 3, 2013  InterContinental Mark Hopkins San Francisco
San Francisco, California

A July 4 burglary resulted in the exposure of guest information. The names, addresses, email addresses, phone numbers, and credit and debit card numbers of guests were on a computer hard drive that was stolen. The hotel learned of the possibility of a breach of guest data on July 14 and alerted guests around August 8.
Patients with questions may call 800-524-7262 extension 1575.

The July 29 car burglary of a laptop computer and flash drive resulted in the exposure of patient information. Patient names, dates of birth, and other information contained in medical records were exposed.

Information
Source: Media

A website breach that occurred on June 1 and was discovered on July 22 resulted in the exposure of customer information. Names, addresses, phone numbers, unencrypted credit card information, and other information stored on temporary data files may have been accessed due to malicious code on the website.

Information
Source: Media

Seven contract baggage handlers were arrested for stealing valuables from customer luggage. The thefts were caught on camera between April 1 and August 28. Items such as iPads, iPhones, cash, and jewelry were discovered in the defendants’ homes and cars.

Information
Source: Media

Customer information may have been exposed when Osprey Packs’ Pro Deal website was hacked. Customer names, phone numbers, email addresses, billing and shipping addresses, and credit card information may have been exposed. Osprey Packs learned of the issue on August 7, 2013 when a customer discovered unauthorized activity on their credit card and connected it to Osprey Packs. Other customers have also noticed fraudulent charges. The attack may have happened as early as July 9, 2013.

Information
Source: Media

Those with questions may call Olson & White at 855-479-9542.

The July 22 office theft of several computers resulted in the exposure of patient health information. Names, addresses, X-rays, photos, and diagnostic findings were exposed.

UPDATE (09/04/2013): Two desktops were stolen. Social Security numbers were also exposed.

Information
Source: Media

Anyone who has shopped at Harbor Freight within the last three months (June, July, and August of 2013) may be at risk for credit or debit card fraud. Online and in store customers were affected. Tens of thousands of dollars were taken from between 300 and 600 member accounts.

UPDATE (11/04/2013): Customers who made purchases in stores between May 6, 2013 and June 30, 2013 may have had their card account numbers, expiration dates, and card verification numbers exposed.

Information
Source: Media
An unencrypted laptop that was housed in a locked closet was discovered missing on August 2. The computer contained names, dates of birth, medical record numbers, and hand and arm image data taken between February 2010 and July 13. The laptop had not been used since July 19.

Information Source: Media

August 29, 2013 Republic Services Phoenix, Arizona

An unspecified number of current and former employees were affected by the theft of a laptop. The laptop was stolen from an employee’s home on August 10. The laptop contained names and Social Security numbers.

UPDATE (09/03/2013): As many as 82,160 current and former employees may have been affected.

Information Source: Media

August 29, 2013 LabMD Atlanta, Georgia

An FTC complaint states that a LabMD spreadsheet with insurance billing data of over 9,000 customers was discovered on a public file sharing network. Social Security numbers, insurance information, medical treatment codes, and dates of birth were exposed by the cyber security issue. Identity thieves were found to have acquired the personal information of at least 500 LabMD customers.

UPDATE (11/15/2013): LabMD disputed the FTC probe and alleged that the government funded the breach to retaliate against LabMD.

Information Source: Media

August 29, 2013 Midwest Supplies Roseville, Minnesota

Customer names, addresses, email addresses, phone numbers, credit card numbers, expiration dates, and security codes may have been exposed after Midwest Supplies' website was hacked. All affected customers were offered a $25 coupon for future purchases.

Information Source: Media

August 28, 2013 Advocate Medical Group, Advocate Health Park Ridge, Illinois

The July 15 office theft of four unencrypted desktop computers resulted in the exposure of patient information. Approximately four million patients who were seen by Advocate Medical Group physicians between the early 1990s and July of 2013 were affected. Names, Social Security numbers, addresses, and dates of birth were exposed. Diagnoses, medical record numbers, medical service codes, and health insurance information was also exposed in some circumstances.

UPDATE (09/06/2013): A class-action lawsuit on behalf of patients in the Chicago area has been filed. It claims that Advocate Medical Center should have done more to protect patient information.

Information Source: Media

August 28, 2013 Missouri Credit Union Columbia, Missouri

A file with customer information was accidentally published on Missouri Credit Union’s website on August 5. The names, Social Security numbers, account numbers, teller and call in passwords, and addresses of Missouri Credit Union members were accessed. The file was accessed 10 times before the issue was discovered and it was taken off of the website.

Information Source: Media

August 28, 2013 Washington Inventory Service Merriam, Kansas

A box of hundred of employee records was found in a publicly accessible recycling dumpster. The box was later recovered by an employee, but the records were still left behind.
August 28, 2013  **Office of Janna Benkelman**  
**Denver, Colorado**  

Patients with questions may call 303-805-7168.

An office burglary resulted in the exposure of patient information. A laptop was stolen from the office of Janna Benkelman, a licensed professional counselor. The laptop was password-protected.

---

August 28, 2013  **Infocrossing Inc, MO HealthNet, Missouri Department of Social Services**  
**Jefferson City, Missouri**  

An error by Infocrossing, Inc. caused the personal information of a group of patients to be mailed to incorrect addresses. The incident was discovered on June 6, 2013 and impacted correspondence sent between October 16, 2011 and June 7, 2013. Names, dates of birth, MO HealthNet identification account numbers, county names, phone numbers, and the last four digits of Social Security numbers were exposed.

**UPDATE** (09/23/2013): The breach was originally thought to have affected fewer than 2,000 individuals and last between 2011 and 2013. The Missouri Department of Social Services reported that the breach began when information was sent out in December of 2009. More than 25,000 Missouri residents were affected.

---

August 28, 2013  **Brookdale University Hospital and Medical Center**  
**Brooklyn, New York**  

The May 24 loss of a portable device resulted in the exposure of patient information.

---

August 28, 2013  **Standard Register, Brookdale University Hospital and Medical Center**  
**Brooklyn, New York**  

The exposure of patient paper records resulted in a breach that was reported in August 2012.

---

August 28, 2013  **Health Plus Amerigroup, Brookdale University Hospital and Medical Center**  
**Brooklyn, New York**  

An accidental exposure of protected health information affected patients. The information was accidentally disclosed to other facilities. The breach was reported in September of 2012.

---

August 28, 2013  **Young Family Medicine Inc.**  
**Sidney, Ohio**  

The June 12 theft of a laptop resulted in the exposure of patient information.
A domain or domains belonging to The New York Times was attacked after activist hackers found a way to access the login credentials of service provider Melbourne IT. Melbourne IT is an Australian domain name registrar that provides hosting and data services for The New York Times and other media sites. The New York Times website was shutdown for approximately six hours.

Information
Source: Media
August 27, 2013 The New York Times, Melbourne IT
New York, New York
BSO HACK Unknown

185
August 22, 2013  United Shore Financial Services, Shore Mortgage  Troy, Michigan  BSF  HACK  Unknown

The servers of an unnamed Shore Mortgage vendor were affected by a computer intrusion. The incident may have begun on June 2 and client information was accessed on August 15. Names, Social Security numbers, contact information, dates of birth, drivers' license information, and financial account information were accessed.

Information  
Source:  
California Attorney General  

August 21, 2013  Hope Community Resources (HCR)  Anchorage, Alaska  MED  DISC  3,700 (No Social Security numbers or financial information reported)

The health information of disabled patients was accidentally released in an email on the night of August 19. A survey was sent via email to supporters of HCR. The email also contained names, dates of birth, guardians and parents, addresses, and other patient information.

Information  
Source:  
Media  

August 21, 2013  Emory University  Atlanta, Georgia  EDU  HACK  Unknown

Anyone with an Emory University netID/username is being advised to change their account password due to a breach. Emory University stated that it appears the attack on their information technology infrastructure is similar to attacks that similar organizations have seen in the past few months. Emory University also stated that it does not appear that sensitive information was accessed.

Information  
Source:  
Media  

August 20, 2013  League of Legends, Riot Games  Santa Monica, California  BSO  HACK  120,000

A security breach has resulted in the usernames, email addresses, first and last names, and encrypted passwords of League of Legends users to be exposed. About 120,000 transaction records from 2011 may have been accessed. The transaction records contained hashed and salted (encrypted) credit card numbers. The information was stored on a system that had not been used since 2011.

Information  
Source:  
Media  

August 16, 2013  Exelixis  San Francisco, California  BSR  PORT  Unknown

The theft of one or more pieces of company electronic equipment exposed client information. The theft was discovered on July 30 and names, Social Security numbers, financial account numbers, addresses, and dates of birth may have been exposed.

Information  
Source:  
California Attorney General  

August 16, 2013  U.S. Department of Energy  Washington, District Of Columbia  GOV  UNKN  104,000 (5,711 confirmed)

An unspecified security incident caused the personal information of current and former employees to be exposed. No classified data was lost.

UPDATE (08/30/2013): An August 29 memo revealed that the system that was hacked was called DOEInfo. A total of 2,539 current employees and 3,172 former employees were affected. Names, Social Security numbers, and dates of birth were exposed.

UPDATE (09/03/2013): Approximately 53,000 current and former federal employees, employee dependents and contractors had their information exposed. The incident occurred in July of 2013.

UPDATE (10/22/2013): The Department of Energy revised the number of affected current and former employees to 104,000.

UPDATE (12/13/2013): Up to 150,000 employees may have been affected.
UPDATE (12/17/2013): A federal audit revealed that the Department of Energy had received warnings about the security of its information systems, yet failed to act.

Information Source: Media

August 16, 2013 Ferris State University
Big Rapids, Michigan
EDU HACK 62,000 (39,000 Social Security numbers)

An unauthorized person gained access to the school’s computer network. Campus ID numbers, names, and possibly other information of staff and students were exposed. In addition to the 39,000 people who had their files with Social Security numbers exposed, 19,000 more individuals were notified of the breach.

UPDATE (10/22/2013): It is estimated that 62,000 people were affected and $380,000 was spent investigating the breach. This number includes providing services to those who were affected.

Information Source: Media

August 16, 2013 California Correctional Health Care Services
Sacramento, California
MED INSD 1,001 (No SSNs or financial information reported)

Missing dental information was discovered to have been removed by a staff member. Patient names, dates of birth, dental treatment plans, and other information were exposed. Dental records may have also been taken. The documents were first discovered missing on June 19 and had not been recovered as of August 16.

UPDATE (08/28/2013): A total of 1,001 inmates were affected.

Information Source: California Attorney General

August 16, 2013 California Department of Corrections and Rehabilitation, Centinela State Prison
Imperial, California
MED DISC Unknown

A file containing staff names, Social Security numbers, and dates of birth was saved to a Centinela State Prison server that was accessible to all staff. It was on the server between July 26 and July 29 before being removed.

Information Source: California Attorney General

August 15, 2013 Harris County
Harris, Texas
GOV HACK 16,000

The information of current and former Harris County employees was found on electronic files in Vietnam. Names, Social Security numbers, and dates of birth were exposed. The files were from 2005 and 2007 and appear to have been created before Harris County put in place stricter identity theft regulations.

Information Source: Media

August 14, 2013 Michigan Department of Community Health, Michigan Cancer Consortium
Lansing, Michigan
MED HACK 49,000

A server for the Michigan Cancer Consortium that housed names, Social Security numbers, dates of birth, cancer screening test results, and testing dates was hacked. The Michigan Department of Community Health claimed that the breach should not fall under strict HIPAA regulations because testing records, rather than medical records, were affected.

Information Source: Media

August 13, 2013 Caledonia Home Health and Hospice
Saint Johnsbury, Vermont
MED PORT Unknown

The theft of an employee’s Netbook on July 20 resulted in the exposure of patient information. The Netbook was stolen from the employee’s home and contained Social Security numbers and other protected patient information.

Information Source: Media
August 12, 2013  **Income and Capital Growth Strategies Inc.**  
Van Nuys, California  
BSF   HACK   Unknown  

An employee was the target of a computer network intrusion sometime between July 12 and July 15. Information about clients and their dependents may have also been exposed. Names, Social Security numbers, addresses, dates of birth, drivers' license numbers, and bank account information may have been accessed.

**Information Source:**  
California Attorney General  

August 11, 2013  **Resources for Human Development, Inc. (RHD)**  
Philadelphia, Pennsylvania  
MED   INSD   40  

At least 40 residents of RHD had their information sold for fraudulent purposes by a dishonest RHD employee. The former employee was part of a bank fraud conspiracy that involved fraudulent tax refunds and bank fraud. The former employee was sentenced to three years in prison and three years of supervised release for aggravated identity theft and bank fraud.

**Information Source:**  
PHIPrivacy.net  

August 9, 2013  **Smartphone Experts**  
Inverness, Florida  
BSR   HACK   Unknown  

A hacker was able to access the computer system Smartphone Experts used to process online payments on June 13. Customer names, addresses, credit and debit card account numbers, CVV codes, and payment card expiration dates were accessed. The credit card information was encrypted, but the hacker may have used a decryption feature within the online payment processing system to access customer information.

**UPDATE (09/06/2013):** The breach occurred on June 13. This entry originally listed it as having occurred on July 12.

**Information Source:**  
California Attorney General  

August 9, 2013  **Auburn University - School of Forestry and Wildlife Sciences**  
Auburn, Alabama  
EDU   DISC   Unknown  

Spreadsheets with donor and alumni information were accidentally uploaded to a publicly accessible server after an administrative error. The error was discovered on June 19 and Auburn’s IT office removed the information. Names, Social Security numbers, maiden names, mailing addresses, first year at Auburn, graduation year, alumni status, email addresses, and phone numbers were exposed.

**Information Source:**  
Databreaches.net  

August 9, 2013  **Northrop Grunman**  
Suwanee, Georgia  
BSO   HACK   70,000  

People who were linguists or applied to be linguists within Northrop Grunman Technical Services, inc. Balkans Linguist Support Program may have had their personal information exposed. A database that contained names, Social Security numbers, dates of birth, blood types, contact information, and additional types of government-issued identification numbers was accessed by unauthorized parties. The breach occurred sometime between November 2012 and May 2013 and was discovered on July 26.

**UPDATE (08/15/2013):** Over 70,000 people, including thousands of linguists, were affected.

**Information Source:**  
Media  

August 8, 2013  **US Airways Group**  
Tempe, Arizona  
BSO   HACK   7,700  

US Airways customers with Divident Miles accounts may have had their information compromised. Dates of birth, security question answers, last four digits of credit card numbers, and frequent-flier miles may have been accessed and compromised.

**UPDATE (08/02/2013):** Names, email addresses, and Known Traveler numbers were exposed. in some cases mileage was stolen from the accessed accounts.

**Information Source:**  
Media  

August 8, 2013  **M2ComSys, Cogent Healthcare, Inc.**  
Brentwood, Tennessee  
MED   DISC   32,000
Cogent Healthcare offices across the country, Cogent Medical Care, Endion Medical Healthcare (Endion SeniorCare), Parkview Community Hospital Medical Center, Inpatient Specialists of Southwest Florida, and Comprehensive Hospital Physicians of Florida were affected.

M2ComSys (M2), a medical transcription company, stored physicians' notes for Cogent Healthcare. It was discovered that the online system that stored the notes could be accessed. Patient care notes with names, physician names, dates of birth, diagnosis descriptions, summary of treatment, medical history, medical record numbers, and other medical information were exposed. The notes could have been accessed on May 5, 2013 and improper access to the site ended on June 24, 2013. M2 no longer provides services for Cogent Healthcare.

**UPDATE** (9/17/2013): At least 32,000 patients were affected across all medical centers.

<table>
<thead>
<tr>
<th>Information Source</th>
<th>California Attorney General</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 7, 2013</td>
<td>Retinal Consultants Medical Group (Vitreo-Retinal Medical Group)</td>
</tr>
<tr>
<td>Sacramento, California</td>
<td>MED PORT</td>
</tr>
<tr>
<td></td>
<td>1,837 (No SSNs or financial information reported)</td>
</tr>
</tbody>
</table>

The theft of a laptop resulted in the exposure of patient information. The laptop was stolen from the medical group's offices sometime between June 5 and June 6. Patient names, dates of birth, gender, race, and medical images were exposed.

**UPDATE** (08/28/2013): The breach affected 1,837 patients.

<table>
<thead>
<tr>
<th>Information Source</th>
<th>Media</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 2, 2013</td>
<td>Medtronic</td>
</tr>
<tr>
<td>Fridley, Minnesota</td>
<td>MED PHYS</td>
</tr>
<tr>
<td></td>
<td>2,764</td>
</tr>
</tbody>
</table>

A box of training records went missing from a Medtronic facility in Minnesota. Most of the records dated back to 2008. People who received training in using insulin pumps or continuous glucose monitoring devices may have been affected. A limited number of patients had their Social Security numbers exposed. Those who may have been affected were notified in early July.

<table>
<thead>
<tr>
<th>Information Source</th>
<th>PHIPrivacy.net</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 2, 2013</td>
<td>Clark Memorial Hospital</td>
</tr>
<tr>
<td>Jeffersonville, Indiana</td>
<td>MED DISC</td>
</tr>
<tr>
<td></td>
<td>1,087 (No SSNs or financial information reported)</td>
</tr>
</tbody>
</table>

A third-party mailing error resulted in the exposure of patient health information. Billing statements with names, dates of service, insurance information, billing information, and financial status were mailed to incorrect addresses.

<table>
<thead>
<tr>
<th>Information Source</th>
<th>Media</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 1, 2013</td>
<td>Bridgewater Associates, LP, Ceridian</td>
</tr>
<tr>
<td>Westport, Connecticut</td>
<td>BSF DISC</td>
</tr>
<tr>
<td></td>
<td>Unknown</td>
</tr>
</tbody>
</table>

An unauthorized individual accessed a database of employee information used for COBRA. Names, Social Security numbers, dates of birth, addresses, and other benefit plan information of employees and their dependents may have been accessed on the Ceridian database. The breach was discovered when a Bridgewater consultant reported that their password for the Ceridian database had been changed and someone else had used the credentials to access the database on three separate occasions. The breach occurred sometime before April 12, 2013.

<table>
<thead>
<tr>
<th>Information Source</th>
<th>PHIPrivacy.net</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 31, 2013</td>
<td>Rocky Mountain Spine Clinic</td>
</tr>
<tr>
<td>Lone Tree, Colorado</td>
<td>MED INSD</td>
</tr>
<tr>
<td></td>
<td>532</td>
</tr>
</tbody>
</table>

An employee in the billing department was fired for sending sensitive patient information to their personal email. The incident occurred in June and it does not appear that the email was sent with malicious intent.

<table>
<thead>
<tr>
<th>Information Source</th>
<th>Media</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 31, 2013</td>
<td>South Central Los Angeles Regional Center</td>
</tr>
<tr>
<td>Los Angeles, California</td>
<td>MED PORT</td>
</tr>
<tr>
<td></td>
<td>Unknown</td>
</tr>
</tbody>
</table>
The July 6 theft of an employee’s vehicle resulted in the exposure of client information. The stolen car contained an iPad with client names and UCI numbers.

**Information**

**Source:**
California Attorney General

**July 31, 2013**  
**Fidelity Investments, Oracle**  
**Redwood, California**

BSF DISC Unknown

Current and former Oracle employees may have had their 401(k) information viewed by a plan administrator at the firm of another Fidelity client. Names, Social Security numbers, compensation, and other 401(k) savings and investment plan information was briefly viewed by accident. The issue was discovered on July 10, 2013.

**Information**

**Source:**
California Attorney General

**July 30, 2013**  
**US Airways, McKesson, City of Houston, Automatic Data Processing (ADP), AlliedBarton Security Services**  
**Tempe, Arizona**

BSO DISC 4,500

A programming error at ADP resulted in the exposure of employee names, Social Security numbers, and other information on W-2 forms. Employees could have inadvertently downloaded the W-2s of other employees. The error was corrected on May 4 and involved W-2 forms for tax years 2010, 2011, and/or 2012. ADP alerted US Airways to the issue on June 6, 2013.

**UPDATE** (09/13/2013): McKesson and the city of Houston were also affected by the breach.

**UPDATE** (09/30/2013): AlliedBarton Security Services was also affected. It appears that 206 ADP customers were affected. Two of the customers affected have at least 4,500 employees.

**Information**

**Source:**
Media

**July 30, 2013**  
**University of Delaware**  
**Newark, Delaware**

EDU HACK 74,000

Additional information can be found on the University of Delaware’s website here: [http://www.udel.edu/it/response/](http://www.udel.edu/it/response/)

Students and staff members may have had their information exposed during a hacking incident. The hacker or hackers were able to exploit a vulnerability in software acquired by a vendor. Names, addresses, Social Security numbers, and university ID numbers were exposed.

**UPDATE** (08/19/2013): An additional 2,000 people were affected. They were not employees but had received payment from the University of Delaware.

**Information**

**Source:**
Media

**July 30, 2013**  
**US Airways, Advanced Data Processing**  
**Tempe, Arizona**

BSO DISC 40,000

A programming error at Advanced Data Processing (ADP) caused employee names, Social Security numbers, and total taxable W-2 wages for the tax years 2010, 2011, and 2012 to be exposed. A group of other US Airway employees were able to download the payroll information of their colleagues. ADP corrected the issue in early May and notified US Airways in early June.

**Information**

**Source:**
Media

**July 30, 2013**  
**California Correctional Health Care Services**  
**Sacramento, California**

MED PHYS Unknown

An employee lost dental records while outside of California Correctional Health Care Services on June 19, 2013. The records contained patient names, CDCR numbers, dates of birth, and dental treatment plan information.

**Information**

**Source:**
California Attorney General

**July 29, 2013**  
**Fairfax County Public Schools**  
**Falls Church, Virginia**

MED PORT 2,000 (No Social Security numbers or financial information reported)
Brookfield, Fairfax Villa, and Navy elementary schools were affected. Lanier and Rocky Run middle schools were affected. Chantilly High School and Chantilly Academy were also affected.

The July 15 theft of a laptop resulted in the exposure of student information. The laptop was stolen from the car of a school nurse and contained school, health and other confidential information. Student names, school identification numbers, allergies, and other medical conditions were on a spreadsheet on the health-department-issued laptop.

Information
Source: Media
July 29, 2013 Wal-Mart, Oklahoma
BSR CARD Unknown

Multiple locations in Oklahoma were affected.

Two men were indicted for their role in a skimming plot. They are accused of fraudulently obtaining $400,000 by placing skimming devices at gas pumps at Wal-Mart stores for up to two months at a time. Then they created counterfeit cards by using the legitimate card information obtained through skimming. The skimming ring ran from April 2012 through January 2013.

Information
Source: Media
July 29, 2013 Oregon Health & Science University (OHSU) Portland, Oregon
MED DISC 3,000 (No SSNs or financial information reported)

Patient data could have been accessed due to a storage error. The information of patients admitted between January 2011 and July 3 of 2013 was placed on Google’s cloud computing system. The information was password-protected, but could have still been used for promotional and other purposes because OHSU does not have a contract with Google. OSHU removed the information from the cloud.

Information
Source: Media
July 29, 2013 Lone Star Circle of Care Austin, Texas
MED PORT 1,955

The theft of a laptop from an employee’s car around May 1, 2013 resulted in the exposure of patient information. Patients who were seen between 2012 and 2013 may have had their or their children’s names, Social Security numbers, and diagnosis information exposed.

Information
Source: HHS via PHIPrivacy.net
July 29, 2013 Jacksonville Spine Center Jacksonville, Florida
MED PHYS 5,200 (No Social Security numbers or financial information reported)

Paper patient records were lost, stolen, or exposed during an April 25 breach.

Information
Source: HHS via PHIPrivacy.net
July 29, 2013 Samaritan Regional Health System Ashland, Ohio
MED PHYS 2,203 (No Social Security numbers or financial information reported)

An exposure of patient paper records was discovered on May 29th.

Information
Source: HHS via PHIPrivacy.net
South Florida Neurology Associates, P.A.
Boca Raton, Florida

The theft of a laptop resulted in the exposure of patient information. The laptop was stolen sometime between May 25 and May 30.

Information
Source: HHS via PHIPrivacy.net

Sheet Metal Local 36 Welfare Fund, People Resource Corporation
St. Louis, Missouri

A data breach occurred between August 1, 2012 and July 8, 2013.

Information
Source: HHS via PHIPrivacy.net

MED-EL Corporation
Durham, North Carolina

An email error that occurred on June 25 resulted in the exposure of health information.

Information
Source: HHS via PHIPrivacy.net

Northrop Grumman Retiree Health Plan, CVS Caremark
Fall Church, Virginia

A breach involving paper records from CVS Caremark affected 4,305 Northrop Grumman Retiree Health Plan enrollees.

Information
Source: HHS via PHIPrivacy.net

NASDAQ OMX Group Inc.
New York, New York

Malware was installed on servers between November of 2008 and October of 2010. This allowed one or more hackers to execute commands to delete, change, and steal data from the computers used by NASDAQ. A total of five foreign hackers were charged for involvement in a series of financial incidents. They were all collaborating in a scheme to target major corporate networks and were able to steal more than 160 million credit card numbers across corporations.

Information
Source: Media

Stanford University
Stanford, California

People who used Stanford University’s computer network have been asked to reset their passwords. Stanford released few details but stated that it does not appear that Social Security numbers and financial information were accessed or exposed.

Information
Source: Media
Current and former members may have had their Social Security numbers, transaction records, and other personal information exposed due to malware that was found on an employee's office computer. The malware was discovered on May 26 and St. Mary's began mailing letters on July 12. The malware could have been on up to 23 workstations as early as February. There has been no evidence of names, Social Security numbers, addresses, account numbers, transaction records, or other sensitive information being accessed by an unauthorized individual so far.

Information Source: Media

July 25, 2013
Securities and Exchange Commission (SEC)
Washington, District Of Columbia
BSF DISC Unknown

A July 8 letter warned current and former employees that SEC employee data had been found on the networks of another federal agency. The outside federal agency was not named. It appears that a former SEC employee inadvertently and unknowingly downloaded the names, Social Security numbers, and dates of birth of SEC employees onto a thumb drive and then transferred them to another agency. The employee wanted a template of the document rather than the actual employee data that it contained. The accidental upload of sensitive information occurred in April of 2012 and again in June of either 2012 or 2013. Employees who were with SEC before October of 2009 were affected. The breach lasted for 10 months before being noticed. The SEC confiscated the flash drive when the breach was uncovered.

Information Source: Media

July 24, 2013
NYC Bike Share, Citibike
New York, New York
BSR DISC 1,200

NYC Bike Share discovered that customer credit card numbers, names, and addresses had been posted on a publicly accessible page of its website. The glitch was corrected after being active between April 15 and late May. Customers who initially entered their information incorrectly had their information posted online for 24 hours. The data was cleared every 24 hours between April 15 and late May.

Information Source: Media

July 24, 2013
Tinder
West Hollywood, California
BSO DISC Unknown

Tinder advertises to users that their physical location information is never shown to other users. An outside engineer discovered an issue with the Tinder app that allowed the locations of users to be available for at least two weeks. Last known locations, Facebook IDs, dates of birth, gender, and names were available.

Information Source: Media

July 23, 2013
Henry Ford Health System
Detroit, Michigan
MED PHYS 15,417 (No SSNs or financial information reported)

A warehouse that was not owned by Henry Ford Health System was raided for old X-rays. X-rays can be stripped for silver
and these medical X-rays also contained the names, addresses, and dates of birth of patients of Henry Ford Health System. The X-rays dated between 1996 and 2003. Henry Ford Health System learned about the issue on May 24.

**Information**

Source: Media  
Records from this breach used in our total: 0

**July 22, 2013**  
**Apple Inc.**  
**Cupertino, California**  
BSR HACK Unknown

Apple's website for developers was accessed by unauthorized parties. Registered developer names, mailing addresses, and email addresses may have been accessed on Thursday, July 18. Encrypted customer information was not affected.

**Information**

Source: Media  
Records from this breach used in our total: 0

**July 19, 2013**  
**University of Virginia, Aetna Health Care**  
**Charlottesville, Virginia**  
EDU DISC 18,700

A mailing error by a third-party mailing vendor used by Aetna Health Care resulted in the Social Security numbers of students being exposed in open-enrollment brochures.

**Information**

Source: Media  
Records from this breach used in our total: 18,700

**July 19, 2013**  
**Regional Medical Center Bayonet Point**  
**Hudson, Florida**  
MED DISC Unknown (10 confirmed)

A patient received the information of other patients in a mailing. Names, patient records, and Social Security numbers were exposed.

**Information**

Source: PHIPrivacy.net  
Records from this breach used in our total: 10

**July 18, 2013**  
**South Shore Physicians, P.C.**  
**Staten Island, New York**  
MED INSD 8,000 (80 people confirmed affected)

A dishonest nurse and three co-conspirators were linked to medical identity fraud after she posted details about the fraud on a social media account. The ring had been active since 2004 and had brought in $675,000 over the past five years. The nurse had been fired from South Shore Physicians after falsifying her work hours. The co-conspirators face at least 64 counts related to fraud, falsifying records, and theft.

**UPDATE** (10/1/2013): Notifications were sent to 8,000 patients in relation to the breach.

**Information**

Source: Media  
Records from this breach used in our total: 80

**July 18, 2013**  
**NASDAQ.com**  
**New York, New York**  
BSO HACK Unknown

Hackers were able to steal passwords from a NASDAQ Community forum. It is likely that only passwords and non-financial information was stolen. NASDAQ alerted users to the issue and took the website offline to upgrade its security. There is concern that the hackers will use the email and password information to send phishing messages and obtain access to various financial accounts.

**Information**

Source: Media  
Records from this breach used in our total: 0

**July 18, 2013**  
**San Jose Medical Supply Company**  
**San Jose, California**  
MED INSD 800

Fraudulent activity by former employees was discovered when a new owner took over San Jose Medical Supply Company in August of 2012. San Jose Medical Supply Company confirmed in June of 2013 that health information was exposed between August of 2011 and December of 2011. The dishonest employees and other affiliated individuals no longer work with San Jose Medical. Names, Social Security numbers, home addresses, dates of birth, Medi-Cal ID numbers, physician names and contact information, prescriptions, diagnosis information, type and quantity of medical supplies ordered, and disability codes were disclosed to Front Medical Supply and/or Living Medical Supply without authorization.

**UPDATE** (07/29/2013): A total of 800 people were affected.

**Information**

Source: California Attorney General  
Records from this breach used in our total: 800

Office of the Medicaid Inspector General (OMIG)
A link to the official notice can be found here: http://apps.cio.ny.gov/apps/mediaContact/public/preview.cfm?parm=E5EBBF4...

An OMIG employee sent an email that contained sensitive records to their own email account on October 12, 2012. Medicaid patient first and last names, Social Security numbers, dates of birth, and Medicaid client information numbers may have been compromised.

Information Source: Media

July 17, 2013
Citigroup
New York, New York
BSF DISC 146,000

Citigroup exposed the Social Security numbers, dates of birth, and other sensitive information of customers by not properly redacting the information for court records. Consumers who went into bankruptcy between 2007 and 2011 were affected. The incident was discovered by the bank on April 2011. Roughly 146,000 consumers were notified of the breach in July of 2013.

Information Source: Media

July 16, 2013
Gap, Banana Republic
San Francisco, California
BSR DISC 20

A customer received a package from Banana Republic that contained documents with employee Social Security numbers, tax forms, resignation letters, legal notices, doctors’ notes, and performance reviews. The package was meant for HR administration and contained the information of around 20 sales support associates who work at Gap. The customers were expecting a tie and pocket square. It appears that the package had been mislabeled.

Information Source: Media

July 16, 2013
Calvert Internal Medicine Group
Prince Frederick, Maryland
MED DISC Unknown

A finance department employee contacted ADP for troubleshooting and an ADP representative removed the firewall of Calvert Internal Medicine Group during the service call. The firewall was not restored after the call and employees began receiving spam emails from the finance department employee’s email account. Malware was also detected in the spam inbox of the employee’s computer. Names, Social Security numbers, addresses, and other payroll information of current and former employees may have been exposed.

Information Source: Media

July 16, 2013
Academy Studios
Novato, California
BSO PHYS Unknown

Personnel records were discarded in a public dumpster after Academy Studios. The non-profit closed in April and many of its assets were sold in an online auction on May 21. The personnel paperwork included names, Social Security numbers, dates of birth, copies of passports, copies of drivers’ licenses, I-9 forms, and other employee information.

Information Source: Media

July 13, 2013
Cedars-Sinai Medical Center
Los Angeles, California
MED INSD 14 (No Social Security numbers or financial information reported)

Five medical workers were fired for their role in a hacking effort that targeted a celebrity. A total of 14 patient records were breached between June 18 and June 24. The employees misused the Hospital’s information system to access patient records for curiosity or media purposes. A volunteer also participated and was barred from working at the Hospital.

Information Source: Media

July 12, 2013
Long Beach Memorial Medical Center
Long Beach, California
MED INSD 2,864 (No SSNs reported)
Patients who received treatment between September 2012 to June 2013 may have had their information exposed by a breach related to an employee. Names, sex, dates of birth, home addresses, phone numbers, account numbers, insurance information, and the reason for admission were exposed. There is currently no reason to believe that the information was used in a malicious manner.

**Information Source:**

**Media**

**July 11, 2013**  
**Texas Health Harris Methodist Hospital Fort Worth, Shred-it**  
**Fort Worth, Texas**  
**MED**  
**PHYS**  
277,000  
(Unknown number of SSNs)

People who may have been affected may call 1-877-216-3789 and use reference code 4537070513.

A concerned citizen alerted police to a situation on May 11. Old microfiche records were discovered in a park even though they should have been destroyed by the Hospital’s contractor Shred-it. The records contained names, addresses, dates of birth, and health information and were from 1980 to 1990. Some records also contained Social Security numbers.

**Information Source:**

**Media**

**July 11, 2013**  
**Guildford County Schools, Page High School**  
**Greensboro, North Carolina**  
**EDU**  
**DISC**  
456 (No SSNs or financial information reported)

Parents with questions may call 336-332-0810.

A Guildford County Schools employee accidentally emailed a PDF file that contained Page High School student personal information. Student names, addresses, phone numbers, course enrollments, grades, school district identification numbers, and other transcript data were in the PDF file. The information was emailed to a single guardian on July 2, 2013.

**Information Source:**

**Media**

**July 8, 2013**  
**Roy’s Holdings, Inc.**  
**Honolulu, Hawaii**  
**BSR**  
**STAT**  
Unknown

Malware infected an employee’s desktop computer. Roy’s restaurants in Ko‘Olina, Waikiki, Kaanapali, Poipu, and Waikoloa were affected. Anyone who used a debit or credit card at those locations between February 1, 2013 and February 25, 2013 may have had their payment card information compromised.

**Information Source:**

**California Attorney General**

**July 8, 2013**  
**Internal Revenue Service (IRS)**  
**Washington, District Of Columbia**  
**GOV**  
**DISC**  
10,000

Public.Resource.org received 990-T forms with sensitive information during a request for information from the IRS. The IRS acknowledged the mistake and Public.Resource.org became curious about where else the information could be found. Public.Resource.org found multiple incidents of Social Security numbers being exposed on the IRS website and wrote a letter that pointed out the issues to the IRS. The IRS was able to remove some or all of the sensitive files from public view over the course of a few days.

**Information Source:**

**Media**

**July 5, 2013**  
**Morningstar Document Research**  
**Chicago, Illinois**  
**BSF**  
**HACK**  
182,000 (2,300 credit card accounts reported)

Client information may have been compromised by an intrusion that took place around April 3. Client email addresses, passwords, credit card numbers, and other information may have been exposed.

**Information Source:**

**Media**

**July 4, 2013**  
**Behavioral Health Network**  
**Springfield, Massachusetts**  
**MED**  
**PHYS**  
Unknown
A concerned citizen found medical records in a publicly accessible dumpster. Behavioral Health Network has a shredding vendor and did not have an explanation for the breach. Behavioral Health Network picked up the remaining files.

**Information**

**Source:**

PHIPrivacy.net

**July 3, 2013**  
**Bureau of Automotive Repair (BAR)**  
Rancho Cordova, California

GOV  HACK  Unknown

Those with questions may call the Consumer Information Center at 1-800-952-5210.

An unauthorized individual accessed the network of a BAR service provider between May 2012 and March 2013. The bank routing information of Smog Check stations licensed with the BAR was exposed. Those who may have had their accounts accessed are encouraged to close their old accounts and open new accounts with new PINs or passwords.

**UPDATE (07/11/2013):** Approximately 7,500 Smog Check stations had bank account and routing numbers associated with the businesses exposed.

**Information**

**Source:**

California Attorney General

**July 3, 2013**  
**Indiana Family and Social Services Administration (FSSA), RCR Technology Corporation**  
Indianapolis, Indiana

GOV  DISC  187,533 (3,926 SSNs exposed)

A computer programming glitch resulted in the exposure of client health, financial, and employment information. Personal and private documents that belonged to certain clients were accidentally made available to other clients between April 6 and May 21 when FSSA contractor RCR Technology Corporation made a programming error. The issue was discovered on May 10 and addressed on May 21. Patients of clients may have had their names, addresses, dates of birth, demographic information, contact information, types of benefits received, monthly benefit amount, employer information, monthly income and expenses, bank balances and other assets, medical providers, medical conditions, and information about household members exposed.

**Information**

**Source:**

Media

**July 2, 2013**  
**Health Net, CalViva Health**  
Suwanee, Georgia

MED  DISC  Unknown

A number of member identification cards were mailed to incorrect addresses. The problem occurred because of a programming error. The member identification cards contained names, dates of enrollment, addresses, telephone numbers of primary care physicians, issue dates of cards, and Medi-Cal client identification numbers.

**Information**

**Source:**

California Attorney General

**July 2, 2013**  
**Quayside Publishing Group**  
Minneapolis, Minnesota

BSO  CARD  Unknown

Qbookshop.com, Qbookshop.net, Motorbooks.com, and WalterFoster.com were affected. A credit card breach resulted in the exposure of information. Customers who made online purchases at Quayside Publishing Group had their information exposed sometime around April 29. Names, addresses, and credit card numbers were exposed until June 17.

**Information**

**Source:**

California Attorney General

**July 2, 2013**  
**Advantage Health Solutions**  
Indianapolis, Indiana

MED  DISC  Unknown

A patient discovered that he could see the information of other users by logging into his Advantage Health Solutions account. Any patients who put in a name or date of birth other than their own were able to see the records of people with those names or dates of birth. Names, phone numbers, addresses, primary care physicians, medical bills, types of medications, and other medical information were exposed.

**Information**

**Source:**

PHIPrivacy.net

**July 1, 2013**  
**Union Security Insurance Company**  
Kansas City, Missouri

MED  UNKN

1,127 (No Social Security numbers or financial information)
A breach that occurred on May 17 may have exposed protected health information. It involved email and/or the improper disposal of records.

Information Source: HHS via PHIPrivacy.net

June 28, 2013 University of South Carolina Columbia, South Carolina

EDU PORT 6,300

The April theft of a faculty laptop resulted in the exposure of current and former student information. The laptop was stolen from a locked room in the Department of Physics and Astronomy. It contained a file with the names, emails, and Social Security numbers of up to 6,300 University of South Carolina students who had taken one of four physics courses between January of 2010 and the fall 2012 semester.

Information Source: Media

June 28, 2013 Greensboro ABC Stores, Triad ABC

BSR HACK Unknown

Stores in the Greensboro, South Carolina and Winston-Salem, North Carolina areas were affected.

Greensboro ABC stores and Triad ABC stores discovered that the software used by cash registers had been hacked. The malware was discovered after customers complained about fraudulent charges on their debit and credit card accounts. The ABC stores stopped accepting credit and debit cards while investigating the issue.

Information Source: Media

June 27, 2013 Millimaki Eggert, LLP

San Diego, California

BSF PORT Unknown

The April 27 office burglary of two password-protected laptops resulted in the exposure of sensitive client information. Names, Social Security numbers, and addresses may have been involved.

Information Source: California Attorney General

June 27, 2013 Citi Prepaid Services

New York, New York

BSF DISC Unknown

Those with questions may call (888) 742-9213.

A code change in the prepaid cardholder website impacted the security features that authenticate cardholder logins. Anyone who logged into the prepaid cardholder website between June 2 and June 13 was affected. The issue was remediated and it does not appear that unauthorized charges have occurred on any of the affected accounts.

Information Source: California Attorney General

June 26, 2013 Iowa Department of Health Services

Des Moines, Iowa

MED PORT 7,335 (No Social Security numbers or financial information reported)

Former patients of the Mental Health Institute in Independence, Iowa and state employees may have had their confidential information exposed. A backup tape was found to have been missing as of April 30. Officials of Iowa Department of Human Services believe the tape was accidentally discarded or destroyed.

UPDATE (06/27/2013): The tape contained the information of 7,300 patients and 700 employees. Only patients who were admitted after June of 2010 were affected.

Information Source: PHIPrivacy.net


Nashville, Tennessee

MED PORT 5,690
The June 15 theft of an employee’s laptop resulted in the exposure of patient information. Names, Social Security numbers, dates of birth, addresses, medical information, and telephone numbers were on the laptop.

UPDATE (08/28/2013): A total of 5,690 patients were affected by the breach.

UPDATE (11/25/2013): Level of care, dates of service, health insurance information, and other medical information were also on the laptop.

Information Source: PHIPrivacy.net

June 25, 2013  Baptist Health South Florida, West Kendall Baptist Hospital
Miami, Florida

An employee of West Kendall Baptist Hospital sold patient information to a man who used the information to file fraudulent tax returns. Patients may have had their names, Social Security numbers, and dates of birth exposed. The man who purchased and used the information was sentenced to 31 months in federal prison after pleading guilty to possessing 15 or more Social Security numbers.

Information Source: PHIPrivacy.net

June 24, 2013  Florida State University, Florida Department of Education
Tallahassee, Florida

The information of 47,000 Florida teachers was publicly accessible for 14 days after a data transfer at Florida State University. The information was from teachers participating in state prep programs. The Department of Education used Florida State University as the contractor for the transfer of teacher data.

UPDATE (06/26/2013): People who participated in Florida teacher preparation programs during the 2009-2010 and 2011-2012 academic years were affected.

Information Source: Media

June 24, 2013  King County Sheriff’s Office
Seattle, Washington

A laptop and portable hard drive were stolen from the truck of an undercover officer in March of 2013. The devices were not encrypted and contained Social Security numbers, drivers license numbers, and personal information about victims, suspects, witnesses, and police officers. The officer received disciplinary action for leaving the laptop unattended in the backseat of a truck.

Information Source: Media

June 21, 2013  Facebook
Menlo Park, California

Facebook’s official notice can be found here: https://www.facebook.com/notes/facebook-security/important-message-from-facebooks-white-hat-program/10151437074840766

Facebook discovered a bug that may have allowed unauthorized users to view the personal contact information of Facebook users. The people who could have used the information would have had some kind of connection to them or some kind of contact information, but users may have thought their email and phone numbers were hidden from these connections. People who used the Download Your Information (DYI) tool may have been able to access the contact information. The issue was discovered by an external group of security researchers involved with the White Hat program. The breach began sometime in 2012.

Information Source: Media

June 21, 2013  North Lincoln Community Health Center Clinic
Lincoln City, Oregon

An April 17 burglary resulted in the possible exposure of patient information. Someone entered locked rooms and cabinets in order to take money. No records or electronic devices were taken; however the room where client medical charts were stored was accessed. Social Security numbers, health information, and other personal information may have been exposed.

Information Source: PHIPrivacy.net
Sight and Sun learned of a patient privacy breach on May 17. Patient names, Social Security numbers, addresses, medical record numbers, and other personal information may have been exposed. An employee accessed and copied patients' electronic medical records without legitimate purpose.

**UPDATE (06/26/2013):** A total of 9,000 patients were affected. It appears that the records were accessed to target patients for other medical service offerings.

---

**Comfort Dental Indianapolis, Indiana**

Nearly 7,000 patient records were found in a publicly accessible dumpster. A local news team investigated the breach and found the names, Social Security numbers, addresses, phone numbers, dates of birth, X-rays, dental information, credit card numbers, medical histories, and other sensitive information of Comfort Dental patients. Comfort Dental patients who were seen at offices in Marion, Indiana and Kokomo, Indiana may have been affected. The news team reported the issue around March 18, 2013 and removed the records.

---

**Ephrata Community Hospital Ephrata, Pennsylvania**

Ephrata Community Hospital posted an official notice here:

http://www.ephrahathospital.org/HospitalOverview/AboutUs/News/tabid/168/anid/100/Default.aspx

Those with questions may call 1-888-414-8021 and enter the reference code: 8934061413.

An employee inappropriately accessed patient information. The incident or incidents were discovered on April 16. Patient clinical and other medical information may have been exposed. No Social Security numbers were exposed.

---

**City of Houston, Automatic Data Processing Houston, Texas**

A software code error caused W-2 information to be exposed. Approximately 1,300 classified Houston Police Department employees and 5,000 other local government workers were affected. Names and Social Security numbers were exposed.

---

**Yolo Federal Credit Union Woodland, California**

Yolo was notified by Visa that there may have been a breach at several merchant locations. Yolo was not the sight of the breach, but customers were issued new payment cards. The issue was reported to Yolo on May 31.

---

**Fayetteville Veterans Affairs Medical Center Fayetteville, North Carolina**

Optical shop consultation reports were placed in a publicly accessible recycling bin over a period of three months rather than properly disposed. The documents contained names, Social Security numbers, addresses, dates of birth, and prescriptions. The issue was discovered on April 17 and most likely started in January of 2013.

---

**Florida Department of Health Florida**

Information on personal drug prescriptions from the Florida Department of Health somehow ended up in the hands of prosecution lawyers. Names, addresses, phone numbers, pharmacies, and drug dosages were obtained by lawyers involved in six prescription-drug fraud cases. The American Civil Liberties Union of Florida began an investigation into how the records were exposed.
Two men claimed to be from a recycling company and stole over 200 pounds of X-ray film that contained sensitive patient information. The men transported the X-rays from the hospital without incident by using a moving truck. The breach occurred in 2012 and affected less than 500 patients.

The Orlando Police Department notified Wyndham Vacation Ownership that a Wyndham employee had been arrested for participating in fraudulent credit card purchases. The dishonest employee was fired the next day and may have obtained customer credit card numbers. Wyndham learned of the issue on January 18.


Between May 2 and May 8, a non-functional laptop computer was stolen from a secured area of the hospital. The laptop was password protected and contained names, ages, medical record numbers, telephone numbers, scheduled surgical procedures, and names of physicians involved in procedures between 2009 and 2012.

Two comScore panelists filed a lawsuit in August of 2011 after downloading comScore software. Allegedly, comScore collected and sold consumers' Social Security numbers, credit card numbers, financial information, retail transactions, and other personal information. The action may have violated the Stored Communications Act, the Computer Fraud and Abuse Act, the Electronics Communications Privacy Act, and the Illinois Consumer Fraud and Deceptive Practices Act. The lawsuit might cover tens of millions of people who have downloaded comScore software since 2005. In June of 2013, the Seventh Circuit Court of Appeals in Chicago denied comScore’s request to overturn a lower court’s decision that had allowed the suit to proceed as a class action suit.

A dishonest employee and his cousin pleaded not guilty to charges of conspiracy to commit identity theft, conspiracy to disclose individuals' health information, access device fraud, wrongful disclosure of health information, and aggravated identity theft. The men are accused of stealing the names and Social Security numbers of patients to file fraudulent income tax returns between September of 2012 and April of 2013.

**UPDATE** (08/28/2013): A total of 710 patients were affected by the breach on April 16.
Independence Care System
New York, New York

The May 7 home burglary of an employee’s home resulted in the theft of a laptop that contained patient information. Fewer than 60% of the affected members had their names, zip codes, and Independence Care System (ICS) Member ID numbers exposed. Approximately 40% of those affected also had their street address, phone number, Medicaid ID number, and enrollment and/or disenrollment date exposed. ICS plans to implement a two-factor authentication system for network access by September of 2013 to prevent the issued from occurring again.

Emmorton Associates
Abingdon, Maryland

A counselor’s file cabinet was burglarized sometime between December 10 and December 21. It contained client files with names, Social Security numbers, dates of birth, addresses, telephone numbers, diagnosis, treatment information, insurance information, and emergency contact information.

Health Resources of Arkansas
Heber Springs, Arkansas

Health Resources of Arkansas’ notice can be found here: http://www.healthresourcesofarkansas.com/assets/files/breach-of-conf-notice.pdf

On April 14, 2013 staff members discovered that their location had been burglarized. Names, Social Security numbers, addresses, dates of birth, diagnosis information, types of treatments, classes attended, court information, services provided, or insurance information of persons served by the location could have been accessed during the burglary. Notifications were sent during the week of May 20.

Integrity Oncology, Baptist Medical Group, North Atlantic Telecom
, Tennessee

Integrity Oncology has multiple locations in Tennessee.

Integrity Oncology’s business associate North Atlantic Telecom discovered a breach incident on March 5.

City of Norwood
Norwood, Ohio

A laptop that contained protected health information was lost between the dates of April 4 and April 19.

Laboratory Corporation of America (LabCorp)
Burlington, North Carolina

The theft of a computer that was scheduled to be destroyed may have exposed patient names, birthdates, and Medicare subscriber numbers.
A hard drive from the therapy service was purchased and then returned to Other World Computing. A doctor in Germany later contacted the therapy service and confirmed that he had received the hard drive. Client information, progress notes, and billing notes could be found on the hard drive though the doctor had believed he was purchasing a new or refurbished hard drive. Other World Computing or the hard drive's manufacturer failed to clear the hard drive before it was resold. The hard drive was resold to its original owner in order to safeguard the therapeutic client information.

Information
Source: PHIPrivacy.net

June 7, 2013
Raley’s Supermarket
West Sacramento, California
BSR HACK Unknown

Raley’s supermarket announced they may have been the target of a cyberattack that affected customers who used their credit or debit cards at any of its stores. The supermarket chain launched an investigation but had yet to find any evidence of unauthorized access to payment card data.

Reportedly, the supermarket chain was contacted by a credit card company regarding suspicious activity on customers credit cards on May 30, 2013.

Information
Source: Media

June 6, 2013
Sutter Health East Bay Region: Alta Bates Summit Medical Center, Sutter Delta Medical Center, Eden Medical Center
Sacramento, California
MED UNKN 4,500

Patients who visited Sutter Health’s Alta Bates Summit Medical Center, Sutter Delta Medical Center, or Eden Medical Center may have had their names, Social Security numbers, dates of birth, gender, addresses, zip codes, home phone numbers, marital status, names of employers, and work phone numbers exposed. The Alameda County Sheriff’s office notified Sutter Health of the potential breach on May 23. It is unclear what the source of the breach might be.

UPDATE (06/10/2013): The information was found during a narcotics raid. The personal information of nearly 4,500 patients was discovered.

UPDATE (07/29/2013): Nelson Family of Companies, a staffing firm, was also involved.

Information
Source: California Attorney General

June 6, 2013
SynerMed, Inland Valleys IPA, Inland Empire Health Plan
Monterey Park, California
MED PORT 1,566 (No SSNs or financial information reported)

The theft of an employee’s laptop resulted in the exposure of patient information. The theft occurred on the night of April 14 or the early morning of April 15 when a thief broke into the employee’s automobile. The laptop was password-protected and reported missing on the morning of the April 15. The laptop’s access to the SynerMed systems was eliminated on the morning of April 15 and the laptop contained member names, membership numbers, member addresses, CPT Codes, Diagnosis Codes, and dates of birth.

UPDATE (06/07/2013): The laptop belonged to a group of independent California physicians managed by SynerMed, Inc. called Inland Valleys IPA.

UPDATE (06/17/2013): There were no Social Security numbers on the laptop.

UPDATE (06/21/2013): A total of 1,566 people were affected.

UPDATE (07/01/2013): A total of 3,164 patients were affected.

Information
Source: California Attorney General

June 6, 2013
Town of Brookhaven
Brookhaven, New York
GOV DISC 78

A law enforcement employee made a clerical error that caused the Social Security numbers of 78 ambulance workers and beneficiaries to be available on the town website for five days. The information was accidentally attached to a resolution. A very similar error had occurred before and this one was caused by a failure to click on the “no public access” check box in the computer system to privatize the information.
June 5, 2013  
**University of Massachusetts - Amherst**  
Amherst, Massachusetts  
EDU  
HACK  
1,700

The information of almost 1,700 clients of the Center for Language, Speech, and Hearing may have been exposed. A computer workstation was found to be infected by a malicious software program. Client Social Security numbers, addresses, names of health insurers, and primary health care or referring doctors may have been accessible because the computer was compromised.

June 5, 2013  
**Massachusetts Mutual Life Insurance Company, MassMutual Financial Group**  
Springfield, Massachusetts  
BSF  
DISC  
Unknown

The 401(k) retirement plan information of certain clients was inadvertently exposed when a MassMutual account manager sent an email on May 8. Names, Social Security numbers, investment elections, and account balances were included in the email. A third party provider received the email and confirmed that the information was deleted without being saved or copied. The employee who accidentally sent the sensitive email received training on proper security procedures.

June 3, 2013  
**Health Information Trust Alliance**  
Frisco, Texas  
MED  
HACK  
111 (No SSNs or financial information reported)

A hacking incident resulted in the exposure of 111 records. Names, phone numbers, addresses, email addresses, and company names were exposed.

June 3, 2013  
**Office of Dr. Lee D. Pollan, DMD, PC.**  
Rochester, New York  
MED  
PORT  
13,806

The theft of the doctor's laptop may have exposed patient information. The theft occurred sometime between November 6, 2012 and November 15, 2012. Information related to patient names, dates of birth, addresses, Social Security numbers, diagnose and surgery billing codes, dates of service, and person responsible for the billing was on the laptop.

June 3, 2013  
**Champlain College**  
Burlington, Vermont  
EDU  
PORT  
14,217

Those with questions may call 877-643-2062.

During the weekend of June 3, a hard drive was discovered to have been misplaced. The device had been left unattended in a computer lab for about two days in March. The hard drive contained names, Social Security numbers, and other information related to admissions and financial aid for the Fall 2010 through the February 2013 school terms. Some graduate and continuing professional studies students may have also been affected.

May 31, 2013  
**Bon Secours Hampton Roads Health System, Bon Secours Mary Immaculate Hospital**  
Newport News, Virginia  
MED  
INSD  
5,000

An April 2013 audit revealed that a patient's medical record had been accessed in a way that was inconsistent with hospital policy. A further investigation revealed that two team members of the patient care team had accessed the records of multiple patients in ways that were inconsistent with their job function. The employees were fired. Patient names, dates and times of service, provider and facility names, Social Security numbers, internal hospital medical records and account numbers, dates of birth, diagnosis, medications, vital signs, and other treatment information may have been accessed.

May 31, 2013  
**RentPath, Inc. (Primedia)**  
Norcross, Georgia  
BSO  
INSD  
56,000
An independent contractor with access to Primedia's network operations group was found to have stolen hardware. The issue was discovered on June 20, 2012. Applicants, employees, and former employees may have had several different types of personal information stolen. Approximately 56,000 Social Security numbers were discovered among the various types of information. Approximately 30,000 former employees, employees, and applicants were identified and notified of the breach. The other 26,000 have yet to be identified.

<table>
<thead>
<tr>
<th>Information</th>
<th>Source</th>
<th>records from this breach used in our total: 56,000</th>
</tr>
</thead>
</table>
| May 31, 2013 | University Dental Associates  
Brooklyn, New York | MED PORT 2,400 |

The November 21 office theft of a laptop resulted in the exposure of patient information. Names, Social Security numbers, dates of birth, addresses, and billing codes were on the laptop.

<table>
<thead>
<tr>
<th>Information</th>
<th>Source</th>
<th>records from this breach used in our total: 2,400</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 30, 2013</td>
<td>Drupal.org</td>
<td>BSO HACK Unknown</td>
</tr>
</tbody>
</table>

Drupal is a volunteer-based organization and doesn’t have a central location.

A hacker or hackers exploited a vulnerability in a third-party software and used it to access accounts on drupal.org. The hackers were able to upload files to the association.drupal.org and compromised Drupal’s server. Accounts on groups.drupal.org may have also been exposed. Usernames, email addresses, hashed passwords, and country information may have been exposed.

<table>
<thead>
<tr>
<th>Information</th>
<th>Source</th>
<th>records from this breach used in our total: 0</th>
</tr>
</thead>
</table>
| May 30, 2013 | California Department of Developmental Services  
Sacramento, California | MED PHYS Unknown |

Stacks of patient and billing records were left in an unsecured and abandoned office in March of 2012. Credit card and Social Security numbers may have been exposed.

<table>
<thead>
<tr>
<th>Information</th>
<th>Source</th>
<th>records from this breach used in our total: 0</th>
</tr>
</thead>
</table>
| May 30, 2013 | California Department of Developmental Services  
Santa Monica, California | MED PORT 18,100 |

An employee at North Los Angeles County Regional Center left a work laptop, a personal laptop, and an iPhone in their car overnight. The items were stolen during the night. The employee worked for a program that served disabled infants and toddlers. Names, Social Security numbers, and other personal information were on the unencrypted work laptop. The theft occurred in November and patients were notified in January of 2013.

<table>
<thead>
<tr>
<th>Information</th>
<th>Source</th>
<th>records from this breach used in our total: 18,100</th>
</tr>
</thead>
</table>
| May 30, 2013 | Anasazi Hotel, LLC  
Santa Fe, New Mexico | BSO HACK Unknown |

Anasazi Hotel learned that it was a common link in a number of fraudulent credit card activities. An investigation revealed that Anasazi’s network had been accessed and customer credit card information had been accessed. Malware that could transmit customer names and credit card information was on Anasazi’s system. Anyone who used a credit card at Anasazi between June 18, 2012 and March 21, 2013 may have been affected.

<table>
<thead>
<tr>
<th>Information</th>
<th>Source</th>
<th>records from this breach used in our total: 0</th>
</tr>
</thead>
</table>
| May 30, 2013 | Utah Division of Motor Vehicles (DMV)  
Salt Lake City, Utah | GOV INSD Unknown |

An employee of the Utah Division of Motor Vehicles was fired in March for releasing confidential, personal information from DMV databases. The former employee was a customer service clerk who had worked for the division for 14 years. Investigators also took the former employee's work hard drive, computer, printer, and other items that might have contained sensitive data. The items will be investigated in a forensics lab.

<table>
<thead>
<tr>
<th>Information</th>
<th>Source</th>
<th>records from this breach used in our total: 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 29, 2013</td>
<td>University of Florida</td>
<td>MED INSD 5,682</td>
</tr>
</tbody>
</table>
The University of Florida’s statement can be read here: [http://news.ufl.edu/2013/05/29/potential-identity-theft-2/](http://news.ufl.edu/2013/05/29/potential-identity-theft-2/)

A dishonest employee working at University of Florida Health Pediatrics at Tower Square is suspected of participating in an identity theft ring. The former employee had access to pediatric patient records that included names, Social Security numbers, addresses, and dates of birth. The University of Florida learned about the issue on April 11.

**Information Source:**
Media

May 29, 2013
**Jackson Health System**
Miami, Florida

A box that contained patient medical records was determined to have been missing since January. Patient medical diagnoses, surgical procedures, and other personal health information may have been exposed. The missing records were either on their way to be electronically scanned or returning from being scanned.

**Information Source:**
Media

**May 29, 2013**

**TJG, Inc., Target Marketing**
Ashland, Virginia

The Target Marketing website was accessed by unauthorized parties on May 14. People who used debit or credit cards on the online e-commerce platform may have had their names, email addresses, payment card numbers, expiration dates, and CVV codes accessed.

**UPDATE** (05/29/2013): Shumsky in Dayton, Ohio was also affected. Shumsky customers may have had their names, addresses, email addresses, credit/debit card numbers, payment card expiration dates, and CVV codes accessed.

**Information Source:**
California Attorney General

**May 28, 2013**

**Beachbody**
Santa Monica, California

Hackers accessed Beachbody’s Powder Blue website. Beachbody learned of the incident on April 17 and found that customer credit card numbers, email addresses, mailing addresses, telephone numbers, full names, and CVV numbers may have been accessed.

**Information Source:**
PHIPrivacy.net

**May 28, 2013**

**Godiva**
New York, New York

An individual contact Godiva sometime around April 15 and informed them that a flash drive with Godiva employee information had been found. The information included employee ID numbers, Social Security numbers, dates of birth, phone numbers, resumes, and photos for people who worked at or applied to Godiva sometime prior to August 5, 2010. The flash drive was once used by an employee with access to human resources data and an investigation revealed that there was no reason to suspect that the information had been misused.

A total of 2,638 California residents may have been affected. It is not clear how many people were affected nationwide.

**Information Source:**
Media
An employee error caused patient information from surgeries to appear on the internet. Names, dates of service, procedures, surgeons, hospital charges, and names of insurance companies were accidentally uploaded. The breach occurred on February 14 and was discovered on April 17.

UPDATE (07/10/2013): Surgical services covering information from July 1, 2011 to June 30, 2012 was posted on the Sonoma Valley Hospital website.

Information Source: PHIPrivacy.net

May 23, 2013

Institutional Shareholder Services
Boston, Massachusetts

An employee of Institutional Shareholder Services (ISS) shared nonpublic voting data in exchange for $15,000 in concert tickets and $20,000 in meals. From 2007 through early 2012 an ISS employee provided nonpublic information on how over 100 ISS clients were voting on proxy ballots to a firm that gathers shareholder votes. ISS will pay The Securities and Exchange Commission $300,000 to settle civil charges and penalties. ISS neither admitted nor denied Securities and Exchange Commission allegations that it violated financial adviser rules designed to prevent misuse of non-public consumer information.

Information Source: Media

May 22, 2013

Department of Homeland Security (Customs and Border Protection, Immigration and Customs Enforcement)
Washington, District Of Columbia

Department of Homeland Security employees working in the headquarters office for Immigration and Customs Enforcement and Customs and Border Protection between 2009 and 2013 may have had their names, Social Security numbers, and dates of birth exposed. Tens of thousands of employees were affected. Though one or more unauthorized users had access to the information, there is no evidence that any employee data was stolen or lost. Law enforcement officials discovered a vulnerability in an unnamed vendor’s system that is used for processing background investigations.

Information Source: Media

May 22, 2013

Vendini, Inc.
San Francisco, California

Those with questions may call Vendini at 800-836-0473.

Vendini’s blog statement can be read here: http://blog.vendini.com

Anyone who used Vendini for ticket purchases may have had their financial information exposed during a March breach. A hacker accessed Vendini’s server and may have obtained customer names, addresses, email addresses, credit card numbers, and credit card expiration dates. A total of 22,900 customers from Augusta, Maine may have been affected. It is unclear if people from other states were also affected.

UPDATE (06/12/2013): The unauthorized intrusion was first detected on April 25.

Information Source: Media

May 21, 2013

Lifeline (Federal Communications Commission), TerraCom Inc., YourTel America Inc.
Washington, District Of Columbia

TerraCom customers who have questions may call 1-855-297-0243.

Around 44,000 application forms and 127,000 supporting documents for Lifeline were posted online. Lifeline is a federal program that provides discount internet and phone service for low-income Americans. Information such as name, Social Security number, scans of food-stamp cards, driver’s licenses, tax records, pay stubs, and parole letters was available online. The information had been available since at least March and was removed April 26.

UPDATE (05/23/2013): The story was originally released by Scripps Howard News Service when a reporter found completed Lifeline applications by searching Google for TerraCom-related information. Terracom and Yourtel are threatening to hold Scripps accountable for costs associated with the breach. These alleged costs include potentially complying with more than 20 state data breach notification laws.
DENT Neurological Institute accidentally emailed the private information of more than 10,000 patients. No sensitive medical files or Social Security numbers were involved.

Erie County Department of Social Services
An audit revealed that several employees had not been following correct protocol for patient record disposal. Employees had inadvertently exposed Social Security numbers, copies of birth certificates, personal medical records, tax returns, bank account information, inmate records, payroll information, court records, and passports. Employees should have been using locked disposal totes for shredding and were discarding documents in recycling totes instead.

Sovereign Medical Group, LLC
An October 10, 2012 breach resulted in the exposure of information. The incident or incidents involved one or more network servers, theft, and/or hacking.

Hawaii State Department of Health - Adult Mental Health Division
An employee noticed unusual activity on a computer and a hacking incident was discovered on September 25, 2012. Information stored on a computer file may have been accessed and dated back to 1997. Names, dates of birth, addresses, phone numbers, consumer record numbers, and a limited number of Social Security numbers were exposed.

Goldman Sachs, Bloomberg LP
Bloomberg News reporters were able to monitor clients' usage of data terminals leased from Bloomberg LP. Goldman Sachs is one of the companies that has complained publicly while JP Morgan Chase, the Federal Reserve, and the United States Treasury Department have started investigations. It is unclear how many other organizations may have been affected.

Public Health - Seattle and King County
A custodian improperly disposed of client medical information on March 7. The records were from the Refugee Screening, WIC, and Needle Exchange programs. Patient names, dates of birth, phone numbers, addresses, medical record numbers, appointment dates, and medical condition or treatment may have been accessed.

Information
Source:  
HHS via PHIPrivacy.net

May 17, 2013  
Orthopedics and Adult Reconstructive Surgery, Texas

The Health and Human Services website of medical breaches reports the loss of a portable electronic device by Orthopedics and Adult Reconstructive Surgery. The breach occurred between March 1 and March 13. AssuranceMD is named as a business associate.

Information
Source:  
HHS via PHIPrivacy.net

May 17, 2013  
Delta Dental of Pennsylvania, ZDI Mechanicsburg, Pennsylvania

The March 20 loss of paper records may have exposed the information of patients. ZDI lost the records of their associate Delta Dental of Pennsylvania.

Information
Source:  
HHS via PHIPrivacy.net

May 17, 2013  
Valley Mental Health Murray, Utah

The February 27 theft of a computer resulted in the exposure of patient information.

Information
Source:  
HHS via PHIPrivacy.net

May 17, 2013  
Wood County Hospital Bowling Green, Ohio

Those with questions may call 855-322-6427.

The March theft of radiology films resulted in the exposure of patient information. The films were most likely stolen from the Hospital's storage room in order to be stripped of their silver. The films contained patient names, medical record numbers, dates of exams, and in some cases, dates of birth. The thieves posed as recycling subcontractors.

Information
Source:  
HHS via PHIPrivacy.net

May 17, 2013  
The Guidance Center of Westchester, Inc. New Rochelle, New York

On February 22, 2013, the Guidance Center of Westchester discovered that a central processing unit (CPU) had been removed from a staff member's office. The CPU was removed on February 21 and contained, names, Social Security numbers, dates of birth, dates of admittance to the Center, names of insurance carriers, home addresses, diagnoses, outpatient treatment authorization request, doctors' names, case numbers, and whether or not a patient was prescribed medication.

Information
Source:  
HHS via PHIPrivacy.net

May 17, 2013  
Stronghold Counseling Services, Inc.

8,500 (No SSNs or financial information reported)
The December 24, 2012 theft of a computer resulted in the exposure of patient information.

Information Source:
HHS via PHIprivacy.net

May 17, 2013
Community Health Network, Community Health Medcheck
Speedway, Indiana

MED INSD 180

A dishonest employee of Community Health Medcheck accessed the medical records of up to 180 people between mid-March and mid-April. Social Security numbers, dates of birth, credit card numbers, and other information may have been exposed.

Information Source:
PHIprivacy.net

May 16, 2013
Louisiana State University (LSU) Health Shreveport, Siemens Healthcare
Shreveport, Louisiana

MED DISC 8,330 (No SSNs or financial information reported)

Those with questions may call (888) 824-0379 or (318) 675-7550.

A computer data entry error resulted in a mailing error that exposed patient information. The names and treatment information of certain patients were mistakenly mailed to other patients. No Social Security numbers, dates of birth, or financial account numbers were exposed.

Information Source:
PHIprivacy.net

May 15, 2013
City of Akron
Akron, Ohio

GOV HACK 47,452 (Unknown number of Social Security numbers)

The City of Akron's website and internal systems were hacked by a foreign group. Files with 47,452 entries were posted online. Names, Social Security numbers, account numbers, credit card numbers, credit card expiration dates, addresses, and other information were in the files. The hacking attack appears to be part of an organized international effort to hack into various U.S. government websites.

Information Source:
Media

May 15, 2013
El Centro Regional Medical Center
El Centro, California

MED PHYS 189,489

May 16, 2013
DENT Neurologic Institute of Amherst
Amherst, New York

MED DISC 10,200 (No SSNs or financial information exposed)

An administrative error led to the personal information of 10,200 patients being emailed to 200 patients. Names, addresses, date of last appointment, visit type, primary care physician, referring physician, email addresses, and whether or not the patient was actively receiving treatment were in an Excel attachment of an email that was sent to unspecified parties. The recipients were called and instructed to delete the email.

Information Source:
Media

May 16, 2013
Weather Shield
Medford, Wisconsin

BSO UNKN Unknown

A total of 55 current and former Weather Shield employees across the country discovered that someone had stolen their identities and filed fraudulent tax refunds. Several employees who were victims of identity theft in 2012 discovered that they had been affected again when filing their taxes in April of 2013. It is unclear how the 2012 or 2013 breaches occurred.

Information Source:
Media

May 15, 2013
Sioux Falls, South Dakota

MED STAT information reported

The December 24, 2012 theft of a computer resulted in the exposure of patient information.
El Centro Regional Medical Center is claiming that they were defrauded by an unnamed company. The company was responsible for digitizing El Centro Regional’s x-rays, but never returned the digitized version. The process should have been completed by the end of July. The original x-rays were most likely taken and destroyed to extract silver.

**UPDATE (05/18/2013):** The information on the records was as recent as February 2011. El Centro Regional Medical Center learned of the issue on March 22, 2013. Patients were notified on May 13.

<table>
<thead>
<tr>
<th>Date</th>
<th>Company Name</th>
<th>Address</th>
<th>Industry</th>
<th>Type</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 15, 2013</td>
<td>OptiNose US Inc.</td>
<td>Yardley, Pennsylvania</td>
<td>MED</td>
<td>PORT</td>
<td>Unknown</td>
</tr>
<tr>
<td>May 13, 2013</td>
<td>80sTees.com</td>
<td>Mount Pleasant, Pennsylvania</td>
<td>BSR</td>
<td>HACK</td>
<td>Unknown</td>
</tr>
<tr>
<td>May 11, 2013</td>
<td>Regional Medical Center</td>
<td>Memphis, Tennessee</td>
<td>MED</td>
<td>DISC</td>
<td>1,200</td>
</tr>
</tbody>
</table>

An unencrypted laptop was stolen from an employee’s car. It may have contained names, Social Security numbers, and personal information related to people who worked at OptiNose.

**UPDATE (05/18/2013):** The information on the records was as recent as February 2011. El Centro Regional Medical Center learned of the issue on March 22, 2013. Patients were notified on May 13.

<table>
<thead>
<tr>
<th>Date</th>
<th>Company Name</th>
<th>Address</th>
<th>Industry</th>
<th>Type</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 15, 2013</td>
<td>OptiNose US Inc.</td>
<td>Yardley, Pennsylvania</td>
<td>MED</td>
<td>PORT</td>
<td>Unknown</td>
</tr>
<tr>
<td>May 13, 2013</td>
<td>80sTees.com</td>
<td>Mount Pleasant, Pennsylvania</td>
<td>BSR</td>
<td>HACK</td>
<td>Unknown</td>
</tr>
<tr>
<td>May 11, 2013</td>
<td>Regional Medical Center</td>
<td>Memphis, Tennessee</td>
<td>MED</td>
<td>DISC</td>
<td>1,200</td>
</tr>
</tbody>
</table>

An unencrypted laptop was stolen from an employee’s car. It may have contained names, Social Security numbers, and personal information related to people who worked at OptiNose.

**UPDATE (05/18/2013):** The information on the records was as recent as February 2011. El Centro Regional Medical Center learned of the issue on March 22, 2013. Patients were notified on May 13.

<table>
<thead>
<tr>
<th>Date</th>
<th>Company Name</th>
<th>Address</th>
<th>Industry</th>
<th>Type</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 15, 2013</td>
<td>OptiNose US Inc.</td>
<td>Yardley, Pennsylvania</td>
<td>MED</td>
<td>PORT</td>
<td>Unknown</td>
</tr>
<tr>
<td>May 13, 2013</td>
<td>80sTees.com</td>
<td>Mount Pleasant, Pennsylvania</td>
<td>BSR</td>
<td>HACK</td>
<td>Unknown</td>
</tr>
<tr>
<td>May 11, 2013</td>
<td>Regional Medical Center</td>
<td>Memphis, Tennessee</td>
<td>MED</td>
<td>DISC</td>
<td>1,200</td>
</tr>
</tbody>
</table>
The theft of an employee's unencrypted laptop resulted in the exposure of patient information. The laptop was stolen from an employee's car on April 9 and contained email records. Patient names, medical record numbers, dates of birth, physician names, diagnoses, and dates of service may have been exposed.

Information Source: Media

PHH Corporation
Suwanee, Georgia

A former employee was indicted on charges related to misuse of applicant and employee personal information. Employee names, Social Security numbers, dates of birth, telephone numbers, email addresses, addresses, I-9 alien registration numbers, and other personal information may have been exposed. The issue was discovered on April 3.

Information Source: California Attorney General

Coinbase
San Francisco, California

A flaw in Coinbase's systems cause the information of some merchants to be exposed. Any merchant who created a "buy now" button, donate button, or hosted a payment page using Coinbase's Merchant Tools and posted a public link to it online had the page publicly visible on the internet. The page contained the company name, website, phone number, email address, and mailing address. Additionally, anyone could search for public Coinbase merchant payment pages and collect the email addresses of merchants. At least one phishing attack targeted merchants with an email that appeared to come from Coinbase.

Information Source: Media

Equity Trust Company
Elyria, Ohio

An unauthorized third party accessed Equity Trust Company's computer network. The breach was discovered at the end of January 2013 and notification letters were sent on April 15. Equity Trust customers may have had their names, Social Security numbers, addresses, and other information viewed by online intruders.

Information Source: California Attorney General

Administrative Office of the Courts - Washington
Olympia, Washington

The Administrative Office of the Courts provided a website for additional information: [www.courts.wa.gov/databreach](http://www.courts.wa.gov/databreach)

Those with questions may call 1-800-448-5584

A breach of the Administrative Office of the Courts' server resulted in the exposure of one million driver's license numbers between fall of 2012 and February of 2013. It was confirmed that at least 94 people had their Social Security numbers accessed. Up to 160,000 Social Security numbers could have been accessed. In April the court was able to confirm that public records and confidential information were exposed. People who were booked in a city or county jail within the state of Washington between September 2011 and December 2012 may have had their name and Social Security number accessed. Anyone who received a DUI citation in Washington state between 1989 and 2011, had a superior court criminal case in Washington state that was filed against them or resolved between 2011 and 2012, or had a traffic case in Washington filed or resolved in a district or municipal court between 2011 and 2012 may have had their names and driver's license numbers exposed.

Information Source: Media

Lutheran Social Services of South Central Pennsylvania
York, Pennsylvania

Lutheran Social Services became aware of a malware program that was on its software system. Resident names, Social Security numbers, dates of birth, Medicare numbers, medical diagnosis codes, payer names, and health insurance numbers may have been exposed. The breach was discovered in March and Lutheran Social Services had not involved investigators or police as of May 9.

Information
Hackers accessed Name.com servers and may have obtained usernames, email addresses, passwords, and credit card account information. Customer passwords and credit card information were encrypted. Customers were notified of the breach and received an email asking them to reset their passwords.

Information Source: Media

May 8, 2013  Name.com
Denver, Colorado

This notice appeared on Linode’s website on April 16, 2013: https://blog.linode.com/2013/04/16/security-incident-update/

Those with questions may email support@linode.com.

Hackers exploited an Adobe vulnerability and used it to access Linode Manager web servers. One of Linode’s web servers, parts of their source code, and their database were accessed. No other components of the Linode infrastructure were accessed by the hackers. Encrypted customer credit card numbers and passwords were obtained. The group HTP claimed responsibility for the hack.

Information Source: Media

May 8, 2013  Linode.com
Galloway, New Jersey

Nearly $41,000 in computer equipment was reported stolen from the Department of Family Support Services on May 7. The Division on Domestic Violence and a satellite senior center share the building where the theft occurred. The types of information that may have been on the device or devices were not reported.

Information Source: PHIPrivacy.net

May 7, 2013  Tomren Wealth Management
San Ramon, California

A server with client information was accessed by an unauthorized outside party between February 21 and March 6, 2013. The attack was an attempt to use the server for spam emailing. Client names, Social Security numbers, driver’s license information, and FSC broker account numbers may have been accessed.

Information Source: California Attorney General

May 7, 2013  Raleigh Orthopaedic Clinic
Raleigh, North Carolina

Raleigh Orthopaedic Clinic contracted with a vendor in order to have information from X-ray films transferred into electronic format. The X-ray film was actually sold by the unnamed vendor and melted harvest for silver by a recycling company in Ohio. Patient names and dates of birth were on the film. The Clinic does not believe that personally identifiable information was on the film.

Information Source: Media

May 7, 2013  Mapco
Brentwood, Tennessee

Customers who made purchases between March 19-25, April 14-15, or April 20-21 may have had their credit or debit card information compromised. Tennessee and six other Southern states may have been affected by the breach. It is not clear if the payment card information was taken inside the stores or outside of the stores at gas pumps.

UPDATE (06/10/2013): The accounts of consumers who used payment cards at 373 Mapco Express stores may have been affected. Two additional locations in Tennessee were affected on April 14 and 15. There are unnamed stores that may have been affected on April 20 and 21.

UPDATE (07/08/2013): Three lawsuits have been filed as a result of data stolen in three MAPCO breaches that occurred in March, April, and June.

Information Source: Media

May 6, 2013  California Department of Public Health (CDPH)
Sacramento, California

Those with questions may call (855) 737-1796.

A reel containing images of 2,000 State of California Birth Records from May through September of 1974 was found in a publicly accessible location. Names, Social Security numbers, addresses, and certain types of medical information were in the birth record images. People in Santa Clara, Santa Cruz, Shasta, Siskiyou, Solano, Sonoma, Stanislaus, Sutter, or Tehama counties and who were born or had a child born in 1974 between May and September were affected.

Information
Source: PHIPrivacy.net

May 3, 2013
University of Rochester Medical Center
Rochester, New York

MED PORT
537 (No SSNs or financial information exposed)

The loss of an unencrypted flash drive exposed sensitive patient information. The flash drive contained name, date of birth, weight, gender, telephone number, URMC internal medical record number, orthopaedic physician name, date of service, diagnosis, diagnostic study, procedure, and complications. The flash drive is believed to have been destroyed after ending up in the medical center laundry. It was not found.

Information
Source: PHIPrivacy.net

May 3, 2013
Schoenbar Middle School
Ketchikan, Alaska

EDU HACK Unknown

A ring of middle school students were able to gain access to and control of more than 300 computers by phishing for teacher administrative codes. At least 18 students were involved. The breach happened when students used software to imitate a legitimate software update on their computers. The students then asked teachers to enter administrative account information so that they could complete the software updates or installations. The phony software then stored teacher credentials. The students were then able to control 300 laptops belonging to other students by using the administrative credentials. The school believes that servers and sensitive information were not exposed. The breach occurred around Friday, April 26 and was discovered on Monday, April 29 when students noticed that other students appeared to be controlling student laptops remotely and reported the issue.

Information
Source: California Attorney General

May 2, 2013
Reputations.com
Redwood, California

BSO HACK Unknown

Reputations.com experienced a hack that exposed customer names, email addresses, mailing addresses, date of birth, and employment information. Additionally, some customers had their encrypted passwords stolen. Reputations.com immediately reset all customer passwords after learning about the breach. Customers are encouraged to change their passwords on other sites if they reused their Reputation.com password.

Information
Source: Media

May 2, 2013
Spellman High Voltage Electronics Corporation
Valhalla, New York

BSR INSD Unknown

A disgruntled employee announced his resignation and then was caught copying files from his computer to a flash drive. Employees at Spellman began experiencing transaction and intranet disruptions after the disgruntled employee left even though his access to company servers was disabled after discovery of his suspicious activities. The events began to occur sometime around January of 2012. An investigation of the events led to the arrest of the former employee and federal prosecutors claim that he caused enough mayhem to cost Spellman over $90,000 by using his knowledge of Spellman’s computer system and stolen passwords. The former employee pleaded not guilty.

Information
Source: Media

May 1, 2013
U.S. Department of Labor
Washington, District Of Columbia

GOV HACK Unknown

The Department of Labor’s website was found to have been infected with malware that spreads to visitors using the web browser Internet Explorer. Microsoft had already released a patch to address the Internet Explorer vulnerability and the malware targets users who have not taken advantage of the patch.

Information
Source: Media

May 1, 2013
U.S. Army Corps of Engineers’ National Inventory of Dams

GOV HACK Unknown

214
Users of the National Inventory of Dams received notification that their information was reset after a hack may have compromised usernames and passwords. Hackers obtained non-public information of around 8,100 major dams in the United States by breaching the database. The information included dam vulnerabilities and could be used by cyber terrorists.

Information Source: Media

May 1, 2013

Lakeshore Mental Health Institute, Middle Tennessee Mental Health Institute
Knoxville, Tennessee

Patient records were found on the floor at an abandoned hospital building named Waterside. The woman who discovered them was a former Lakeshore employee and she alerted a local news station. Names, Social Security information, case numbers, dates of birth, and other patient information were exposed.

UPDATE (06/27/2013): At least 20 boxes of patient records were found in an abandoned building at the Clover Bottom Campus of the Middle Tennessee Mental Health Institute. The records dated back to the 1980's and had been reviewed to confirm which had sensitive information that needed to be destroyed.

Information Source: PHIPrivacy.net

April 29, 2013

Hope Hospice
New Braunfels, Texas

Those with questions may call CEO Debra Houser-Bruchmiller's office at 800-499-7501.

An employee used an unsecured email to send sensitive patient information. Two separate administrative violations occurred on December 27, 2012 and on February 22, 2013. The issue was discovered on February 25. The information was secured on February 28, 2013. Patient names, referral sources, Hospice admission and discharge dates, the names of insurance providers, and chart numbers may have been exposed.

Information Source: PHIPrivacy.net

April 29, 2013

Gomez Gasoline and Automotive
Watsonville, California

Those with information or questions about the investigation may call 831-768-3350 or the anonymous tip line at 831-768-3544.

More than 50 reports of credit card fraud have been traced to people who were customers at Gomez Gasoline and Automotive. Police suspect that a credit-card skimming device was placed on one or more gas pumps. The skimming devices have been spotted at other gas stations.

Information Source: Media

April 28, 2013

Orthopedic Physician Associates, Proliance Surgeons
Seattle, Washington

Proliance Surgeons' breach notice can be found here: http://proliancesurgeons.adhostclient.com/images/PDF/websitenotice.pdf.

Those with questions may call 1-888-608-7344 or email hipaa@proliancesurgeons.com

An employee's car was the target of an April 1 break-in. A company laptop and 10 patient files were taken during the car theft. The paper files were recovered, but the laptop also contained patient information. Names, Social Security numbers, addresses, telephone numbers, health insurance information, names of providers, and the reasons for patients' appointments may have been included in emails stored on the laptop.

Information Source: PHIPrivacy.net

April 26, 2013

LivingSocial
Washington, District Of Columbia

As many as 50 million LivingSocial members may have had their names, email addresses, dates of birth, and encrypted passwords exposed by a cyber attack. Customer credit card information was not compromised. Customers were encouraged to change their passwords on any other sites on which they used the same or similar passwords.
**UPDATE (05/03/2013):** As many as 50 million accounts may have been affected. It is estimated that 29 million people used LivingSocial and many had multiple accounts.

**Information Source:** Media

**April 26, 2013**

*Life Flight (IHC Health Services Inc.)*

*Aurora, Oregon*

MED DISC 842 (107)

An administrative error caused the information of patients flown by Life Flight helicopters to be available online. Patients flown during April, May, and June of 2004 may have had unspecified information exposed. It was confirmed that 107 patients had their Social Security numbers exposed. It is unclear how long the information was available and if patients flown during additional months may have been affected. The information was moved to a secure server to address the breach.

**UPDATE (05/17/2013):** The sensitive information was available online as early as October 12, 2009.

**Information Source:** PHIPrivacy.net

**April 26, 2013**

*Upstate University Hospital*

*Syracuse, New York*

MED PORT 283 (No SSNs or financial information reported)

A portable electronic device was stolen from Upstate University Hospital on March 30 or 31. It contained the names, hospital medical record numbers, dates of birth, and diagnosis information of patients.

**Information Source:** PHIPrivacy.net

**April 25, 2013**

*Child and Family Services of New Hampshire*

*Manchester, New Hampshire*

MED PHYS 23 (No SSNs or financial information exposed)

Someone took 23 files from a secure area in the Child and Family Services of New Hampshire main office sometime between March 15 and March 18. The breach was discovered on March 19. The files contained client names, dates of birth, addresses, Medicaid numbers, notes from home visits, and other health information related to home visits.

**Information Source:** PHIPrivacy.net

**April 24, 2013**

*City of Berkeley*

*Berkeley, California*

GOV DISC 11,000

A media group who regularly collects public employee salary and benefit information released Social Security numbers after they were mistakenly included in a file that the City of Berkeley provided. The information was sent by Berkeley in March and the mistake was discovered in early April. Around 2,000 active staff members and 9,000 retirees were affected. Mistakenly released the Social Security numbers of the employees as well.

**Information Source:** Media

**April 23, 2013**

*Portal Healthcare Solutions, Glens Falls Hospital*

*Glens Falls, New York*

MED DISC 2,300 (No SSNs reported)

Two patients ran a google search of their names and were able to find their medical information online. Doctors' reports with medications, medical treatments, lab information, future and past treatment plans, physical examination information, and lifestyle information could be downloaded by anyone who found the information online. The documents were from November 2012 through January 2013 and discovered online in mid-March. Portal Healthcare secured the sensitive information on its servers on March 14. A lawsuit was filed against Glens Falls Hospital, Portal Healthcare Solutions LLC, and Carpathia Hosting in mid-April for patient privacy violations.

**Information Source:** PHIPrivacy.net

**April 23, 2013**

*Hostgator*

*Houston, Texas*

BSO INSD Unknown

An employee was found to have installed backdoors on more than 2,700 company servers. The issue was discovered the day after the dishonest employee was dismissed. He worked for Hostgator from September 2011 to February 15, 2012. The dishonest employee was arrested and charged with breach of computer security.
Kmart, Sears
Little Rock, Arkansas
April 23, 2013

An assistant manager was forced to open a Kmart safe and give a thief access to $6,000 in cash and an unencrypted backup disk with a day’s worth of customer information. The backup disk contained names, addresses, dates of birth, prescription numbers, prescription providers, insurance cardholder IDs and drug names. The armed robbery occurred on March 17.

Macy’s
Lafayette, Indiana
April 23, 2013

A man guessed or accessed the Social Security numbers of Macy’s customers in order to exploit a Macy’s policy for the purpose of making fraudulent purchases. He then created ID cards that paired his picture with the customer information. A Macy’s policy allowed him to charge purchases to the accounts of other Macy’s customers by using their Social Security numbers and showing his falsified IDs.

City of Monroeville
Monroeville, Pennsylvania
April 23, 2013

A number of inappropriate security practices may have exposed the information of people who called Monroeville’s 911 dispatch center, police department, fire department, or EMS department in 2012 or 2013. Monroeville is being investigated for possible violations of federal health privacy laws. An August 2012 complaint to the U.S. Department of Health and Human Services’ Office for Civil Rights stated that protected health information may have been given to a former police chief via email and that weak and poorly managed usernames and passwords were used to access a database of 911 callers’ medical information.

UPDATE (07/18/2013): Monroeville 911 records from August 2010 through February 2013 were available to volunteer firefighters and former and inactive emergency responders. There was no protocol in place for removing the former personnel from the list of people who received 911 dispatch data.

OneWest Bank
Pasadena, California
April 23, 2013

A OneWest service provider suffered an unauthorized network intrusion during the first quarter of 2011. OneWest client names, Social Security numbers, addresses, dates of birth, phone numbers, driver’s license numbers, and passport numbers may have been exposed.

Erlanger Health System, Erlanger Hospital
Chattanooga, Tennessee
April 17, 2013

Erlanger Health System sent notes to 87 families and apologized for an incident that left the patient records of children exposed. The records contained names, Social Security numbers, phone numbers, and diagnosis information. Erlanger has not been made aware of the records being used in an unauthorized manner.

Arizona Counseling and Treatment Services (ACTS), Cenpatico Behavioral Health of Arizona
Yuma, Arizona
April 17, 2013

The home theft of any employee’s laptop and external drive resulted in the exposure of patient information. The theft occurred sometime between March 18 and March 25; other items were stolen besides the laptop and hard drive. Neither the laptop nor the hard drive were encrypted. Patients who visited either Cenpatico or its contractor ATS between 2011 and 2013 may have had their names, dates of birth, and treatment plans exposed.

UPDATE (04/17/2013): More than 3,000 patients were affected by the breach.
April 16, 2013  Schneck Medical Center
Seymour, Indiana

A Schneck Medical Center employee gave a presentation that was later placed online. People who searched through the files from the presentation could find the names of 3,000 Schneck Medical Center patients. The presentation was removed from online and Google removed all cached information from the Internet.

Information
Source:
Media

April 16, 2013  Iberdola USA, Central Maine Power
Augusta, Maine

A hack of Iberdrola USA's recruitment website may have exposed the information of anyone who applied for a job at Central Maine Power or any of its sister companies since January 2007. Rochester Gas and Electric Corp and New York State Electric and Gas Corp. were also affected.

Information
Source:
PHIPrivacy.net

April 15, 2013  Wawa
Burlington, New Jersey

Customers who shopped at a Wawa on Salem Road in Burlington, New Jersey noticed fraudulent purchases on their credit cards. Investigators were able to trace the fraud to four people and arrest them. The four men were charged with credit card theft, credit card fraud, identity theft, and having electronic devices for criminal use. More victims are expected to be found.

Information
Source:
Media

April 12, 2013  Chapman University
Orange, California

An administrative error caused the personal information of some students to be exposed online. The issue was discovered on February 27. Authenticated users of Chapman’s on-campus network could have viewed names, Social Security numbers, student identification numbers, and dates of birth. The documents were blocked from access by unauthorized users once the breach was discovered.

Information
Source:
California Attorney General

April 12, 2013  Pentagon
Washington, District Of Columbia

Lawyers working with Guantanamo Bay detainees had to pause their work after being told to stop using the Pentagon’s computer system. An unspecified issue left over 500,000 emails unsafe to access or deleted from a Pentagon common drive. The breach left defense files unsecured and it may have been possible for prosecutors to view confidential defense emails.

Information
Source:
Media

April 11, 2013  Chapman University
Orange, California

Sensitive documents could have been viewed electronically by authenticated users of the on-campus network. The issue was discovered on February 27. Names, Social Security numbers, student identification numbers, and dates of birth may have been viewed by people who could log into Chapman’s system, but shouldn't have been able to access the information.

Information
Source:
California Attorney General

April 10, 2013  Schnuck Markets Inc.
St. Louis, Missouri

218
A lawsuit was filed against Schnucks Markets Inc. after customers learned that Schnucks failed to warn customers about a data breach within two weeks. On March 15, Schnucks learned that a portion of their loyalty cards were affected, but waited until March 30 to send a press release. Customer payment card numbers and expiration dates were exposed through a magnetic strip swiping security breach. No customer names were exposed.

UPDATE (04/15/2013): The breach affected about 2.4 million customer debit and credit cards at 79 Schnucks locations. Payment cardholders’ contact and identifying information were not exposed. Customers who visited a Schnucks between December of 2012 and March 29, 2013 may have been affected.

UPDATE (05/24/2013): A class action lawsuit was filed against Schnuck Markets in early May. Schnuck Markets claims that the lawsuit belongs in federal court because of the case's scope and damages. The lawsuit sought damages from Schnucks for time and effort that affected individuals had to put into monitoring and managing compromised credit card information. The lawsuit also alleges Schnucks of willful and wanton neglect, a charge for which punitive damages are available under Illinois law. However Schnucks states that the “time and effort” claims for Illinois alone easily exceed the $5 million threshold for federal consideration.

UPDATE (06/21/2013): A new estimate from Schnucks states that 500,000 unique credit or debit cards may have been involved.

UPDATE (07/11/2013): After a review, the Missouri Attorney General’s office has stated that Schnuck Markets did not violate state data security law.

UPDATE (08/31/2013): Liberty Mutual Insurance Co. is suing Schnuck Markets Inc. Liberty Mutual claims that it should not be held liable for eight lawsuits filed against Schnucks.

Information Source: Media
April 9, 2013 VUDU Santa Clara, California

Those with questions may call 855-968-8838 or email passwordreset@vudu.com.

A March 24, 2013 VUDU office theft resulted in the exposure of customer information. Hard drives with customer names, addresses, email addresses, account activity, dates of birth, and encrypted passwords were stolen. Customers who used their VUDU passwords for other sites should change the passwords on other sites as well.

Information Source: Media
April 9, 2013 Kirkwood Community College Cedar Rapids, Iowa

Hackers accessed Kirkwood Community College’s website and applicant database system on March 13. Anyone who applied to a Kirkwood Campus may have had their names, Social Security numbers, dates of birth, race, and contact information exposed. People who applied to take Kirkwood college-credit classes between February 25, 2005 and March 13, 2013 were affected.

Information Source: Media
April 9, 2013 Hospice Palliative Care of Alamance-Caswell, LifePath Home Health Burlington, North Carolina

The February 24 burglary of three laptops resulted in the exposure of patient information. The laptops were stolen from the hospital in addition to needles, syringes, and miscellaneous items. The unencrypted laptops contained emails that had sensitive patient information.

Information Source: Media
April 9, 2013 Connextions, Anthem Blue Cross Blue Shield of Indiana, Anthem Blue Cross Blue Shield of Ohio, Empire Blue Cross Blue Shield of Indiana Orlando, Florida

A Connextions employee used Social Security numbers from a number of other organizations for criminal activity. At least four members of Anthem Blue Cross and Blue Shield were affected by the criminal activity. The breach was reported on HHS as affecting 4,814 patients, but more were affected.

Information Source: HHS via PHIPrivacy.net
April 9, 2013 Works Bakery Cafe Portland, Maine
Customers who used a debit or credit card at any Works Bakery Cafe location are advised to check their payment cards for fraudulent activity. A breach occurred when malware was introduced to the Works Bakery Cafe computer system. Locations in Durham, Manchester, Keene, Concord, Brattleboro Vermont, and Portland Maine were affected.

Information
Source: Media
April 7, 2013
Agincourt Wallboard
Westbrook, Maine
BSR HACK Unknown

On, January 19, Agincourt Wallboard notified employees of a breach of its payroll system. Agincourt Wallboard became aware of the issue on January 17 when eight employees reported receiving a physical payroll check. Someone had entered Agincourt Wallboard’s payroll vendor and edited information without authorization so that the employees received a physical check rather than an electronic deposit. The person who hacked into the payroll vendor also attempted to change the bank routing information for 10 of its employees. Agincourt Wallboard is investigating how the hacker could have obtained the administrator’s credentials and notified employees of the issue immediately. Agincourt Wallboard also learned that five of the computers on its network were infected with malware called a Trojan horse.

Information
Source: Media
April 5, 2013
Scribd
San Francisco, California
BSO HACK

A hack affected less than 1% of Scribd’s 50 million users. "A few hundred thousand" users had their passwords stolen. Users who were affected received instructions for resetting passwords. The passwords were encrypted and it is unlikely that hackers were able to decrypt and use the passwords before Scribd and Scribd users learned of the breach.

Information
Source: Media
April 5, 2013
William Jennings Bryan Dorn VA Medical Center
Columbia, South Carolina
MED PORT 7,405

The February 11 theft of an unencrypted laptop from the respiratory department resulted in the exposure of patient information. Veterans who were patients may have had their name, Social Security number, age, race, weight, and medical test results on the laptop. The laptop was taken during regular clinic hours.

UPDATE (05/01/2013): A lawsuit has been filed by two veterans on behalf of people who were affected by the breach.

UPDATE (07/22/2013): The Dorn VA has motioned to dismiss the case. On July 16 the Dorn VA said that it has not been proven that the records were improperly disclosed. It also argued that the plaintiffs never asserted that the records had been shown to another or unauthorized person.

Information
Source: PHIprivacy.net
April 3, 2013
United HomeCare Services, Inc., United Home Care Services of Southwest Florida, LLC
Fort Myers, Florida
MED PORT 13,617

A total of 12,299 United HomeCare Services, Inc. clients were affected. Additionally, 1,318 United Home Care Services of Southwest Florida clients were affected.

The January 8 theft of a billing manager’s laptop resulted in the exposure of patient information. It was stolen from the manager’s car. It contained client names, Social Security numbers, health plan numbers, dates of birth, and addresses dating as far back as 2002. Some patients may have also had treatment service codes or diagnostic codes on the laptop.

Information
Source: HHS via PHIprivacy.net
April 3, 2013
Computer Sciences Corporation
Raleigh, North Carolina
BSO PORT Unknown

A thumb drive with information from the Medicare Exclusion Database was placed on a thumb drive. The thumb drive was discovered to be missing from the CSC facilities in Raleigh, North Carolina in early March; it had most likely been lost in late February. The thumb drive contained names, Social Security numbers, federal tax Employer Identification numbers, dates of birth, and other information.

A hacker may have accessed credit card information, names, and addresses associated with Shoplet accounts. The breach was discovered on January 11, 2013. A new firewall was installed and Ellison Systems, Inc. moved their database server to a more secure zone.

Information Source:  California Attorney General

April 1, 2013  Oregon Health and Science University  Portland, Oregon  MED  PORT  4,022 (Nine Social Security Numbers reported)

The theft of a surgeon’s unencrypted laptop resulted in the exposure of patient information.

UPDATE (04/25/2013): The laptop was stolen from a surgeon’s Hawaii rental home and was used for research purposes. Any laptops used for patient care are required to be encrypted while laptops used for research are not required to be encrypted. The laptop was used to access emails related to patient care such as patient names, medical record numbers, types of surgery and dates of surgery, times and locations of surgery, gender, age, and name of surgeon and anesthesiologist information. Nine patients had their Social Security numbers exposed.

Information Source:  Media

April 1, 2013  Granger Medical Clinic  West Valley City, Utah  MED  PHYS  2,600 (No SSNs or financial information reported)

A total of 2,600 medical appointment records disappeared before they could be shredded. The records contained patient names, dates of appointments, times of appointments, and reason for appointment. No medical claim information, financial information, or Social Security numbers were exposed.

Information Source:  Media

April 1, 2013  Tennis Express, American Express  Houston, Texas  BSR  HACK  Unknown

A hacker or hackers accessed Tennis Expresses computer network on or around December 19, 2012. The breach was discovered in mid-February of 2013. The issue was caused by a vulnerability in a third party vendor program. Names, addresses, credit card numbers, verification value, and expiration dates may have been exposed.

Information Source:  California Attorney General

March 31, 2013  Allen County  Lima, Ohio  GOV  DISC  1,100

An administrative error caused the Social Security numbers and other personal information of Allen County employees to be available online for less than an hour.

Information Source:  Media

March 29, 2013  Washington Department of Social and Health Services  Gig Harbor, Washington  GOV  PORT  652

A private contractor working for the Department of Social and Health Services discovered that their laptop had been stolen on February 4. The laptop was recovered in a pawn shop on February 14. It contained the names, ID numbers, psychological evaluations, dates of birth, diagnoses, dates of services, addresses, and last four digits of Social Security numbers of clients.

UPDATE (10/14/2013): The private contractor was a psychologist who had his license suspended as a result of the incident. The Washington State Department of Health suspended the license after a history of being charged with unprofessional conduct. He is accused of misrepresenting the number of people who could be affected by the breach and failing to report it to the Department of Social and Health Services until five days after the breach.

Information Source:  Media
Hackers were able to access and disrupt American Express' website. American Express was offline for two hours.

**Information**  
**Source:**  
Media

**March 28, 2013**  
**MedStar Good Samaritan Nursing Center, Mid America Health, Inc. (MAH)**  
**Baltimore, Maryland**

A paper file was stolen from the car of a dental assistant who was treating residents at the MedStar Good Samaritan Nursing Center. The file contained names, dates of birth, medical and dental evaluation information, medical and dental providers' names and license numbers, and the Social Security numbers of three residents.

**Information**  
**Source:**  
PHIPrivacy.net

**March 28, 2013**  
**Tooele County**  
**Tooele, Utah**

A former employee received a CD with the names and Social Security numbers of around 200 current and former employees when he requested his personnel file. The disc may have held the information of employees who signed up for a specific dental insurance plan in 1996 and workers who joined the Utah Public Employees Association in 1999. When the HR department realized their mistake they requested that the former employee return the CD. He initially refused; he then gave the CD to the Tooele County Attorney's office.

**Information**  
**Source:**  
Media

**March 28, 2013**  
**Citi**  
**Irving, Texas**

Current and former parties involved in a bankruptcy proceeding for a Citi loan may have had their information exposed. Citi filed legal documents that should have been concealed but were accidentally made available online. The information, which included personally identifiable and loan related information, could be exposed and read by any person who accessed court records. The issue was addressed and Citi is not aware of any instances where information was accessed.

**Information**  
**Source:**  
California Attorney General

**March 28, 2013**  
**JPMorgan Chase**  
**New York, New York**

JPMorgan Chase's website was taken offline by a hacker or hackers. The website was made unavailable by a denial-of-service attack. Chase.com was down for around a day.

**Information**  
**Source:**  
Media

**March 28, 2013**  
**Mid America Health**  
**Greenwood, Indiana**

The theft of a laptop resulted in the exposure of patient information. Names, Social Security numbers, dates of birth, residential facility names, and digital oral x-ray images may have been exposed. Specific details of the case are being withheld until the breach investigation has concluded.

The location of the breach is listed as the corporate headquarters of MAH. Those with questions or concerns may contact the MAH Compliance Department at 1-855-224-0004.

**Information**  
**Source:**  
PHIPrivacy.net

**March 27, 2013**  
**Rollins, Inc.**  
**Atlanta, Georgia**

An administrative error caused a mailing distribution to contain the Social Security numbers of some people. Rollins learned of the issue on March 12. The Rollins TODAY quarterly issue mailed during the week of March 4 contained Social Security numbers within a number sequence on the mailing label.

**Information**  
**Source:**
March 26, 2013  Texas Tech University Health Sciences Center (TTUHSC)  Lubbock, Texas

Patients with questions may call (877) 272-0570.

An administrative error caused the billing statements of around 700 patients to be sent to the mailing addresses of other patients. Patient names, account numbers, invoice numbers, charge amounts, dates of service, department and provider names, adjustment amounts, payments from insurance companies, amounts due, and total account balances may have been exposed.

March 26, 2013  The Finish Line, Inc.  Indianapolis, Indiana

The January 11 theft of an employee's laptop resulted in the exposure of sensitive information. The laptop was stolen from the employee's vehicle and contained names, Social Security numbers, and other information related to current and former Finish Line staff.

March 22, 2013  Comfort Inn and Suites  Willard, Missouri

A dishonest employee working at a Comfort Inn and Suites in Willard, Missouri during 2009 worked with a conspirator to misuse the information of hotel customers. They were ordered to pay restitution of $23,000. The dishonest employee was sentenced to three years of probation and her accomplice was sentenced to 42 months for aggravated identity theft and conspiracy to commit wire fraud.

March 22, 2013  University of Mississippi Medical Center (UMMC)  Jackson, Mississippi

A laptop used by UMMC clinicians was discovered missing on January 22. The password-protected laptop contained information from patients who entered the hospital between 2008 and 2013. Patient names, Social Security numbers, addresses, diagnoses, medications, treatments, dates of birth, and other personal information may have been exposed.

UPDATE (04/25/2013): The laptop may have been lost or stolen in November of 2012.

March 22, 2013  Tallahassee Community College (TCC)  Tallahassee, Florida

Federal investigators informed Tallahassee Community College that a hacker gained access to their main computer system. The personal information of students who applied for financial aid may have been accessed. It appears that an insider hacked into the computer system. Hacked 2011 TCC financial aid records were misused to file fraudulent tax refunds. Federal Investigators told TCC when they traced where the information came from.

March 22, 2013  United Shore Financial Services, LLC  Troy, Michigan

A computer intrusion resulted in the exposure of names, Social Security numbers, contact information, dates of birth, driver's license numbers, and financial account information. The breach occurred sometime around December 2, 2012.

March 22, 2013  OCS America, Inc.  Long Island City, New York

A phishing attack affected an OCS America computer on March 4, 2013. The computer contained names, Social Security numbers, addresses, telephone numbers, dates of birth, job titles, and salary information. It appears that only one computer was affected.
Information Source: California Attorney General
March 22, 2013  
**TLO, LLC**  
Boca Raton, Florida

BSO  HACK  Unknown

On January 15, 2013 TLO discovered that there had been limited fraudulent access to their system. A hacker or hackers were able to access names, Social Security numbers, and driver’s license numbers between August 2012 and January 2013.

---

Information Source: California Attorney General
March 21, 2013  
**National Institute of Aerospace, National Aeronautics and Space Administration (NASA)**  
Hampton, Virginia

NGO  INSD  Unknown

A Chinese national who worked as a contractor for the National Institute of Aerospace had access to NASA’s Langley Research Center. He was caught boarding a plane with two external hard drives, two laptops, a memory stick, and an SIM card on March 16. He originally did not reveal the second laptop, hard drive, and SIM card when detained. The information he was attempting to steal was not revealed.

---

Information Source: Media
March 21, 2013  
**Insurance Co. of the West (ICW)**  
Del Mar, California

BSF  PHYS  Unknown

Confidential medical records were found under a freeway by a concerned citizen. A local news team investigation traced the documents back to the insurance claims processor ICW. ICW reported that the issue occurred on February 28 when a bin with files broke open on the way to a disposal site. An unnamed document destruction company responsible for the documents was replaced. Names, dates of birth, Social Security numbers, and other sensitive and medical information were on the documents.

---

Information Source: Media
March 20, 2013  
**Savannah River Site (SRS)**  
Aiken, South Carolina  

GOV  DISC  12,000

A security breach allowed access to the personal records of at least 12,000 SRS workers. The breach does not appear to be the result of a cyber attack. Workers may have had financial information exposed.

---

Information Source: Media
March 19, 2013  
**Subway**  
California

BSR  HACK  Unknown

No specific California city was involved. Subway restaurants in California, Massachusetts, and Wyoming were involved.

A former owner of a Subway franchise used software from his new job to access the computer systems of Subway restaurants. The former owner sold point-of-sale software to Subway restaurants across the country and then worked with an accomplice to remotely hack into at least 13 Subway point-of-sale systems. The fraud began in 2011. Fraudulent Subway gift cards totaling at least $40,000 were created. Two of the California participants were indicted on March 6.

---

Information Source: Media
March 19, 2013  
**General Services Administration (GSA)**  
Washington, District Of Columbia

GOV  DISC  Unknown

GSA users may have been able to view the financial information and trade secrets of other GSA users due to a security vulnerability. The specific database that was affected is called the System for Award Management (SAM). Contractor and vendor registration records are cataloged by SAM. It is not clear how GSA became aware of the issue or how long it was a problem. Agency officials revealed that users could purposefully or inadvertently view the information of other users after following a series of steps.

**UPDATE** (03/23/2013): Users had Social Security numbers and tax identification numbers exposed.

---

Information Source: Media
March 16, 2013  
**Salem State University**

EDU  HACK  25,000
A server was found to be infected with a virus. The University computer contained information related to paychecks distributed by the University. Current and former employees who may have been students or staff may have been affected.

Information Source: Media
March 16, 2013 Lawrence Melrose Medical Electronic Record, Inc. Melrose, Massachusetts

Patients at Baystate Gastroenterology, Hallmark Health Medical Associates, Main Street Family Practice, and Women's Healthcare Associates were affected. Patients of Maury Goldman, MD and John Mudrock, MD were also affected.

An employee of Lawrence Melrose accessed patient information for reasons unrelated to their work. It is unclear what type of patient information was exposed and how many patients were affected.

Information Source: PHIPrivacy.net
March 15, 2013 Tribune Co. Sacramento, California

A former employee revealed a password and username combination for Tribune Co. to hackers. The hackers were part of the anonymous and used the information to access Tribune Co.'s servers in 2010. A number of online stories that had been published through Tribune Co. were defaced by hackers as a result.

The former employee of a TV station owned by Tribune Co. was indicted on charges of conspiracy to cause damage to a protected computer, transmission of malicious code, and attempted transmission of malicious code.

UPDATE (04/23/2013): The former employee worked at Reuters as a deputy social media editor at the time of the cyber attack. He was fired from Reuters in April of 2013.

Information Source: Media
March 11, 2013 Stanley Black & Decker, Inc. New Britain, Connecticut

Those with questions or concerns may contact (877) 795-2356.

The theft of an employee's laptop resulted in the exposure of information from employees and people who received checks from Stanley Black & Decker. Names, and the account numbers and routing numbers associated with direct deposits may have been exposed. The laptop was stolen from a finance employee on January 28.

Information Source: California Attorney General
March 8, 2013 University of Connecticut Health Center Farmington, Connecticut

An employee accessed patient records for reasons unrelated to their job function. The Health Center became aware of an unauthorized access in January of 2013. Patient names, addresses, dates of birth, and, in some cases, health information and Social Security numbers may have been exposed.

Information Source: Media
March 7, 2013 Uniontown Hospital Uniontown, Pennsylvania

A hacker or hackers accessed patient information and posted it online. The breach was discovered by a data privacy expert. Uniontown indirectly notified the public of the breach and breach containment after the privacy expert attempted to reach Uniontown Hospital for several days. Names, encrypted passwords, contact names, email addresses, and usernames may have been exposed. It is unclear how long the information was available.

Information Source: PHIPrivacy.net
March 4, 2013 TD Bank, N.A. Cherry Hill, New Jersey
Two backup tapes with customer and customer dependent names, Social Security numbers, addresses, account numbers, debit card numbers, and credit card numbers went missing while being transported between two TD Bank office locations in March of 2012.

Information Source: California Attorney General

March 4, 2013 The Prudential Insurance Company of America, Unisys Newark, New Jersey BSF DISC Unknown

An administrative error resulted in documents with sensitive information from Unisys members being emailed to an incorrect party associated with Unisys. The mistake occurred on December 13, 2012. The document may have contained names, Social Security numbers, dates of birth, and salary information. The mistake was immediately noticed by the recipient and the information was deleted from their computer.

Information Source: California Attorney General

March 4, 2013 Family Intervention Services Hiram, Georgia MED PHYS Unknown

A caller contacted a local news team member and an investigation of mishandled medical documents began. The documents were in an unlocked dumpster and contained Social Security numbers, bank account information, addresses, dates of birth, and health information. The documents were associated with Family Intervention Services and an unnamed orthopedic office.

Information Source: PHIPrivacy.net

March 3, 2013 Evernote Redwood City, California BSO HACK 50,000,000 (No SSNs or financial information reported)

Evernote's breach notice can be found here: http://evernote.com/corp/news/password_reset.php.

A hacker or hackers attacked and may have accessed Evernote's online system. Evernote reset all user passwords as a precaution. User names, email addresses, and encrypted passwords may have been exposed.

UPDATE (03/09/2013): A total of 50 million users were told to reset their passwords.

Information Source: Media

March 1, 2013 Samaritan Hospital, Rensselaer County Jail Troy, New York MED INSD Unknown

A nursing supervisor of Rensselaer County Jail was found to have misused credentials to access patient records without cause. The Rensselaer County Jail information is maintained by Samaritan Hospital. The hospital learned of the breach in November 2011, disabled the employee's account, and notified the sheriff's office immediately. Subsequently, the Hospital may have delayed notifying patients because of the ongoing investigation. Notifications were sent out during the first week of March in 2013.

UPDATE (04/01/2013): A total of 48 people have been notified. Patients from as far back as 2006 may have been affected.

Information Source: PHIPrivacy.net

March 1, 2013 South Miami Hospital, Baptist Health Miami, Florida MED INSD 834

A dishonest hospital employee misused patient records that were dated from June 2011 to February of 2012. Patients may have had their names, Social Security numbers, and dates of birth exposed.

UPDATE (03/15/2013): A respiratory therapist provided Social Security numbers, dates of birth, patient names, and other patient data in exchange for payment. The patient data was then used to file fraudulent tax returns. The dishonest employee now faces charges for selling the information to two others.

UPDATE (04/26/2013): Two women who purchased patient information from a Hospital employee were sentenced for their roles in the breach. One woman was sentenced to 26 years and five months in federal prison in addition to being ordered to pay over $1.9 million in restitution. She was convicted of 33 fraud and identity theft charges in January. The other was sentenced to 10 years and one month in prison after pleading guilty to conspiracy to defraud the government and aggravated identity theft. The fraud ring produced fraudulent income tax refunds totalling $11.7 million.
UPDATE (07/18/2013): A respiratory therapist who engaged in the theft of patient information between June of 2011 and February of 2012 pleaded guilty. She faces up to seven years in federal prison and is scheduled to receive a lightened sentence for cooperating with authorities in the investigation of the tax fraud ring’s leaders.

Information
Source: PHIPrivacy.net
March 1, 2013

**Bank of Hawaii, First Hawaiian Bank**
Oahu, Hawaii

BSR HACK Unknown

An unnamed restaurant in Oahu experienced a computer system breach. Customers who visited the restaurant during a period in February had their credit and debit cards blocked by Bank of Hawaii and First Hawaiian Bank when the breach was discovered. Not all of the payment cards that were blocked had been compromised.

Information
Source: Media
March 1, 2013

**Fabric Depot**
Portland, Oregon

BSR HACK Unknown

An unnamed restaurant in Oahu experienced a computer system breach. Customers who visited the restaurant during a period in February had their credit and debit cards blocked by Bank of Hawaii and First Hawaiian Bank when the breach was discovered. Not all of the payment cards that were blocked had been compromised.

Information
Source: California Attorney General
February 28, 2013

**First National Bank of Southern California**, California

BSF PORT Unknown

On January 7, 2013 Fabric Depot became aware of a breach that had occurred sometime around October 16, 2012. Fabric Depot changed their online payment system and notified customers. Customer names, credit card numbers, credit card verification codes, debit card numbers, and account billing addresses may have been exposed.

Information
Source: California Attorney General
February 28, 2013

**First National Bank of Southern California**, California

BSF PORT Unknown

On January 7, 2013 Fabric Depot became aware of a breach that had occurred sometime around October 16, 2012. Fabric Depot changed their online payment system and notified customers. Customer names, credit card numbers, credit card verification codes, debit card numbers, and account billing addresses may have been exposed.

Information
Source: California Attorney General
February 28, 2013

**First National Bank of Southern California**, California

BSF PORT Unknown

On January 7, 2013 Fabric Depot became aware of a breach that had occurred sometime around October 16, 2012. Fabric Depot changed their online payment system and notified customers. Customer names, credit card numbers, credit card verification codes, debit card numbers, and account billing addresses may have been exposed.

Information
Source: California Attorney General
February 28, 2013

**First National Bank of Southern California**, California

BSF PORT Unknown

On January 7, 2013 Fabric Depot became aware of a breach that had occurred sometime around October 16, 2012. Fabric Depot changed their online payment system and notified customers. Customer names, credit card numbers, credit card verification codes, debit card numbers, and account billing addresses may have been exposed.

Information
Source: California Attorney General
February 28, 2013

**First National Bank of Southern California**, California

BSF PORT Unknown

On January 7, 2013 Fabric Depot became aware of a breach that had occurred sometime around October 16, 2012. Fabric Depot changed their online payment system and notified customers. Customer names, credit card numbers, credit card verification codes, debit card numbers, and account billing addresses may have been exposed.

Information
Source: California Attorney General
February 28, 2013

**First National Bank of Southern California**, California

BSF PORT Unknown

On January 7, 2013 Fabric Depot became aware of a breach that had occurred sometime around October 16, 2012. Fabric Depot changed their online payment system and notified customers. Customer names, credit card numbers, credit card verification codes, debit card numbers, and account billing addresses may have been exposed.

Information
Source: California Attorney General
February 28, 2013

**First National Bank of Southern California**, California

BSF PORT Unknown

On January 7, 2013 Fabric Depot became aware of a breach that had occurred sometime around October 16, 2012. Fabric Depot changed their online payment system and notified customers. Customer names, credit card numbers, credit card verification codes, debit card numbers, and account billing addresses may have been exposed.

Information
Source: California Attorney General
February 28, 2013

**First National Bank of Southern California**, California

BSF PORT Unknown

On January 7, 2013 Fabric Depot became aware of a breach that had occurred sometime around October 16, 2012. Fabric Depot changed their online payment system and notified customers. Customer names, credit card numbers, credit card verification codes, debit card numbers, and account billing addresses may have been exposed.

Information
Source: California Attorney General
February 28, 2013

**First National Bank of Southern California**, California

BSF PORT Unknown

On January 7, 2013 Fabric Depot became aware of a breach that had occurred sometime around October 16, 2012. Fabric Depot changed their online payment system and notified customers. Customer names, credit card numbers, credit card verification codes, debit card numbers, and account billing addresses may have been exposed.

Information
Source: California Attorney General
February 28, 2013

**First National Bank of Southern California**, California

BSF PORT Unknown

On January 7, 2013 Fabric Depot became aware of a breach that had occurred sometime around October 16, 2012. Fabric Depot changed their online payment system and notified customers. Customer names, credit card numbers, credit card verification codes, debit card numbers, and account billing addresses may have been exposed.

Information
Source: California Attorney General
February 28, 2013

**First National Bank of Southern California**, California

BSF PORT Unknown

On January 7, 2013 Fabric Depot became aware of a breach that had occurred sometime around October 16, 2012. Fabric Depot changed their online payment system and notified customers. Customer names, credit card numbers, credit card verification codes, debit card numbers, and account billing addresses may have been exposed.

Information
Source: California Attorney General
February 28, 2013

**First National Bank of Southern California**, California

BSF PORT Unknown

On January 7, 2013 Fabric Depot became aware of a breach that had occurred sometime around October 16, 2012. Fabric Depot changed their online payment system and notified customers. Customer names, credit card numbers, credit card verification codes, debit card numbers, and account billing addresses may have been exposed.

Information
Source: California Attorney General
February 28, 2013

**First National Bank of Southern California**, California

BSF PORT Unknown

On January 7, 2013 Fabric Depot became aware of a breach that had occurred sometime around October 16, 2012. Fabric Depot changed their online payment system and notified customers. Customer names, credit card numbers, credit card verification codes, debit card numbers, and account billing addresses may have been exposed.

Information
Source: California Attorney General
February 28, 2013

**First National Bank of Southern California**, California

BSF PORT Unknown

On January 7, 2013 Fabric Depot became aware of a breach that had occurred sometime around October 16, 2012. Fabric Depot changed their online payment system and notified customers. Customer names, credit card numbers, credit card verification codes, debit card numbers, and account billing addresses may have been exposed.

Information
Source: Media
February 27, 2013

**Information Handling Services, Inc. (IHS)**
Englewood, Colorado

BSO HACK Unknown

Hackers breached the servers of IHS and may have been able to access credit card, customer, and nuclear information. IHS does not believe that confidential information was compromised. However, the hacker group claimed to have obtained the records of 8,500 customers. The hacker group is known to attack sites in order to further their goal of revealing sensitive nuclear data to pressure the Israeli government and others into disclosing their nuclear activities.

UPDATE (05/13/2013): The unauthorized parties acquired the relevant data from the IHS Jane’s environment on or about November 22, 2012.

Information
Source: Media
February 27, 2013

**Bit9, Inc.**
Waltham, Massachusetts

BSO HACK Unknown

Hackers were able to exploit a vulnerability in a web application and use an SQL injection. The breach occurred in July of 2012, however the server was shut down until January of 2013. Hackers then used Bit9’s systems to attack other organizations who relied on Bit9 as a security platform vendor. Three unnamed companies were affected. The vulnerability was caused by Bit9 failing to install its own security software.

Information
Source: Media
February 26, 2013

**Massachusetts Mutual Life Insurance Company, Convey Compliance Systems, Inc.**
Springfield, Massachusetts

BSF DISC Unknown

An error at Convey Compliance Systems, Inc. resulted in 1099 forms being mailed to incorrect addresses. The 1099 forms contained names, Social Security numbers, tax identification numbers, and addresses. The financial information of some Massachusetts Mutual Life Insurance Company clients was exposed.

Information
Source: California Attorney General
February 26, 2013

**Massachusetts Mutual Life Insurance Company, Convey Compliance Systems, Inc.**
Springfield, Massachusetts

BSF DISC Unknown

An error at Convey Compliance Systems, Inc. resulted in 1099 forms being mailed to incorrect addresses. The 1099 forms contained names, Social Security numbers, tax identification numbers, and addresses. The financial information of some Massachusetts Mutual Life Insurance Company clients was exposed.

Information
Source: California Attorney General
February 26, 2013

**Massachusetts Mutual Life Insurance Company, Convey Compliance Systems, Inc.**
Springfield, Massachusetts

BSF DISC Unknown

An error at Convey Compliance Systems, Inc. resulted in 1099 forms being mailed to incorrect addresses. The 1099 forms contained names, Social Security numbers, tax identification numbers, and addresses. The financial information of some Massachusetts Mutual Life Insurance Company clients was exposed.

Information
Source: California Attorney General
February 26, 2013

**Massachusetts Mutual Life Insurance Company, Convey Compliance Systems, Inc.**
Springfield, Massachusetts

BSF DISC Unknown

An error at Convey Compliance Systems, Inc. resulted in 1099 forms being mailed to incorrect addresses. The 1099 forms contained names, Social Security numbers, tax identification numbers, and addresses. The financial information of some Massachusetts Mutual Life Insurance Company clients was exposed.
A group of co-conspirators used Medicaid information from Medicare beneficiaries in and near Detroit to defraud Medicaid and file for $24.7 million in fraudulent claims. The fraud took place between 2008 and May of 2012. Hundreds of patients had their information misused so that co-conspirators could bill Medicare for psychotherapy, home health services, and other medical services.

Information Source: PHIPrivacy.net

A February 7 or 8 office burglary at Mercedes-Benz of Walnut Creek resulted in the exposure of customer information. Locked file cabinets that contained customer deal files were burglarized and customer files were taken from the Service Department. The theft was discovered on the morning of February 8 and immediately reported. Customer names, Social Security numbers, addresses, credit reports, driver’s license information, insurance information, and credit card numbers may have been exposed.

Information Source: California Attorney General

A number of credit card terminals in 19 California and Arizona stores were affected by point-of-sale malware between January 25 and 29. Credit card and debit card numbers were exposed. Customer PINs associated with the payment cards were not affected. Sprouts identified the issue within a few days of the breach and updated customer information protection procedures in all of its stores.

Information Source: Media

Capella University's official breach notice can be found here: http://www.atg.state.vt.us/assets/files/Capella%20University%20Security%20Notice%20to%20consumer.pdf

A collection department employee sent sensitive information to a personal email account. The incident was discovered on January 28 and the employee was fired. A small group of learners may have had their names, Social Security numbers, and other information that was kept by Capella’s collection department exposed.

Information Source: Security Breach Letter

Desktop computer hardware was stolen from the Anaheim Billing Center of Crescent Healthcare, Inc. on December 28, 2012. The theft was discovered on Monday, December 31 and reported to law enforcement. Names, Social Security numbers, health insurance identification numbers, health insurance information, dates of birth, diagnoses, other medical information, disability codes, addresses, and phone numbers may have been exposed.

UPDATE (04/03/2013): Over 100,000 people were affected.

Information Source: California Attorney General

NBC’s website was attacked by malware in the form of a Citadel Trojan. The purpose of the attack was most likely to steal usernames, passwords, and other personal information. NBC is unclear on how the malware entered their system.

Information Source: Media

Government agencies do not collect information on the number of records from breaches used in our total.
An employee working as an administrative manager in the Enforcement Division viewed the DMV information of around 5,000 people outside of work hours and for no job-related reason. His activities between January 2008 and October 2012 were discovered and he was discharged on January 11, 2013. It is believed that the driver’s license and other motor vehicle record information was viewed for curiosity and not malicious purposes.

UPDATE (05/01/2013): A group of people who had their driver’s license information accessed filed lawsuits against Minnesota. The state asked the federal judge hearing the case to dismiss the motions and argued that the state isn’t liable under a federal law that protects the privacy of driver’s license data. The employee responsible for the breach is facing criminal charges; though the breach may not have been for malicious purposes.

UPDATE (08/07/2013): The lawsuit was filed against other state employees as well as the employee responsible for the breach.

UPDATE (09/25/2013): A district court dismissed the lawsuit. The judge ruled that state agencies are not liable for a rogue employee’s actions. The case against the dishonest employee is still active. The liability of the employee’s supervisors has been limited and they will not pay damages for the breach.

Information Source: Media
February 22, 2013
LexisNexis, Sprechman & Associates
Miami, Florida
BSO INSD 20,000

LexisNexis informed Sprechman & Associates that the unusual, excessive activity of an associate caused them to eliminate that associate's access to LexisNexis' database. The associate was later found to have misused Social Security numbers in order to file over 11 million dollars in fraudulent tax refund claims. The dishonest associate was not immediately fired from Sprechman & Associates and was terminated in July 2012 when law enforcement used a warrant to search his home and office computers.

Information Source: Databreaches.net
February 22, 2013
Microsoft
Redmond, Washington
BSR HACK Unknown

Microsoft’s official notice can be found here: https://blogs.technet.com/b/msrc/archive/2013/02/22/recent-cyberattacks....

Microsoft security discovered that a number of employee devices were affected by malware. The employees had visited unsafe websites and downloaded material. It is unclear if the employee devices spread the infection to other areas of Microsoft’s network, but Microsoft found no evidence of customer data being affected. Facebook, Twitter, and Apple were affected by a similar issue around the same time.

Information Source: Media
February 21, 2013
Zendesk
San Francisco, California
BSR HACK Unknown

An official notice can be found here: http://www.zendesk.com/blog/weve-been-hacked.

Those with questions may call (415) 287-9976.

A hacker accessed Zendesk information that was online. Three clients who use Zendesk to store information had user lists downloaded by the hacker. Users who contacted those clients for support may have had their email addresses and the subject lines of those email addresses accessed.

UPDATE (02/22/2013): Tumblr, Twitter, and Pinterest were the affected clients. Twitter let users know that emails, phone numbers, Twitter usernames, and any other information that was provided to Twitter may have been exposed. Passwords were not compromised.

Information Source: Media
February 21, 2013
Polk County School District
Bartow, Florida
EDU DISC 200

Students who paid tuition for education programs may have had their 1098T tax forms sent to the incorrect address. Between 150 and 200 people out of 2,000 were sent to the wrong address because a group of the tax forms were placed in envelopes without being properly separated. Some people received the forms of several people while others never got their tax forms. The district implemented a new step of sampling some of the envelopes in order to review the process before completing an entire batch.
February 20, 2013  
Mid-Florida Urological Associates  
Orlando, Florida  

MED  INSD  Unknown

A dishonest employee misused patient information in order to claim them as her children and receive insurance compensation. The dishonest employee was charged with insurance fraud and ID theft.

UPDATE (02/22/2013): Orlando Health patient records were accessed. The Orlando Health hospitals include MD Anderson Cancer Center Orlando, Orlando Regional Medical Center, Winnie Palmer Hospital for Women and Babies, Dr. P. Phillips Hospital, Arnold Palmer Hospital for Children, South Seminole Hospital, South Lake Hospital, and Health Center Hospital.

Information Source: PHIPrivacy.net

February 20, 2013  
Central Hudson Gas & Electric  
Poughkeepsie, New York  

NGO  HACK  110,000

Central Hudson learned of a cyber attack that occurred over President's Day weekend. Customers were notified the day after the holiday and encouraged to monitor their bank accounts and credit reports. Customer banking information and other personal information may have been accessed during the attack.

Information Source: Databreaches.net

February 19, 2013  
Hotusa Group  

BSR  HACK  Unknown

Hotusa Group is headquartered in Barcelona, Spain. A server breach or other incident related to credit cards may have affected people who used their American Express cards at locations linked to Hotusa Group's servers. Account numbers, names, credit card expiration date, and other credit card information may have been exposed for American Express and other cards. The incident occurred on August 24, 2012.

Information Source: California Attorney General

February 19, 2013  
Kork and Keg  
Greencastle, Indiana  

BSR  HACK  Unknown

Fraudulent activity on the accounts of DePauw University students was linked to Kork and Keg. It is not clear how the store's payment system was compromised; however it was a common link among those who had their accounts breached. Kork and Keg did not make a statement.

Information Source: Media

February 19, 2013  
Apple  
Cupertino, California  

BSR  HACK  Unknown

Apple detected malware on employee computers. A small number of employee computers had been affected after their users went to a website for software developers. Facebook, Microsoft, and Twitter experienced the same breach around the same time.

Information Source: Media

February 18, 2013  
Express Scripts, Ernst & Young  
St. Louis, Missouri  

BSF  DISC  Unknown

A partner at Ernst & Young is accused of sneaking into the headquarters of Express Scripts Holding Co. It is not clear how the Ernst & Young partner got into the headquarters, but it is believed that he emailed over 20,000 pages of data to a personal account. Express Scripts Holding Co. accused Ernst & Young of stealing the information in order to develop its health care division. Express Scripts Holding filed a lawsuit; the accused partner is no longer employed by Ernst & Young.

Information Source: Media

February 17, 2013  
Sierra View District Hospital  
Porterville, California  

MED  HACK  Unknown

The Information Technology Department at Sierra View District Hospital detected unusual activity on its computer network. Patient information may have been affected and the investigation is ongoing.

Information Source:
Heyman HospiceCare, Floyd Medical Center  
Rome, Georgia  
MED  PORT  Unknown

The theft of a password-protected laptop from an employee’s car may have resulted in the exposure of patient information. The theft occurred on January 4, 2013 and was reported immediately. Patients who were treated between July 1, 2006 and January 3, 2013 may have had their names, Social Security numbers, addresses, phone numbers, dates of birth, insurance policy numbers, diagnoses, visit notes, physician names, caregiver names, and advance directives exposed.

Facebook
Menlo Park, California  
BSO  HACK  Unknown

Facebook's official notification can be found here: http://www.facebook.com/notes/facebook-security/protecting-people-on-fac...  

Facebook discovered that hackers had exploited a vulnerability and accessed unspecified data. Facebook found no evidence that Facebook user data was compromised. Malware was installed on a number of employee laptops after a small number of them visited a mobile developer website that turned out to be unsafe. Microsoft, Twitter, and Apple were affected by the same issue around the same time.

Froedtert Health  
Milwaukee, Wisconsin  
MED  HACK  43,000 (less than 3% contained SSNs)

A computer virus was discovered on an employee’s work computer account on December 14, 2012. One of the files on the employee's computer contained patient names, addresses, telephone numbers, dates of birth, medical record numbers, names of health insurers, diagnoses, and other clinical information. A limited number of Social Security numbers were also exposed.

FCC, Emergency Alert System  
Washington, District Of Columbia  
GOV  HACK  Unknown

The Emergency Alert Systems (EAS) of several TV stations nationwide were hacked and alerted people to a fictitious zombie attack. The FCC ordered local broadcasters to change their passwords on EAS equipment and check the security of firewalls before resuming normal internet connections.

Häagen-Daz  
Tampa, Florida  
BSR  HACK  Unknown

Anyone who made a purchase at the Häagen-Daz inside the food court in International Plaza since April of 2012 may have been affected by identity theft. A flash drive that contained key-loger software was connected to a register at the store. It recorded payment card transactions and allowed thieves to make counterfeit credit cards. Two men were arrested in June of 2012 for using fraudulent card information and that information was later linked to the Häagen-Daz shop.

University of North Carolina  
Chapel Hill, North Carolina  
EDU  HACK  3,500
A cyber attack on two servers resulted in the exposure of employee information. The servers were at the UNC Lineberger Comprehensive Cancer Center. Employees, contractors, and visiting lecturers at the Lineberger Center may have had their Social Security numbers or passport numbers exposed. The breach was discovered in May of 2012 and notifications were sent in December of 2012. Fewer than 15 people who were subjects in research studies were also affected by the breach.

Information
Source: Media
February 13, 2013
Sinai Medical Center of Jersey City LLC
Jersey City, New Jersey
MED INSD Unknown

A pediatrician misused patient information in order to defraud Medicaid of nearly one million dollars. The pediatrician owned Sinai Medical Center and billed Medicaid for wound repairs and other procedures that were never performed. Police arrested the dishonest pediatrician on January 16, 2013.

Information
Source: PHIPrivacy.net
February 13, 2013
Los Angeles Times, OffersandDeals.latimes.com
Los Angeles, California
BSO HACK Unknown

The Los Angeles Times learned that a segment of its website housed malicious code for six weeks. The subdomain OffersandDeals.latimes.com redirected visitors to a malicious website. The website then used code to receive compensation for web traffic. The compromise appears to have occurred sometime before December 23, 2012. An LA Times spokesperson initially responded to the breach by claiming that a glitch in Google's display ad exchange had caused a malicious script warning rather than actual malicious script.

Information
Source: Media
February 13, 2013
Jawbone
San Francisco, California
BSR HACK Unknown

Hackers were able to access Jawbone's MyTALK customer accounts for several hours. Names, email addresses, and encrypted passwords were exposed. Any customers who were affected received an email warning them to reset their passwords.

Information
Source: Media
February 12, 2013
Palm Beach County Health Department
Palm Beach, Florida
MED INSD 2,800

Patients with questions may call (561) 671-4014

A senior desk clerk was arrested for obtaining and releasing patient information for identity theft purposes. The dishonest employee took home client lists with names, Social Security numbers, and dates of birth. Patients born between 1991 and 1996 may have had their personal information misused.

Information
Source: PHIPrivacy.net
February 12, 2013
J.P. Morgan Chase, Capital One
New York, New York
BSF CARD 6,000

ATMs in New Jersey, Illinois, and Wisconsin were also compromised.

Two men face charges of conspiracy to commit bank fraud, conspiracy to commit access device fraud, and aggravated identity theft after being indicted for attaching skimming devices to ATMs in New York, New Jersey, Illinois, and Wisconsin. At least nine other people are believed to have participated in the bank fraud scheme. Over 6,000 J.P. Morgan Chase and Capital One bank accounts were defrauded for over $3 million.

Information
Source: Media
February 11, 2013
Crafts Americana Group, Inc. (Knitpicks.com, ArtistsClub.com, ConnectingThreads.com)
Columbus, Ohio
BSR DISC Unknown

Customers who had credit card numbers on file after using them at Knitpicks.com, ArtistsClub.com, or ConnectingThreads.com may have had their information exposed. A file on the Crafts Americana Group, Inc. servers was accessible for a period of time before being removed on January 25, 2013. The file contained names, credit card numbers, addresses, and phone numbers.
A network server was stolen or discovered stolen on January 15, 2012. The incident appeared on the HHS website in February of 2013.

Information
Source: HHS via PHIPrivacy.net

A laptop was stolen or discovered stolen on October 11, 2012. The incident appeared on the HHS website in February of 2013.

Information
Source: HHS via PHIPrivacy.net

Five laptops were stolen during the weekend of November 17, 2012. They did not contain Social Security numbers and did contain unspecified personal information of patients. A notice about the incident was sent on January 18, 2013 and the breach appeared on the HHS website in February of 2013.

Information
Source: HHS via PHIPrivacy.net

A computer network attack resulted in the exposure of customer information. The cyber attack was discovered on December 13, 2012 and affected customer databases with names, Social Security numbers, credit and debit card numbers, payment card expiration dates, payment card security codes, addresses, telephone numbers, dates of birth, and mothers’ maiden names may have been exposed.

Information
Source: California Attorney General

The hacking group known as Anonymous claimed responsibility for a hack of the Alabama Criminal Justice Center and indicated that they had access to US Federal Reserve servers. Some internal documents were also exposed. The hack attack was a response to the US Federal Reserve’s reaction, or failure to react, to the February 4 hack of the Alabama Criminal Justice Center. Anonymous released a document showing that they had extensive access to US Federal Reserve servers and internal documents. Anonymous hacked into the Grand Banks Yachts website and used it to host a file that contained the document.

UPDATE (08/23/2013): Federal Reserve employee data was posted on a website. Phone numbers, emails, and other Federal Reserve employee information was placed on a publicly accessible spreadsheet. Anonymous claims to have full details of every Federal Reserve Bank of America employee. The information may have been from the breach in February.

Information
Source: Media

Hackers were able to access customer credit card information stored on computer servers. The cyber attack affected customers who made purchases on www.thorlo.com between November 14, 2012 and January 22, 2013. Credit card numbers, credit card expiration dates, credit card security codes, names, and contact information were exposed.
A vendor's mailing error resulted in the exposure of employee Social Security numbers. Call for Candidacy letters were mailed sometime around January 16 that had Social Security numbers, names, and addresses visible through the address window of the letter.

Information
Source: California Attorney General

February 7, 2013 Schneider-Electric Palatine, Illinois 
BSO DISC Unknown

Wayne Memorial Hospital Honesdale, Pennsylvania 
MED PORT 1,182 (No SSNs or financial information reported)

An unencrypted disc that contained patient information was lost in transit. The disc had names, Medicare account numbers, and outstanding account balances from patients who visited the Honesdale hospital between 2007 and 2012. A legal envelope that contained the disc was mailed on November 28 and arrived at Novitas Solutions in Pittsburgh in a cardboard box without the disc.

Information
Source: PHIPrivacy.net

February 7, 2013 McDonald’s, Shogun Japanese Steakhouse, Krystal, Polished Nail Salon, Georgia 
BSR INSD Unknown

Dishonest employees from multiple cities and states were involved. The location listed is the state where many fraudulent purchases took place.

Eleven people were charged with participating in an identity theft ring. Some of the defendants obtained customer credit and debit card information by using skimmers at their places of employment. Others used the stolen information to make fraudulent payment cards. The ring was in action between June of 2009 and November of 2010.

Information
Source: Dataloss DB

February 6, 2013 Bashas’ Chandler, Arizona 
BSR HACK Unknown

The location of the breach is listed as the corporate headquarters of Bashas’

Bashas’ online systems suffered an online breach. Customers in Lake Havasu City and Pinal County who entered their credit and debit card information online have been affected. All customers are being warned to check their payment card transactions for suspicious activity.

Information
Source: Dataloss DB

February 6, 2013 Boca Raton Regional Hospital Boca Raton, Florida 
MED INSD Unknown

Eight people were charged for participating in an identity theft ring. One of the members was employed as a scheduler at Boca Raton Regional Hospital. She passed along patient information in exchange for payments. One member allegedly filed 57 fraudulent tax returns with the stolen information in attempt to get $306,720 in refunds. Another member is accused of filing 75 fraudulent returns for $750,469 in refunds.

UPDATE (07/30/2013): The dishonest employee was convicted of unauthorized disclosure of medical records, using stolen Social Security numbers to file fraudulent tax claims, and conspiracy to commit false claims. She was sentenced to 18 months in prison and ordered to pay $15,795 in restitution to the IRS. A co-defendant was sentenced to 40 months for her role in filing fraudulent tax returns and stealing patient information.

Information
Source: PHIPrivacy.net

February 5, 2013 U.S. Department of Energy Washington, District Of Columbia 
GOV HACK Unknown

The U.S. Department of Energy discovered that unidentified malicious activity had been detected on 14 servers and 20 workstations in January. The personal information of several hundred employees was exposed. The U.S. Department of Energy had known about the need to patch computers, network systems, and servers since 2012.
February 4, 2013  **Alabama Criminal Justice Information Center**  
**Montgomery, Alabama**  

Information related to over 4,000 American bank executive accounts was exposed by hackers. Hackers placed an Alabama Criminal Justice Information Center spreadsheet with the login information, credentials, contact information, and IP addresses of bank executives online.

February 3, 2013  **Premier Tax**, **Alabama**  

The area of Alabama where the breach occurred is unclear.

Six people who worked in tax preparation were charged with fraud and filing false tax returns in March of 2012. Over 1,000 false tax returns were filed between October 2009 and April 2012. The fraudulent returns totalled more than $1.7 million.

**UPDATE** (01/29/2013): Two others were linked to the conspiracy and charged. One of them was an employee of an unnamed Alabama state agency. She was able to access a state database of personal information and provide it to others in the identity theft ring.

February 2, 2013  **River Falls Medical Clinic**  
**River Falls, Wisconsin**  

River Falls Medical Clinic officials reported a burglary during the summer of 2012. The equipment and paper documents that were stolen were recovered by police on November 28. An employee of a cleaning service that subcontracted with the Clinic is the main suspect. The items were found in the employee’s home and he was charged with felonies associated with theft and drug possession. It is believed that the documents were intended to be shredded. They contained patient names, dates of birth, patient account and billing account information, diagnosis codes, insurance information, account numbers, medical chart numbers, and scheduling information. An unspecified number of patients also had their Social Security numbers, home addresses, and phone numbers exposed.

February 2, 2013  **Twitter**  
**San Francisco, California**  

Online attackers were able to access the usernames, email addresses, session tokens, and encrypted passwords of 250,000 users. Twitter notified affected users and told them to create a new password. Anyone who used the same password and username or email combination for other sites is encouraged to change the password on other sites as well.

**UPDATE** (03/11/2013): Facebook, Microsoft, and Apple were all affected by a similar breach around the same time.

February 1, 2013  **Antioch Unified School District**  
**Antioch, California**  

A document with sensitive Worker's Compensation claim information was accidentally sent out with an email to a limited number of Antioch Unified School District employees. Social Security numbers and other information related to current and former employees that reported injuries were exposed. The incident occurred on January 18 and people who received the email were instructed to remove and destroy any saved information contain in the email. Those who received the email were also instructed to provide written verification that they had removed and destroyed the information.
A former Tallahassee Memorial HealthCare food service employee was indicted on 31 counts of filing false tax returns, wire fraud, false claims, and aggravated identity theft. He and two others are believed to have participated in a conspiracy that led to $818,000 in fraudulent claims. The employee worked for Tallahassee Memorial HealthCare for three years. He gathered patient names and dates of birth from food tray receipts when he delivered food to the rooms of patients in August of 2011 and stole emergency room data sheets from the trash. The information was then passed to the two others who participated in the conspiracy.

Information
Source: PHIPrivacy.net
February 1, 2013
Central Laborers’ Pension Fund, Central Laborers’ Welfare Fund, Central Laborers’ Annuity Fund, Illinois
BSF PORT Unknown

A home burglary resulted in the theft of a CD that contained the information of over 30,000 beneficiaries. The CD contained names, Social Security numbers, and dates of birth and was taken from the home of an accountant at an unnamed counting firm. The three funds sued the accounting firm for $200,000 to cover the cost of credit monitoring and insurance.

Information
Source: Databreaches.net
January 31, 2013
Bank of Prairie du Sac, Prairie du Sac, Wisconsin
BSF HACK 200

Customers were affected by an ATM hacking scheme. A skimming device is believed to have been placed on the bank’s ATM at a food store. A suspect was arrested after being seen using stolen card information at an ATM.

Information
Source: Dataloss DB
January 31, 2013
Silver Star Motors, Cortland, Illinois
BSR INSD 25

The owner of Silver Star Motors was charged with seven counts of identity theft and may have been involved in 25 cases of identity theft. Customer information was used to defraud lending companies associated with the used-car dealership.

UPDATE (02/13/2013): At least 44 people have had their information misused. The dishonest owner also operated Edge Auto Sales at one time.

Information
Source: Dataloss DB
January 30, 2013
BSO HACK Unknown

The New York Times’ computer system was hacked after Chinese government officials warned the Times about consequences for investigating the wealth of government family members. The Times began monitoring its system closely on October 24 and noticed unusual activity on October 25 when an article about the wealth of a Chinese official’s family was published. The breach began on September 13 and was allowed to continue until January so that the hackers’ behavior could be studied. It appears that the passwords of every Times employee were compromised and 53 Times employees had their personal computers accessed. The 53 employees were located outside of the United States and appear to have been the ones who may have covered the Chinese stories.

Information
Source: Media
January 30, 2013
Police Department of Littleton, Massachusetts
GOV DISC 100

A police activity log for the period of January 7 through January 13 was published on the Littleton department’s website. Someone forgot to remove personal details from the log and the sensitive information was available online for 10 days. Names, Social Security numbers, dates of birth, and addresses, were available between January 14 and January 24.

Information
Source: Media
January 29, 2013
North Los Angeles County Regional Center (NLACRC), Van Nuys, California
MED PORT Unknown

The November 13, 2012 theft of a laptop resulted in the exposure of consumer information. Names, addresses, phone numbers, dates of birth, residential information, and medical information may have been exposed.
A hacker accessed the webserver used to host stethoscope.com on December 3. The breach was discovered in mid-December during routine server maintenance. Customer names, addresses, email addresses, and credit card information such as numbers, expiration dates, and security codes may have been exposed.

Information
Source: California
Attorney General

January 29, 2013 Stethoscope.com
Natick, Massachusetts

Those with questions may call (877) 288-8057.

A hacker accessed the webserver used to host stethoscope.com on December 3. The breach was discovered in mid-December during routine server maintenance. Customer names, addresses, email addresses, and credit card information such as numbers, expiration dates, and security codes may have been exposed.

Information
Source: California
Attorney General

January 28, 2013 RR Donnelley, UnitedHealthcare, Boy Scouts of America
Chicago, Illinois

UnitedHealthcare has established a hotline for those with questions: 1-866-896-4209.

An unencrypted desktop computer was stolen from an RR Donnelley facility sometime between mid September and the end of November, 2012. RR Donnelley is a vendor of UnitedHealthcare. It is unclear why the breach was not noticed until December 3, 2012. The stolen computer contained UnitedHealthcare member information that was related to participation in the Boy Scouts of America 2003 health benefit plan. Names, Social Security numbers, and addresses may have been exposed.

UPDATE (10/01/2013): A total of 8,911 Boy Scouts of America Employee Benefit Plan participants were notified of the breach.

Information
Source: Walz and Associates Law Firm
Albuquerque, New Mexico

A concerned citizen found hundreds of documents in a recycling center and notified a local news team. The documents included criminal histories, depositions, medical records, personal phone numbers, and addresses. Most were from the 1990’s. Most or all of the information did not need to be shredded because it was considered public record. The local news team contacted a director from the solid waste division and the documents were removed for shredding.

Information
Source: PHIprivacy.net

January 28, 2013 Cbr Systems
San Bruno, California

The 2010 theft of a company laptop, a hard drive, and a number of unencrypted backup tapes resulted in the exposure of sensitive information. Social security numbers, credit and debit card numbers, driver’s license numbers, and dates of birth were contained on one or more of the devices.

Cbr Systems reached a settlement with the Federal Trade Commission in early 2013. Cbr Systems must establish an information security program and be independently audited every other year for 20 years. The full settlement can be found here: http://ftc.gov/opa/2013/01/cbr.shtm

Information
Source: Media

January 28, 2013 Los Angeles County Department of Public Social Services
Los Angeles, California

A dishonest employee pleaded guilty to using a Los Angeles County computer system to file fraudulent tax refunds. The fraudulent activity occurred between July 2009 and the 2011 tax year. The IRS found 44 pages of screen prints with the information of 132 assistance participants in the employee’s home. The employee, her spouse, and three others were indicted in January of 2012.

Information
Source: Databreaches.net

Woodridge, Illinois

Customers who made purchases on www.wilton.com between October 8, 2012 and January 8, 2013 may have had their credit or debit card information exposed. A Wilton service provider discovered the issue on or around January 8, 2013. A
malicious user accessed the website information and payment card numbers, expiration dates, and security codes may have been exposed. Customer names, addresses, and telephone numbers are also at risk.

This incident is in addition to the hacking incident that took place between July and October of 2012. That incident was reported on December 12, 2012.

**Information**

**Source:**
California Attorney General

**January 24, 2013** **Brentwood Primary Care Clinic**
**Jacksonville, Florida**

MED INSD 261

A dishonest intern was caught using a cell phone to illegally photograph patient Social Security numbers and names. The photos were then sent to another person; presumably for fraudulent activity. The office intern was charged with fraudulent use of personal identification information. It is unclear when the breach was discovered since the photos were taken between May 7 and June 19.

**Information**

**Source:**
PHIPrivacy.net

**January 24, 2013** **Eastern Illinois University**
**Charleston, Illinois**

EDU DISC 430 (No SSNs or financial information reported)

At least 65 students received information about the grade point average of 430 students during early January 2013. The breach occurred when a spreadsheet that contained the information and the E-number of 430 students was accidentally made available online.

**Information**

**Source:**
Databreaches.net

**January 22, 2013** **NECA/IBEW Family Medical Care Plan**
**Rockville, Maryland**

MED DISC Unknown

NECA/IBEM Family Medical Care Plan (FMCP) participants received disclosure documents related to benefits coverage and modifications. The outside of the envelopes in which the documents arrived displayed participant Social Security numbers.

**Information**

**Source:**
California Attorney General

**January 18, 2013** **Stanford School of Medicine, Lucile Packard Children's Hospital**
**Palo Alto, California**

MED PORT Unknown

Those with questions may call 1-855-731-6016.

The January 9 theft of a laptop from a physician's car may have exposed sensitive information. The laptop may have contained some combination of patient names, dates of birth, and contact information.

**UPDATE** (01/22/2013): A total of 57,000 patients are being notified. Medical information and medical record numbers were exposed. A limited number of patients had their contact information exposed. Most of the information on the laptop was from 2009.

**Information**

**Source:**
California Attorney General

**January 17, 2013** **St. Mark's Medical Center**
**La Grange, Texas**

MED HACK 2,988

An employee's computer was found to contain malware. The malware infection began on May 21, 2012 and was discovered on November 15, 2012. Files stored on the computer contained billing information with patient names, Social Security numbers, account numbers, medical record numbers, dates of birth, gender, treatment dates, insurance provider names, and account balances.

**Information**

**Source:**
PHIPrivacy.net

**January 16, 2013** **Utah Department of Health, Goold Health Systems**
**Salt Lake City, Utah**

MED PORT 6,000 (No SSNs or financial information reported)
An employee of Goold Health Systems lost an unencrypted USB memory stick that contained the information of around 6,000 Medicaid recipients in Utah. Goold Health Systems is a contractor for the Utah Department of Health. Medicaid recipient names, Medicaid identification numbers, ages, and recent prescription drug use were on the memory stick. The memory stick was lost during travel between Salt Lake City, Denver, and Washington. The loss was confirmed on Tuesday, January 15.

Information Source: Media

January 13, 2013 Advanced Micro Devices (AMD), Nvidia Sunnyvale, California BSR INSD Unknown

Four managers who left AMD to work for Nvidia are being sued by AMD for intellectual property theft. AMD accused the former employees of setting up a spying ring in the company before leaving to work for rivaling company Nvidia. One of the managers is accused of using two external hard drives to download Microsoft Outlook email files, licensing agreements, and strategic plans from his work computer before leaving AMD in July of 2012. Another employee is accused of taking an AMD technical work and development database with over 200 files. The four employees are accused of taking over 150,000 documents.

Information Source: Media

January 12, 2013 Zaxby's Athens, Georgia BSR HACK Unknown

Over 108 Zaxby’s restaurants experienced a breach related to customer credit and debit cards. A number of people experienced credit card fraud and an investigation led to Zaxby’s as a common point of purchase. Suspicious files were found on Zaxby's system during the subsequent investigation.

Information Source: Databreaches.net

January 12, 2013 Florida Department of Juvenile Justice Tallahassee, Florida GOV PORT


A mobile device that contained both youth and employee records was reported stolen on January 2, 2013. Over 100,000 records were on the device and may have been exposed. The device was taken from a Department of Juvenile Justice office and was neither encrypted nor password-protected. Department of Juvenile Justice policy requires such devices to be encrypted.

Information Source: Databreaches.net

January 12, 2013 Florida Department of Juvenile Justice Tallahassee, Florida MED STAT

On September 6, 2012 it was reported that three computers that contained information from the Florida Department of Juvenile Justice were stolen from an apartment site earlier in the week. A television was also taken at the time of the theft.

UPDATE (01/12/2013): At least one of the devices was neither encrypted nor password protected and held the personal information of over 100,000 youth and employees.

Information Source: Databreaches.net

January 11, 2013 EJ Phair Brewing Company and Alehouse Concord, California BSR HACK Unknown

Customers who used credit or debit cards at EJ Phair discovered fraudulent chargers on their payment cards. A hacker or hackers managed to access and misuse payment card numbers once they ran through EJ Phair’s system. It appears that customers who used cards at the location between September and late November of 2012 may have been affected.

Information Source: California Attorney General

records from this breach used in our total: 0
A computer repair shop bought used computers on govdeals.com in 2011. The computers were found to have information from city employees when they were removed from storage on January 5. Social Security numbers, pension information, and other personal information from Macon police officers were on the computers. Information from local businesses that was used for city purposes was also on the computers. A total of 39 hard drives, two servers, and two CPUs were purchased and may have contained sensitive information.

**Information Source:** Databreaches.net

---

Texas Southern University's radio station KTSU gave a volunteer position to a person with a criminal history of credit card fraud. The volunteer was later arrested for allegedly using the radio station's donation drive to steal credit card information. The dishonest volunteer faces up to 300 counts of credit card fraud for attempting to misuse the information on donor pledge sheets.

**Information Source:** Databreaches.net

---

Employees accidentally threw out hundreds of patient records. The dental records were found by someone looking through a dumpster and the incident was reported to a local news team. Names, Social Security numbers, dates of birth and addresses were exposed. Employees from Bujanda-Wagner's office came to recover the documents.

**Information Source:** PHIPrivacy.net

---

An unencrypted flash drive was stolen from a teacher's car. It contained student Social Security numbers and other information.

**Information Source:** Databreaches.net

---

An employee working in human resources was robbed while transporting information between school districts. The employee stopped for lunch and discovered that personnel files containing names, Social Security numbers, addresses, dates of birth, and driver's license numbers had been stolen from their car.

**Information Source:** Databreaches.net

---

A dishonest employee was arrested on suspicion of misusing client information to apply for credit cards. The dishonest employee was able to pose as different clients seeking immunizations and other services. She was charged with fraudulent use or possession of identifying information and credit card abuse.

**UPDATE** (01/31/2013): The employee was working for the Northeast Texas Public Health district when she was arrested for stealing the identities of patients at a clinic in Mount Pleasant. She began working in the Texas Department of State Health Services clinic in 2008.

**Information Source:** PHIPrivacy.net

---

It is not clear if this breach is related to the August 2010 theft of a laptop from Centric Software in Campbell, California.

Those with questions may call 1-800-416-4601.

Anyone who purchased items on [www.accesscatalog.com](http://www.accesscatalog.com) using a credit card may have been affected by a breach that began in August 2010. An unauthorized party may have obtained names, credit or debit card numbers, expiration dates, and payment card verification codes. Centric Group learned of the incident on or around December 13, 2012.
January 7, 2013  
Office of Dr. Calvin L. Schuster  
Reedley, California

Those with questions may call Dr. Schuster's office at 1-855-638-1443.

A computer was stolen during an office burglary that occurred sometime around November 5, 2012. The computer contained patient names, dates of birth, and a minimal amount of patient medical information.

January 7, 2013  
Woodwinds Hospital  
Woodbury, Minnesota

An employee kept 200 pages of confidential information in an effort to prove that Woodwinds Hospital was trying to conceal evidence of medical misconduct. The employee was discharged in 2010 for reasons unrelated to removing the information. She claims to have taken them home after being ordered to destroy any information related to incidents that could damage Woodwinds Hospital's reputation.

January 6, 2013  
Oldcastle APG, Inc.  
Atlanta, Georgia

A laptop was stolen from an employee's car on or around December 10. APG employees may have had their names, Social Security numbers, bank account information, and other information exposed.

January 4, 2013  
Reyes Beverage Group  
Rosemont, Illinois

Those with questions may call Reyes Holdings Ethics Hotline at (888) 295-6392 or email ethicshotline@reyesholdings.com

A report containing the names and Social Security numbers of a group of Reyes Beverage Group's California employees was accidentally sent to the personal email address of an employee of Reinhart Foodservice. Reinhart Foodservice is a Reyes Holdings company as well. It is unclear how the email was accidentally sent and why it ended up in the personal email of an employee at a different division.

January 4, 2013  
Healing Hearts  
Jacksonville, North Carolina

The owner of a group of childcare services pleaded guilty to defrauding Medicaid of $8 million. She and a co-defendant targeted medicare recipients in order to enroll them in a program and make fraudulent Medicare claims for mental and behavioral health services. Additionally, the owner pleaded guilty to misusing at least one therapist's credentials in order to make the claims for mental and behavioral health services. The scheme took place between 2008 and 2012.

January 3, 2013  
Mission Hospital, St. Joseph Health  
Mission Laguna Beach, California

Someone called Mission Hospital on August 28, 2012 and claimed that he found a flash drive with sensitive patient information in his garage. The flash drive was returned to Mission Hospital via mailed envelope on September 11, 2012. Patients who received services at Mission Hospital between September and November of 2008 may have had their information exposed. The notice that was sent to patients was dated September 14, 2012. It appears that a contractor or employee misplaced the unencrypted flash drive.

The flash drive contained names, medical record numbers, and account numbers. Additionally, the flash drive may have contained some combination of date of admission, age, birth date, vital readings, physical examination, gender, race,
name of physician, medical history, past and current treatment and illnesses, history of substance use, family history, lab
tests and results, imaging tests and results, body weight, physician notes on patient, care plan, employment status and
employer, prognosis, diagnosis, treatment recommendations, allergies, medications, comments about patient's
appearance, patient health complaint, symptoms, reason for referral, and reason for admission information.

Information
Source: PHIPrivacy.net

January 3, 2013  King Drug & Home Care
Owensboro, Kentucky

An employee reported that a portable hard drive was missing on November 23, 2010. The device had last been seen
sometime around November 19. The data on the device included information from before July 31, 2009. Client names,
Social Security numbers, medical record numbers, account numbers, dates of service, race, insurance carriers and
insurance numbers, addresses, phone numbers, sex, dates of birth, diagnosis information, allergies, initial referral forms,
patient assessments/plans of care, physician orders and/or delivery ticket information may have been on the hard drive.

Information
Source: PHIPrivacy.net

January 2, 2013  Rosenthal Collins Group
Chicago, Illinois

Anyone who suspects they were a victim of identity theft because of this incident should report it to Rosenthal Collins
Group at creditprotection@rcgdirect.com.

An unauthorized intrusion was detected on the morning of Tuesday November 27. The unauthorized access began on
November 26 and access to the breached web application was immediately shut down upon discovery. Customers who
completed Rosenthal Collins Group account forms online may have had their names, Social Security numbers, addresses,
dates of birth, range of net worth and income, bank names, passwords for accessing the web application, and email
addresses exposed.

Information
Source: California
Attorney General

January 2, 2013  Hospice of North Idaho (HONI)
Hayden, Idaho

441 (No SSNs or
financial
information
reported)

Read the full agreement between HHS and HONI here: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/honi-
agreement...

The June 2010 theft of an unencrypted laptop from an employee's car resulted in the exposure of patient information. The
HHS Office for Civil Rights investigated the breach and found that HONI had not conducted a risk analysis to safeguard
electronic protected health information. It was also discovered that HONI did not meet a HIPAA Security Rule that
required them to have policies or procedures in place to address mobile device security. HONI agreed to pay the U.S.
Department of Health and Human Services' (HHS) $50,000 regarding potential Health Insurance Portability and
Accountability Act of 1996 Security Rule violations. HONI also began taking extensive steps to improve their HIPAA
Privacy and Security compliance program since the June 2010 breach.

Information
Source: PHIPrivacy.net

December 31, 2012  Sunview Vineyards Of California, Inc.
Delano, California

An office theft of an unencrypted laptop on or around December 15 resulted in the exposure of confidential personal
information. The laptop contained an Excel spreadsheet with workers' compensation information such as names, Social
Security numbers, telephone numbers, and other workers' compensation claim or injury information.

Information
Source: California
Attorney General

December 29, 2012  US Army Fort Monmouth
Oceanport, New Jersey

Those with questions may call (443) 861-6571.

Hackers were able to access database information from Command, Control, Communications, Intelligence, Surveillance
and Reconnaissance as well as nongovernmental personnel and people who visited Fort Monmouth. The breach was
discovered and addressed on December 6. names, Social Security numbers, dates of birth, places of birth, home
addresses, and salaries were exposed.
A sensitive document was accidentally attached to an email that was sent to students. The attachment contained names, Social Security numbers, dates of birth, student attendance information, and information regarding their program. The email was intended to inform students about open positions.

Information Source: California Attorney General

December 28, 2012
Gibson General Hospital
Princeton, Indiana

The November 27 theft of a laptop may have resulted in the exposure of patient information. Names, Social Security numbers, addresses, and clinical information may have been exposed. Patients who have received services since 2007 may have been affected.

Information Source: PHIprivacy.net

December 28, 2012
Carewise Health, Hewlett-Packard Enterprise Services
Louisville, Kentucky

An employee responded to a telephone computer phishing scam. The person was employed by a subcontractor of Hewlett-Packard Enterprise Services (HP ES) named Carewise Health. Unauthorized users were able to remotely access a database of Medicaid client information as a result of the phishing attempt. Eventually HP ES and Carewise Health were able to disable the laptop and notify the Cabinet for Health and Family Services of the breach.

UPDATE (01/02/2013): The employee revealed information to the hacker in mid-November.

Information Source: PHIprivacy.net

December 26, 2012
Integris Health
Oklahoma City, Oklahoma

A team of cyber security consultants discovered vulnerabilities in the Omnicell web system. Unauthorized users could gain control of certain hospital operations run by Integris Health. The issue was immediately addressed by Omnicell.

Information Source: PHIprivacy.net

December 24, 2012
State of California Department of Health Care Services (DHCS)
Sacramento, California

Those who were affected may call DHCS at (855) 297-5064.

Beneficiary Identification Cards (BICs) were mailed to the wrong recipients between December 10 and December 18. A computer programming error caused the BICs of children being moved from Healthy Families program enrollment to Medi-Cal enrollment to be sent to households of other Medi-Cal and Healthy Families participants. Names, Client Index Numbers, dates of birth, genders, and card issue dates were exposed. People who received incorrect cards were instructed to return them. Stamped envelopes that were addressed to DHCS were sent out with breach notifications.

Information Source: California Attorney General

December 22, 2012
Omnicell, University of Michigan Health System
Ann Arbor, Michigan

An electronic device was stolen from an Omnicell employee’s car on November 14. The device was not encrypted and contained the medication, demographic, and health information of 4,000 patients from three hospitals in the University of Michigan Health System.

UPDATE (1/2/2013): A total of 3,997 people who were treated between October 24 and November 13 at three hospitals in the University of Michigan Health System were affected. However, patients of at least 10 Sentara Healthcare and South Jersey Healthcare medical facilities were also affected. A total of 56,000 Sentara Healthcare patients from Sentara CarePlex, Sentara Leigh Hospital, Sentara Norfolk General Hospital, Sentara Obici Hospital, Sentara Princess Anne Hospital, Sentara Virginia Beach General Hospital, Sentara Williamsburg Regional Medical Center, Sentara Belle Harbour, Sentara Independence, and Sentara Port Warwick who were treated between October 18, 2012 and November 9,
2012 were affected. A total of 8,555 patients from South Jersey Healthcare who were either treated or scheduled for admission between June 1, 2012 and November 12, 2012 were affected.

Information Source: PHIPrivacy.net

December 22, 2012 Coastal Behavioral Healthcare, Inc. Sarasota, Florida

Numerous documents containing patient information were found in a vehicle during a traffic stop. A law enforcement officer notified Coastal Behavioral Healthcare of the potential breach on October 10, 2012. The documents contained a list of 136 Coastal Behavioral Healthcare patient names and identifying information dated April 2011. It is unclear how the information was breached and how many additional patients may have been affected.

Information Source: HHS via PHIPrivacy.net

December 22, 2012 Office of Dr. James M. McGee Stone Mountain, Georgia

The September 19 theft of paper records may have resulted in the exposure of dental patient information.

Information Source: HHS via PHIPrivacy.net

December 22, 2012 Robbins Eye Center Bridgeport, Connecticut

The data of 1,749 patients was stolen during an October 7 incident.

Information Source: HHS via PHIPrivacy.net

December 22, 2012 Vidant Pungo Hospital Belhaven, North Carolina

Paper jackets that held radiology films were thrown away with office trash instead of being properly discarded. The paper jackets contained names, addresses, dates of birth, ages, sex, race, and information on dates and names of radiology procedures prior to May of 2012. The paper jackets are believed to have been picked up by a sanitation company and discarded in a landfill.

Information Source: HHS via PHIPrivacy.net

December 22, 2012 Brigham and Women's Hospital Boston, Massachusetts

The October 16 theft of a desktop computer may have resulted in the exposure of patient information.

UPDATE (12/28/2012): The computer was stolen from the Brigham and Women's Hospital office. Medical record numbers, age, medications, laboratory values and other clinical information may have been on the computer. Up to 615 people may have been affected by the theft.

Information Source: HHS via PHIPrivacy.net

December 21, The Children's Center
An employee of Grand Teton Storage removed documents from The Children’s Center’s storage facility after they failed to pay storage bills. A concerned citizen found seven boxes of the old medical records and other personal information next to a dumpster. The information was seven to eight years old and included names, Social Security numbers, addresses, dates of birth, and payroll information. A Grand Teton Storage employee acknowledged that a mistake had been made and the employee who improperly disposed of the records will face disciplinary action. Idaho Department of Health and Welfare eventually recovered and secured the records.

Information Source: PHIPrivacy.net

December 21, 2012 CCS Medical Savannah, Georgia

The breach occurred in Florida and the location listed is that of CCS Medical’s headquarters.

An employee reported that another employee appeared to have been misusing patient information. The dishonest employee may have accessed, recorded, and disclosed Social Security numbers and other personal information for the purpose of obtaining fraudulent tax returns. The employee was reported on September 20 and the possibility that the employee had engaged in dishonest behavior was confirmed on October 17. Patient information that was maintained by CCS Medical between May 1, and September 21, 2012 may have been accessed. Notifications were sent to patients on December 7, 2012.

At least 23 New Hampshire residents may have been affected. The total number of affected patients nationwide was not reported.

UPDATE (10/1/2013): A total of 6,601 people may have been affected.

Information Source: PHIPrivacy.net

December 21, 2012 Skagit Valley Casino Resort, Bally Technologies Inc. Las Vegas, Nevada

An electronic device was stolen from the home office of an employee of Bally Technologies. The electronic equipment contained names, Social Security numbers, driver’s license numbers, and bank account information. The equipment may have been stolen for its resell value rather than the value of the information.

Information Source: California Attorney General

December 21, 2012 Fairfax High School Fairfax, Virginia

Fairfax County Public Schools discovered that student names, ID numbers, grades, and other information were posted online. Students enrolled in 9th, 10th, and 11th grade were affected. The information may have only been available for a day before Fairfax County Public Schools began the process of removing it from online.

Information Source: Databreaches.net

December 21, 2012 Workers United New York, New York

The theft of a hard drive from the office of an unnamed independent contractor resulted in the exposure of sensitive information. The theft occurred on either October 13 or 14 of 2012 and Workers United learned of the issue on October 25. A database with former Workers United member names and Social Security numbers was on the hard drive.

Information Source: Databreaches.net

December 20, 2012 Jetro, Restaurant Depot College Point, New York

Customers who used payment cards in several store locations discovered fraudulent charges on their debit and credit cards. It is unclear if a breach affected the physical machines in the stores or if the payment processing system was hacked. The company discovered the issue on December 4 and an investigation revealed that the intrusions began on November 7, 2012. Anyone who used their payment card in a store between November 7 and December 5 of 2012 should closely review their financial statements. Customers are also warned to be suspicious of phishing emails or phone calls. Customers should not give their information out over the phone or respond to emails asking for sensitive information.
Over 480 registered medical marijuana patients received an email from the New Jersey Department of Health. The email instructed them not to call New Jersey or the dispensary in Montclair to make an appointment. The email did not hide the email addresses of the recipients.

Information Source: PHIPrivacy.net

A staffing manager collaborated with the owner of A Caring Hand Home Health Care Services, Inc. (A Caring Hand) to hide Medicaid fraud. Between January of 2008 and October of 2011 the owner of A Caring Hand submitted about 900 fraudulent Medicaid claims for payment for services provided to 30 Medicaid recipients. The Medicaid recipients never received those services and around $630,000 was fraudulently obtained by the owner of A Caring Hand. The staffing manager and other staff members falsified office records at A Caring Hand to cover up the fraud between September 2010 and October 6 of 2011. The staffing manager was sentenced and the owner of A Caring Hand will be sentenced in January of 2013.

Information Source: PHIPrivacy.net

Western University of Health Sciences’ BanWeb Self-Service Federal Work Study reports were accessible to people who used BanWeb with a Western University of Health Sciences user ID and password. The reports contained names, Social Security numbers, and direct deposit bank account information in some cases. The information was available for an unspecified amount of time. Western University of Health Sciences conducted an investigation and reported that there was no reason to believe sensitive information was accessed by unauthorized BanWeb users. Western University of Health Sciences disabled access to the reports after learning about the breach on November 14. Notifications were sent on December 18.

Information Source: California Attorney General

An unauthorized party accessed WTH’s booking system by misusing the log-in credentials of an authorized user. Encrypted credit card numbers and expiration dates that were stored and could be decrypted in the system were exposed.

Information Source: California Attorney General

The owner of EZ Step and an employee were both charged with conspiracy to commit health care fraud. They were also charged on multiple counts of health care fraud. The charges come from allegations that the two people sought reimbursement by forging physician signatures, fabricating prescriptions and equipment orders, forging patient signatures on delivery forms to misrepresent prescription medication and durable equipment deliveries, and altering valid prescriptions between 2005 and 2007. Arrests were first made in July of 2011.

Information Source:
At least 36 Walgreens stores in San Diego County had violations. Over 600 Walgreens stores in California counties such as Alameda, Riverside, Los Angeles, San Joaquin, Solano, Monterey, and Yolo were also involved in the lawsuit.

Walgreens was ordered to pay $16.57 million as a part of a settlement of a civil environmental prosecution. Walgreens was accused of illegally dumping hazardous waste as well as confidential customer medical information. It is unclear what type of customer medical information was mishandled.

UPDATE (12/13/2012): The civil enforcement lawsuit was first filed in Alameda County in June of 2012. It was the result of investigations that took place in San Diego County in the summer and fall of 2011. Investigators discovered that “Walgreens routinely and systematically sent hazardous waste to local landfills and failed to take measures to protect” customer medical privacy.

A skimming device on an ATM resulted in fraudulent transactions on over 800 accounts. The fraudulent transactions appear to date from October 27, 2012 to November 7, 2012. It is not clear how many skimming devices were involved and where they were located.

Wilton learned that a malicious user was able to view user information between July 19 and October 2 of 2012. The user had added a file to a computer server that hosts www.wilton.com and www.copco.com. Names, addresses, telephone numbers, and payment card numbers, expiration dates, and security codes may have been accessed. The discovery was made sometime around October 31 and notifications were sent on December 10.

The malicious user was unable to access payment card information between October 2 and the discovery of the breach on October 31 because Wilton changed its payment processing system on October 2. Wilton took additional security measures after learning of the breach on or around October 31.

A December 1 office burglary resulted in the theft of an unencrypted computer. The computer contained files that included current and former Mt. Diablo Unified School District employee names, Social Security numbers, dates of birth, and addresses. People who were employees between 1998 and 2010 may have been affected.

A University laptop was stolen from an employee’s locked car. Pepperdine learned of the theft on November 12, 2012. The laptop may have contained names, Social Security numbers, addresses, and/or dates of birth.

UPDATE (12/11/2012): As many as 8,300 people may have been affected. The laptop had been used for work related to the IRS and contained data from as far back as 2008. About 75 percent of the people affected were students.

Approximately 1,200 photo records of 566 patients were publicly posted on November 30. The information was removed
and two managers resigned as a result of the breach.

Information
Source: Media
December 10, 2012, **Accume Partners, WeiserMazars**
Mooresstown, New Jersey

The October 10 theft of a laptop resulted in the exposure of sensitive information. A WeiserMazars employee had a laptop stolen that contained names, Social Security numbers, and in some cases, addresses, dates of birth, 401(k) information, and payroll information for Accume Partner 401(k) Plan participants. WeiserMazars audits the statement of net assets available for Accume Partner's 401(k) plan. WeiserMazars notified Accume Partners on October 31 and Accume Partners sent notifications to those who may have been affected on November 16.

Information
Source: California Attorney General
December 10, 2012, **ABQ Health Partners**
Albuquerque, New Mexico

A laptop computer was discovered lost or stolen. It contained a spreadsheet of patient names, dates of birth, health plan ID numbers, and diagnosis information.

Information
Source: PHIprivacy.net
December 10, 2012, **West Pittsburgh Partnership**
Pittsburgh, Pennsylvania

A concerned citizen investigated a pile of documents next to a dumpster. The documents contained names and Social Security numbers. A local news team responded to the story and contacted a representative from West Pittsburgh Partnership. West Pittsburgh Partnership began an investigation into how the job placement program documents dating back to 1992 were exposed.

Information
Source: Databreaches.net
December 10, 2012, **Michigan State University**
East Lansing, Michigan

A hacker published approximately 1,500 Michigan State University names, email addresses, user IDs, encrypted passwords, and mailing addresses.

Information
Source: Media
December 7, 2012, **Pinkerton Government Services (PGS)**
Washington, District Of Columbia

The November 15 office theft of several computers may have resulted in the exposure of current and former employee information. PGS believes that the computers were stolen for their hardware and software value rather than the information they contained. Some former and current PGS employees had their names, addresses, Social Security numbers, and possibly other types of information exposed.

Information
Source: California Attorney General
December 7, 2012, **Carolinas HealthCare System**
Charlotte, North Carolina

An unauthorized electronic intrusion may have affected up to 6,300 patients from Carolinas Medical Center-Randolph. The intruder accessed a provider's email account and could have obtained patient names, dates and times of service, dates of birth, diagnosis and prognosis information, medications, results, and referrals. The Social Security numbers of five patients who had their Social Security numbers sent through or received by the email account may have also been obtained.

The issue was discovered on October 8 and the intruder is believed to have accessed emails from the account between March 11, 2012 and October 8, 2012.
December 7, 2012

**Rock Bottom Auto Sales**

Hudson, Florida

BSR  PHYS  Unknown

At least eight garbage bags that were left unattended on a dirt road contained sensitive documents. A woman found the bags and reported the issue to a local news team. The paperwork included credit applications with names, driver’s license information, and Social Security numbers.

---

December 5, 2012

**California Department of Healthcare Services**

Sacramento, California

MED  DISC  14,000

Those who may have been affected may call 1-855-297-5064 for assistance from DHCS.

Names and Social Security numbers were discovered on the website of the Department of Health Care Services. People who sent their information in order to become a provider of In-Home Supportive Services (IHSS) may have had their information exposed online between November 5, 2012 and November 20. The issue was discovered on November 14 and was not fully addressed until November 20.

The list should have only contained provider names, addresses, and provider types. It also contained Social Security numbers that were listed in the column for Provider Billing Numbers. The Social Security numbers were not easily recognizable in this format.

**UPDATE (12/11/2012):** Nearly 14,000 people were affected.

---

December 4, 2012

**Louisiana State University (LSU) Hospital System**

Baton Rouge, Louisiana

MED  INSD  416

A dishonest employee working in the billing department used her position to access account information. She scanned checks and identification information from the LSU hospital system database and passed them on to at least four women. The scheme was discovered when the four women were allegedly caught on camera making purchases with fake checks. Handwritten Social Security numbers, check and ID card printing items, computers, and copies of scanned checks were found when the women’s homes were searched.

At least seven people face charges that include identity theft, conspiracy to commit identity theft, conspiracy to commit monetary abuse, and possession of fraudulent documents for identification purposes. The dishonest employee was charged with 377 counts of identity theft.

**UPDATE (01/02/2013):** LSU Health notified 416 patients after a hospital employee discovered fraudulent activity on her checking account.

---

December 4, 2012

**Surgical Associates of Utica, Quanterion Solutions, Inc.**

Utica, New York

MED  STAT  1,017 (No SSNs or financial information reported)

The theft of a network server on or around September 18 may have resulted in the exposure of sensitive patient information. A notification was sent to the US Department of Health and Human Services (HHS) on November 16.

---

December 4, 2012

**First Step Counseling, Inc.**

Metuchen, New Jersey

MED  PHYS  638 (No SSNs or financial information reported)

An unauthorized disclosure of paper records may have exposed patient information. The breach may have taken place between May 1, 2011 and August 5, 2011. It was discovered or reported on November 16 of 2012.
The theft of paper records may have resulted in the exposure of patient information. The theft may have occurred on August 13, 2012 and was reported or discovered on November 16, 2012.

Information Source: HHS via PHIPrivacy.net

December 1, 2012 University of Virginia Medical Center, Continuum Home Infusion Charlottesvillle, Virginia MED PORT 1,846 (Unknown number of SSNs)

A handheld electronic devices used by Continuum pharmacists was discovered missing on October 5. The device was not encrypted and contained patient names, addresses, diagnoses, medications, and health insurance identification numbers. Some health insurance identification numbers were Social Security numbers or contained Social Security numbers. Patients who received services from Continuum during the month of September 2012 and potential patients who were referred to Continuum between August 2007 and September 2012. Notifications were sent on November 30.

Information Source: PHIPrivacy.net

December 1, 2012 Jackson North Medical Center, Jackson Health System Miami, Florida MED INSD 566

A dishonest volunteer was caught passing patient information to people who used it to file fraudulent tax returns. The volunteer used his smart phone to capture patient records while working in an emergency room. Around 1,200 photos of 566 patient records were found on his phone. The breach was discovered when three men were caught using free wi-fi at McDonald’s to file fraudulent tax returns in March.

UPDATE (01/11/2013): Jackson Health banned volunteers from using cell phone in patient areas in order to prevent similar events from occurring.

Information Source: PHIPrivacy.net

November 30, 2012 Inova Fairfax Hospital Cardiac Care Center, Inova Fair Oaks Hospital Fairfax, Virginia MED CARD Unknown

Someone discovered card skimming devices at an ATM near a gift shop of the Inova Fairfax Hospital Cardiac Care Center and at an ATM next to the Inova Fair Oaks Hospital cafeteria. One device was discovered by a hospital employee who attempted to use the ATM and witnessed the skimmer fall from the ATM. A skimming device was previously discovered at the same Inova Fairfax Hospital Cardiac Care Center ATM in September. It is unclear how long the devices were there and people who used them are urged to check their financial statements.

Information Source: PHIPrivacy.net

November 30, 2012 Florida Hospital Tampa (formerly University Community Hospital Medical Center), Crothall Healthcare, Naval Medical Center (Bob Wilson Naval Hospital) Tampa, Florida MED INSD 45

Three people were arrested for their roles in filing 225 fraudulent tax returns. They face charges of conspiracy, theft of government property, and aggravated identity theft. About $555,000 in refund money was obtained. One of the defendants worked at Florida Hospital Tampa through a maintenance and housekeeping company. Information came from a variety of medical centers in California and Florida. There was an incident where the dishonest worker provided her co-conspirators with a list of names and Social Security numbers from patients seen at Florida Hospital Tampa on January 17 of 2012 and another incident where ER patient names, Social Security numbers, and other information was stolen from Crothall Healthcare in January.

Information Source: PHIPrivacy.net

November 30, 2012 Western Connecticut State University Danbury, Connecticut EDU DISC 235,000

A computer vulnerability allowed the information of students, student families, and other people affiliated with the University to be exposed. The records covered a 13 year period and included Social Security numbers. High school students who had associations with the University may have had their SAT scores exposed as well. The issue existed between April 2009 and September 2012.

Information Source: Media
November 29, 2012
WestCoast Children's Clinic
Oakland, California

A referral document containing sensitive information was accidentally sent in an email to an unauthorized recipient. Patient names, Social Security numbers, dates of birth, addresses, and health concerns were sent to a county social worker. The county social worker deleted the sensitive email and any other existing copies of the document were securely deleted from the network.

The WestCoast Children's Clinic will not provide referral forms to outside agencies in order to protect against future inadvertent sharing of private information. Disciplinary actions will also be taken against the employees involved in the privacy breach.

Information
Source: California Attorney General

November 29, 2012
St. Catherine Medical Center
Ashland, Pennsylvania

Sensitive patient and employee records were left unsecured in the abandoned medical center. A November 10 auction of office equipment and computers was held in the medical center, but one person reported seeing piles of sensitive documents and being able to access sensitive items like badges of former employees. The person provided pictures of personnel records and other items that should have been secured. A representative speaking on behalf of those responsible for safeguarding private information responded that the pictures were taken behind an area that had been secured with a rope. Additionally, the person claims that one of the computers that was purchased at the auction still contained sensitive information.

Information
Source: PHIprivacy.net

November 29, 2012
Vidant Pungo Hospital
Belhaven, North Carolina

Patient information was exposed by the accidental disposal of paper jackets with old radiology films. Patient information such as name, address, age, date of birth, race, sex, name of radiology procedure and radiology procedure date was exposed. The paper jackets were sent to a local landfill.

Information
Source: PHIprivacy.net

November 28, 2012
Advanced Data Processing, Inc. (ADPI), Grady EMS
Roseland, New Jersey

Information from certain ambulance agencies was inappropriately accessed and disclosed. Patient account information such as names, Social Security numbers, dates of birth, and record identifiers were exposed by a dishonest ADPI employee. ADPI learned of the breach on October 1. The dishonest employee was fired and apprehended by authorities.

UPDATE (12/04/2012): The former ADPI employee stole information associated with Grady EMS ambulance service. About 900 Grady EMS patients had their information exposed between June 15, 2012 and October 12, 2012.

UPDATE (01/05/2013): A detailed list of the organizations and number of people who were affected is available on phiprivacy.net here: http://www.phiprivacy.net/?p=10825

UPDATE (03/08/2013): Osceola County EMS released a notification in March of 2013 here: http://tinyurl.com/a335kak

UPDATE (03/14/2013): The Yuma, Arizona Fire Department was also affected by the breach. ADP handles the billing for Yuma's emergency medical services. Names, Social Security numbers, dates of birth, and record identifiers may have been accessed.

UPDATE (08/28/2013): ADPI learned of the tax scheme after being notified by Tampa, Florida police. The IRS confirmed that Valparaiso Fire Department information was compromised by the breach in July of 2013. Patients seen at Valparaiso Fire Department or by Valparaiso Fire Department ambulances between January 1 and June 21 of 2012 may have had their names, Social Security numbers, and dates of birth exposed.

Information
Source: California Attorney General

November 28, 2012
Westside Park Elementary School Based Health Center
Adelanto, California

1,370 (No SSNs or financial information reported)
A burglary sometime around October 1 may have resulted in the exposure of patient names, Social Security numbers, phone numbers, addresses, dates of birth, health conditions, medications, and other health information. The information was in a locked room that was accessed, but it appears that none of the paper records were stolen. Thieves took a television and other items.

**Information Source:**
PHIPrivacy.net

**November 27, 2012**
**Soundental Associates P.C.**
**West Haven, Connecticut**
MED PORT Unknown

A bag of personal items and back-up media cartridges from Soundental was stolen from an employee’s car on September 24. The back-up cartridges had patient names, addresses, treatment records, and dates of birth. Social Security numbers were also exposed in some cases. The cartridges had been scrambled to prevent easy access.

**Information Source:**
PHIPrivacy.net

**November 27, 2012**
**Long Chiropractic**
**Dayton, Ohio**
MED PHYS Unknown

A November 26 office burglary may have resulted in the theft of patient records. A safe with computer disks and a laptop computer were stolen. It is unclear if either contained sensitive patient information. The burglars were in the office for 15 minutes and may have taken or viewed sensitive patient information in other areas.

**Information Source:**
PHIPrivacy.net

**November 27, 2012**
**University of Arkansas for Medical Sciences (UAMS)**
**Little Rock, Arkansas**
MED INSD 1,500 (No SSNs or financial information reported)

Anyone who was a patient at UAMS and had surgery or was seen by a neurosurgeon from January 2010 to June 2010 may call UAMS toll-free hotline at 888-729-2755 to learn if they were affected by the breach.

A former resident doctor kept the personal information of about 1,500 patients as part of a lawsuit she filed against UAMS. She also claimed to have kept the information for research purposes. UAMS became aware of the issue on October 9 when the former resident doctor used the documents as part of her lawsuit. UAMS learned that she kept additional documents on November 7 and had provided them to UAMS attorneys on June 25. Some patients had their names, addresses, dates of birth, medical record numbers, and dates of service exposed. Other patients had their ages, locations of care, dates of service, diagnoses, medications, surgical procedures, procedure names, and lab results exposed.

**Information Source:**
PHIPrivacy.net

**November 27, 2012**
**Pinnacle Foods Group, LLC**
**Clinton, Wisconsin**
BSR PORT 1,818

Those with questions may call Pinnacle at (855) 477-6879.

A laptop taken from an employee’s home on October 11 contained sensitive information. It contained names, Social Security numbers, driver’s license numbers, credit card numbers, and other personal information.

**Information Source:**
Databreaches.net

**November 27, 2012**
**Sourcefire**
**Columbia, Maryland**
BSO PORT 500

The November 6 theft of an unencrypted laptop may have resulted in the exposure of employee Social security numbers. It is unclear if other types of information were also exposed. A total of 500 employees may have been affected.

**Information Source:**
Media

**November 27, 2012**
**Pulaski Bank**
**Overland Park, Kansas**
BSF PHYS Unknown

An employee left sensitive loan application documents in a vehicle while at the gym. The documents were stolen and included loan applicant tax returns. The breach occurred in September.

**Information Source:**
Databreaches.net
An unencrypted flash drive was discovered lost or stolen on September 25. It contained patient names, Social Security numbers, dates of birth, health insurance information, diagnoses, and progress notes. The information came from patients who participated in the St. John Sports Medicine Program and were treated between January 1, 2011 and July 31, 2012.

**Information Source:**
PHIPrivacy.net

---

Scripps College is located in Claremont, California and the theft took place in Anaheim, California.

Sensitive records were stolen from a tote bag in a staff member’s vehicle on the night of November 18. The records included names, dates of birth, cell phone numbers, email addresses, and emergency contact information.

**Information Source:**
Databreaches.net

---

An employee disclosed personal information about workers compensation claimants between October 2011 and March 2012. Workers compensation claimants who received spinal surgery in Southern California between 2004 and 2011 or had urinalysis testing, diagnostics or medical services performed in California between 2006 and 2011 may have had their information exposed.

It does not appear that Social Security numbers or other identifying information exposed were used to compromise the security, confidentiality, or integrity of the personal information.

**UPDATE (11/23/2012):** About 2,700 workers’ compensation claimants were affected.

**Information Source:**
California Attorney General

---

A hacker gained access to the ATS system and may have accessed financial information. The attack was discovered on August 1 and financial information was immediately removed from the ATS online system.

**Information Source:**
California Attorney General

---

Affected Georgia consumers may call 1-800-760-1125. Other consumers with questions may call 1-800-656-2298.

A portion of the computer network used by Nationwide and Allied Insurance agents was breached by cyber criminals on October 3. The attack was discovered on the same day and contained. On October 16, it was determined that names, Social Security numbers, driver’s license numbers, dates of birth, marital status, gender, occupation, and employer information had been stolen. Affected parties were identified on November 2 and notifications were sent on November 16.

**UPDATE (11/20/2012):** At least 28,000 people in Georgia were affected. The total number of affected people is not known.

**UPDATE (12/10/2012):** A total of 28,468 people in Georgia, 534 in Oklahoma, 12,490 in South Carolina, 286 in Maryland, 5,050 in California, 91,000 in Iowa, 170 in Hawaii, 8,000 in New Mexico, and 98,191 in Minnesota were affected. This brings the known total to 244,188. Nationwide/Allied Group reported that the breach compromised the information of one million policyholders and non-policyholders nationwide.

**Information Source:**
California Attorney General

---

The office theft of a laptop resulted in the exposure of patient information. A spreadsheet with sensitive information that
could be easily accessed was on the stolen laptop. It is unclear what type of information was exposed, but Social Security numbers, addresses, and medical information were not involved.

**UPDATE** (12/21/2012): A Health and Human Services (HHS) notice reveals that the theft occurred on October 1. A total of 683 patients were affected by the breach.

### Information
**Source:** PHIPrivacy.net

**November 14, 2012**
**Highlandtown Community Health Center, Johns Hopkins Hospital**
**Baltimore, Maryland**

MED INSD 250

At least four people were involved in an identity theft ring that affected over 250 people. One member of the ring was employed by Highlandtown Community Health Center and provided personal and financial patient information that he accessed through his position. The information was used by other ring members to create counterfeit checks and fraudulent state identification cards. The fraud occurred between August and October of 2009.

Another member of the ring was employed by Johns Hopkins Hospital and provided the information of doctors who applied for fellowships there. Several ring members rented apartments under the identities of doctors. Two of the members pleaded guilty to conspiring to commit wire fraud and aggravated identity theft. The four members of the ring are required to collectively pay restitution for fraudulently obtained cash, merchandise, and services worth over $188,000.

### Information
**Source:** PHIPrivacy.net

**November 14, 2012**
**Adobe**
**San Jose, California**

BSO HACK 230 (No SSNs or financial information reported)

A hacker released the names, email addresses, and encrypted passwords of 230 members of Adobe’s company database. The hacker claimed to have access to over 150,000 records. Adobe announced that it would reset approximately 150,000 passwords of members of the Connectusers.com site.

**UPDATE** (11/14/2012): The 230 people who were affected also had their titles, affiliated organizations, and usernames exposed. A number of those affected were associated with U.S. government agencies such as the Department of Transportation, the Department of Homeland Security, the U.S. State Department, and the Federal Aviation Administration.

### Information
**Source:** Databreaches.net

**November 13, 2012**
**Sprechman & Associates, P.A.**
**Miami, Florida**

BSF INSD Unknown

An employee may have performed unauthorized searches on clients. The employee is no longer with the company. Names, Social Security numbers, addresses, dates of birth, and driver’s license numbers may have been exposed. The potential breach was discovered in July and clients were notified in October after their contact information was confirmed.

### Information
**Source:** California Attorney General

**November 13, 2012**
**National Aeronautics and Space Administration (NASA)**
**Washington, District Of Columbia**

GOV PORT 10,000 (No SSNs or financial information reported)

An October 31 theft of a NASA laptop and sensitive NASA documents from an employee’s locked car resulted in the exposure of employee information. Contractors and other non-employees associated with NASA were also affected. Employees are encouraged to be suspicious of communication from individuals claiming to be from NASA. It may take up to 60 days to send official notifications to those who were affected.

**UPDATE** (12/14/2012): Up to 10,000 employees and people associated with NASA may have been affected.

### Information
**Source:** Databreaches.net

**November 13, 2012**
**Chicago Board of Elections Commissioners**
**Chicago, Illinois**

GOV DISC 1,200 (No SSNs or financial information reported)

The sensitive information of Chicago voters was exposed online due to a mistake by the election authority. A database
that included names, the last four digits of Social Security numbers, addresses, and drivers license numbers was accidentally placed online in a publicly accessible place. Only people who applied to work for the board in Chicago polling places on Election Day were determined to have been affected.

A forensic investigation firm believes that as many as 1.7 million registered voters had their names, addresses, and voter registration numbers exposed. However the Chicago Board does not believe that information should be considered sensitive.

Information
Source: Databreaches.net

November 11, 2012
Labelmaster (American Labelmark Company)
Chicago, Illinois
BSO HACK Unknown

A hacker accessed the e-commerce site labelmaster.com. Customer names, addresses, credit card numbers, and credit card expiration dates were exposed.

Information
Source: Databreaches.net

November 10, 2012
Aler Home Monitoring, Inc.
Livermore, California
MED PORT 100,000

The September 23 theft of an employee’s unencrypted laptop resulted in the exposure of information of over 100,000 patients. The laptop was stolen from the employee's home. Names, Social Security numbers, addresses, and diagnosis information of patients taking drugs to prevent blood clots were exposed. Aler became aware of the breach on October 1.

Information
Source: PHIPrivacy.net

November 10, 2012
Gulf Coast Health Care Services
Pensacola, Florida
MED INSD 13,000 (No SSNs or financial information reported)

A network security incident resulted in the expose of patient information. The breach occurred on August 17.

UPDATE (11/26/2012): An employee accessed and downloaded patient information without authorization or a legitimate purpose on five occasions between June 29 and September 20 of 2012. Gulf Coast Health Care Services discovered the issue on September 26. Patients who were seen between 1992 and September 20, 2012 may have had their names, addresses, dates of birth, and phone numbers accessed. It appears that the employee was accessing the data for the purpose of helping outside practitioners recruit patients to their own practices. The incident was reported to the FBI, the Sarasota Police Department, and the Florida Department of Law Enforcement.

This entry on the Privacy Rights Clearinghouse Chronology of Data Breaches was previously listed as a hack and was reclassified as an insider breach based on new information.

Information
Source: HHS via PHIPrivacy.net

November 10, 2012
Baptist Physicians Lexington
Lexington, Kentucky
MED PORT 2,376 (No SSNs or financial information exposed)

A device with patient information was discovered lost or stolen on August 15.

Information
Source: HHS via PHIPrivacy.net

November 10, 2012
Bob Ward & Sons
Bozeman, Montana
BSR HACK Unknown

The Bob Ward & Sons website was hacked on June 6, 2011. Customers who made online purchases between May 31 and August 3 of 2012 may have had their names, addresses, and credit card information exposed. Ward became aware of the issue when he received a notice from Discover that revealed some customers had experienced fraudulent charges.

Information
Source: Databreaches.net

November 9, 2012
Memorial Hospital
Colorado Springs, Colorado
MED PHYS 6,400 (No SSNs or financial information exposed)
Concerned patients may call 1-866-283-9930

Laboratory reports for about 6,400 patients were discovered missing. The reports contained bill processing information and charges for laboratory services. Patients who had lab work done between May 1, 2012 and August 31, 2012 had their names, Memorial internal account numbers, lab work dates, and types of lab work exposed.

**Information Source:**
PHIPrivacy.net

<table>
<thead>
<tr>
<th>Date</th>
<th>Organization</th>
<th>Location</th>
<th>Affected Patients</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>November 7</td>
<td>4Access, National Processing Company</td>
<td>Louisville, Kentucky</td>
<td>6,400</td>
<td>An unauthorized person may have gained access to the computer network that supported certain 4Access terminals. These terminals were connected to a computer network that allowed merchant transaction processing. The unauthorized entry was discovered on September 24. Check processing information stored in the network such as check writer’s name, checking account and routing numbers, address, and driver’s license number may have been accessed. No credit card information was exposed.</td>
</tr>
<tr>
<td>November 6</td>
<td>Women &amp; Infants Hospital</td>
<td>Providence, Rhode Island</td>
<td>14,004</td>
<td>WomenandInfants.org posted a notice: <a href="http://www.womenandinfants.org/news/Confidentiality-Notice-for-Patients.cfm">http://www.womenandinfants.org/news/Confidentiality-Notice-for-Patients.cfm</a> Those with questions may call 1-877-810-7928. Unencrypted backup tapes containing ultrasound images from ambulatory sites were discovered missing on September 13. The information was from Providence, Rhode Island between 1993 and 1997 and New Bedford, Massachusetts between 2002 and 2007. Patient names, dates of birth, dates of exams, physicians' names, and patient ultrasound images were exposed. A limited number of current and former patients also had their Social Security numbers exposed. Notifications began on November 5. <strong>UPDATE</strong> (11/10/2012): A total of 14,004 patients were affected.</td>
</tr>
<tr>
<td>November 5</td>
<td>Illinois Department of Healthcare and Family Services</td>
<td>Springfield, Illinois</td>
<td>508</td>
<td>The August 31 theft of a briefcase from the home of a contractor resulted in the exposure of nursing home residents. The briefcase contained names, Social Security numbers, Medicaid recipient numbers, and dates of birth.</td>
</tr>
<tr>
<td>November 4</td>
<td>Symantec, ImageShack</td>
<td>Mountain View, California</td>
<td>1,000 (No SSNs or financial information exposed)</td>
<td>A hacking spree resulted in unauthorized access to the ImageShack server and a Symantec portal. Names, phone numbers, emails, domains, passwords, usernames, and other information were exposed.</td>
</tr>
<tr>
<td>November 1</td>
<td>Salinas Valley State Prison (SVSP)</td>
<td>Soledad, California</td>
<td>2,000</td>
<td>Names and Social Security numbers of people associated with Cornell were publicly available for five days. The information was on a computer in Cornell’s athletics department and was accidentally placed online from September 5, 2012 until September 10, 2012.</td>
</tr>
</tbody>
</table>
Sensitive staff information on a database file was found to have been accessible to all SVSP staff. Staff names, Social Security numbers, phone numbers, addresses, and institutional-position information were exposed. The breach was discovered on September 26 and it is unclear how long the information was available.

Information  
Source: California Attorney General  
October 30, 2012  
**HSBC Bank USA National Association**  
New York, New York  
BSF INSD Unknown  

An employee resigned and left with customer account information. Names, Account numbers, account types, and phone numbers may have been exposed. The breach occurred in late July.

Information  
Source: California Attorney General  
October 29, 2012  
**Kaiser Permanente**  
Oakland, California  
MED DISC Unknown  

Those with questions may call 866-578-5413.

A Kaiser Permanente Northern California Region Recruitment employee mistakenly sent an email to unauthorized parties on August 24. Former Northern California Kaiser employees who left Kaiser between 1990 and 2006 may have had their names and Social Security numbers exposed. Kaiser IT Security conducted a detailed analysis to confirm that the recipient did not forward or print the email. The analysis also revealed that the email had been deleted and could no longer be accessed.

Information  
Source: California Attorney General  
October 29, 2012  
**Massachusetts Eye and Ear Infirmary**  
Boston, Massachusetts  
MED INSD 3,600  

A dishonest employee was arrested and fired in March after stealing patient information from Massachusetts Eye and Ear Infirmary. The former employee opened fake accounts to avoid paying for electricity. The investigation began in January when one of the victims noticed that her Social Security number had been used to open an account. Names and dates of birth were also compromised.

Information  
Source: PHIprivacy.net  
October 29, 2012  
**Abilene Telco Federal Credit Union, Experian**  
Abilene, Texas  
BSF HACK 847  

A hacker or hackers were able to access an Abilene Telco Federal Credit Union employee's computer in September 2011. The Bank's online account with Experian was then used to download the credit reports of 847 people. Social Security numbers, dates of birth and detailed financial data were exposed.

Information  
Source: Dataloss DB  
October 28, 2012  
**Optimum HealthCare Inc.**  
Tampa, Florida  
MED INSD 32  

An Optimum HealthCare claims specialist stole the personal information of at least 32 clients. The documents information was later found on a man who was arrested after a traffic stop in 2011. The man who was arrested never worked for Optimum and the dishonest employee who stole the documents is believed to have separated from Optimum.

Information  
Source: PHIprivacy.net  
October 28, 2012  
**Prescription Monitoring Program**  
Olympia, Washington  
MED UNKN 34  

An unauthorized party gained access to a physician's identity in order to view patient records. A fraudulent account was created under the doctor's identity in the Washington medical system. Medical information such as drugs dispensed and quantity dispensed may have been accessed before the fraudulent account was shut down.

Information  
Source: PHIprivacy.net  
October 27, 2012  
**Department of State Bureau of Consular Affairs**  
GOV INSD Unknown
A dishonest employee misused sensitive information in a State Department database to obtain fraudulent credit cards. He was part of a conspiracy sometime during his employment between September 2007 and March 2008. The group of conspirators successfully obtained $71,774 and attempted to obtain an additional $133,494 in fraudulent transactions. The dishonest employee pled guilty to conducting illegal transactions with credit cards and agreed to pay $71,774 in restitution.

Information Source: Databreaches.net

October 26, 2012
Alabama Department of Human Resources, Vinson Guard Service Inc., Jefferson Davis High School
Montgomery, Alabama

A notice from The United States Attorney's Office Middle District of Alabama can be found here: http://www.justice.gov/usao/alm/programs/vwa/victimnotification.html

An alert stating that the United States Attorney's Office is prosecuting cases related to the theft of personal identifying information and misuse of that personal identifying information was released. The information was stolen between January 1, 2009 and March 25, 2011. People from various organizations may have had their information misused to prepare fraudulent tax returns.

Information Source: PHIPrivacy.net

October 26, 2012
South Carolina Department of Revenue
Columbia, South Carolina

Citizens concerned about exposure may visit protectmyid.com/scdor and enter the code SCDOR123 or call 1-866-578-5422.

South Carolina Department of Revenue's website was hacked by a foreign hacker. The hack most likely began on August 27, was discovered on October 10, and was neutralized on October 20. Around 3.6 million Social Security numbers and 387,999 credit card and debit card numbers were exposed. A total of 16,000 payment card numbers were not encrypted.

UPDATE (10/31/2012): Tax records dating back to 1998 were exposed. A lawsuit alleging that South Carolina failed to protect citizens of South Carolina and failed to disclose the breach quickly enough was announced on October 31.

UPDATE (11/05/2012): Trustwave was named as the data security contractor who handled the South Carolina website and added to the group being sued over the breach. Trustwave is an international company based in Chicago.

UPDATE (11/15/2012): Over 4.5 million consumers and businesses may have had their tax records stolen by hackers. It appears that Trustwave focused on helping the Southern Carolina Department of Revenue comply with regulations regarding how credit card information is handled. Neither Trustwave nor the Southern Carolina Department of Revenue detected the breach.

UPDATE (11/29/2012): The total number of people or businesses affected was updated to 6.4 million. Approximately 3.8 million taxpayers and 1.9 million of their dependents had their information exposed. Additionally, 3.3 million tax payers had bank account information obtained. It is unclear how much overlap there is between the 3.8 million taxpayers and the 3.3 million tax payers who had bank account information obtained.

UPDATE (01/11/2013): A State IT division director reported that the SCDOR's former chief information officer and current computer security chief were notified on August 13 that 22 computers were infected with malicious code. The State's division of IT recommended that passwords be reset after the discovery, but they were not reset.

UPDATE (03/01/2013): A lawsuit brought against TrustWave and SCDOR by a former state senator has been dismissed by a judge. The former senator accused the agencies of conspiring to hide the fact that a massive breach had occurred and failing to adequately protect taxpayers from a potential hack.

UPDATE (04/02/2013): About 1,448,798 people signed up for free individual credit monitoring and 41,446 signed up for free family credit monitoring.

UPDATE (10/25/2013): It is estimated that South Carolina taxpayers will pay at least $8.5 million to pay for one year’s worth of free credit monitoring to those affected by the data breach. Over 650,000 businesses had their tax information exposed.

Information Source: Media

October 25, 2012
Waipahu Aloha Clubhouse
Waipahu, Hawaii

An employee noticed unusual activity on a computer on September 25, 2012. It is possible that former and current members of the Waipahu Aloha Clubhouse had information on the computer that was remotely accessed by an unauthorized party. Names, Social Security numbers, dates of birth, addresses, phone numbers, and consumer record numbers dating back to 1997 may have been exposed. Though the Clubhouse services people living with severe and persistent mental illness, no medical records were exposed.
Two dishonest employees misused customer credit card information to make more than $26,000 in fraudulent purchases. The two men face a maximum of 10 years in prison and a $50,000 fine for each of six counts of deceptive practices. The men were arrested on July 29.

Concerned customers may call 1-888-471-7809 or visit www.barnesandnobleinc.com

PIN pad devices used to process credit and debit card information in stores were compromised. The breach was discovered around September 14 during maintenance and inspection of the devices. Anyone who used a credit or debit card at a Barnes & Noble may have been affected by a sophisticated criminal effort to steal that information. Names, payment card account numbers, and PINs may have been exposed. Barnes & Noble removed all PIN pads. Fewer than 1% of the inspected PIN pads had been affected.

UPDATE (10/24/2012): A total of 63 Barnes and Noble stores in nine states had at least one compromised PIN pad device. Malicious code was installed on the PIN pads.

UPDATE (09/05/2013): A federal judge ruled that customers failed to show that their personal information was stolen in the data breach.

Two unencrypted backup tapes were discovered missing on September 10. They were lost sometime between August 27, and September 10. Names, Social Security numbers, financial account information, driver’s license numbers, and transaction records were exposed.

People who made purchases at Aultman Hospital’s gift shop may call 330-363-5319.

Hardware at Aultman was discovered to have been infected by a cyber attack. Unauthorized parties may have been able to access credit and debit card information from Aultman gift shop purchases between February and September of 2012.

A mailing error caused ID cards to be mailed to the wrong members. The cards were mailed on September 17, 2012 and the problem was discovered on September 18, 2012. Names, member ID numbers, and dates of birth were exposed.

UPDATE (05/21/2013): A total of 18,000 people were affected.
An office burglary resulted in the theft of a computer. The incident was discovered on September 15, 2012. Patient names and Social Security numbers were on the computer.

**UPDATE** (10/24/2012): The computer contained medical records and insurance information.

**Information**
Source: California Attorney General

October 22, 2012 **UPMC**
**Monroeville, Pennsylvania**

An assistant police chief filed a complaint alleging that the chief of police breached federal privacy law. The complaint alleges that the chief of police received information about ambulance dispatches that was primarily intended for medics and other active first responders. He also claims the chief of police forwarded the information to a third party.

**Information**
Source: PHIPrivacy.net

October 22, 2012 **Compete Inc**
**Boston, Massachusetts**

Compete Inc. reached an agreement with the Federal Trade Commission regarding the collection of consumer information. Compete agreed to obtain end users’ consent before collecting future online browsing data. Compete will also delete or anonymize consumer data already collected and provide direction for removing tracking software installed on the computers of those who had their data collected.

FTC charged that Compete failed to adequately describe two products used to collect details about end users’ browsing habits. A toolbar and input panel were used to collect extensive information about consumer activities and transmit the information in clear readable text to Compete’s servers. All websites visited by, links followed by, and advertisements displayed to Compete consumers were collected and stored.

**Information**
Source: Dataloss DB

October 19, 2012 **Sierra Plastic Surgery**
**Reno, Nevada**

Patients with questions or concerns about their information may call Sierra Plastic Surgery’s hotline at (866) 979-2596.

A computer system error caused sensitive information to be exposed. The breach occurred sometime between August 19, 2011 and September 20, 2011.

**UPDATE** (11/28/2012): It appears that the breach was related to a terminated employee who could still access Sierra Plastic Surgery’s network after leaving the company. The former employee accessed Social Security numbers, personal contact information, payment information, and other sensitive information in less than 50 instances. It also appears that some copies of patient surgery estimates were printed and subsequently surrendered by the former employee when the breach was discovered in August of 2012. The former employee was seeking information on compensation owed.

**Information**
Source: HHS via PHIPrivacy.net

October 19, 2012 **Valley Plastic Surgery, P.C.**
**harrisonburg, Virginia**

The July 15 theft of an electronic device exposed patient information.

**Information**
Source: HHS via PHIPrivacy.net

October 19, 2012 **Ecco Health, LLC, Colon & Digestive Health Specialists**
**Scottsdale, Arizona**

A vendor working with patient data for digital conversion from Colon & Digestive lost a flash drive on or around July 16. It contained patient names, Social Security numbers, dates of birth, addresses, telephone numbers, account numbers, diagnoses, and other protected health information.
Silver Spring, Maryland

Hackers targeted the U.S. National Weather Service website Weather.gov in an attempt to exploit vulnerabilities in U.S. government online systems. The hackers claim to have begun a campaign in response to U.S. cyber attacks in Muslim nations. Partial login credentials and system and network configuration files were accessed and posted online.

**Information**

**Source:**
Dataloss DB

**October 19, 2012  The College of St. Scholastica**  
Duluth, Minnesota

Hackers were able to guess the answers to student account challenge questions. The email account passwords of at least 28 students were reset and their account information was most likely accessed. The hackers may have been based in Beijing and most likely gathered the information needed to pass the challenge questions from information on the students' Facebook pages.

**Information**

**Source:**
Databreaches.net

**October 18, 2012  Blount memorial Hospital**  
Maryville, Tennessee

A password-protected laptop was stolen from an employee's home on August 25. It contained two groups of patient data. Patient names, dates of birth, responsible party names, patient addresses, physician names, and billing information for 22,000 patients were on the laptop. An additional 5,000 patients had similar information exposed as well as their Social Security numbers and other non-medical information.

**Information**

**Source:**
PHIPrivacy.net

**October 18, 2012  Southern Environmental Law Center**  
Charlottesville, Virginia

Sensitive information from Southern Environmental Law Center was placed online. Credit card, medical, and donor information such as addresses, phone numbers, and client files were exposed. The data was accessible via Google search for an unspecified amount of time. Southern Environmental Law Center is warning people not to open emails about the security failure or click on any links in emails that appear to be from Southern Environmental Law Center.

**Information**

**Source:**
Databreaches.net

**October 16, 2012  University of Georgia (UGA)**  
Athens, Georgia

The passwords of two University of Georgia (UGA) IT employees were reset and misused by an intruder. Names, Social Security numbers, and other sensitive data of current and former school employees may have been exposed. The breach may have begun as early as September 28, 2012.

**Information**

**Source:**
Media

**October 15, 2012  District 202, Plainfield School District**  
Plainfield, Illinois

People who applied online at www.applitrack.com for a job in District 202 may have had their information accessed by a hacker. The hacker sent messages to former and current job applicants and informed them that the Plainfield School District 202 website was breached.

**UPDATE** (10/19/2012): A 14-year-old Joliet West High School student was removed from class and taken to a juvenile detention center for his alleged involvement in the breach.
October 13, 2012  City of Burlington, Washington  
Burlington, Washington  
GOV  HACK  Unknown

A hacker or hackers managed to transfer $400,000 in city funds to accounts across the country. The cyber attack occurred sometime between Tuesday night and Wednesday morning. City employees may have also had their direct deposit bank account information compromised.

Information Source:  
Databreaches.net  
records from this breach used in our total: 0

October 12, 2012  AutoCarry  
North Bergen, New Jersey  
BSO  PHYS  100

An office burglary that occurred on October 10 resulted in the exposure of customer information. Paper documents that contained credit card numbers, addresses, and other personal information were taken.

Information Source:  
Databreaches.net  
records from this breach used in our total: 100

October 12, 2012  Korn/Ferry International  
Los Angeles, California  
BSO  HACK  Unknown

Those with questions may call 1-800-971-5875.

A cyber breach affected Korn/Ferry databases. Names, Social Security numbers, driver's license numbers, government-issued identification numbers, credit card numbers, and health information may have been exposed. The information may have been available to unauthorized parties for months before the breach was discovered in August of 2012.

Information Source:  
Databreaches.net  
records from this breach used in our total: 0

October 12, 2012  Army Material Command  
Huntsville, Alabama  
GOV  PHYS  400 (Unknown number of SSNs)

An employee transported a hard copy of sensitive employee documents home. The employee is not believed to have took the information for fraudulent or criminal activity.

Information Source:  
Databreaches.net  
records from this breach used in our total: 0

October 12, 2012  FEI Company  
Hillsboro, Oregon  
BSR  PORT  Unknown

The August 29 theft of a laptop resulted in the exposure of employee information. Employee names, Social Security numbers, information related to taxpayer I.D., dates of birth, home addresses, and employment information such as salaries were exposed.

Information Source:  
Databreaches.net  
records from this breach used in our total: 0

October 11, 2012  Centers for Medicare & Medicaid Services (CMS)  
Baltimore, Maryland  
GOV  UNKN  363 (No SSNs or financial information reported)

The CMS experienced 13 breaches between September 23, 2009 and December 31, 2011. The CMS failed to notify beneficiaries of seven of the breaches in a timely manner. The HHS's Office of the Inspector General (OIG) also alleges that the notifications mailed to beneficiaries did not disclose what type of information had been exposed, the date the breach occurred, or how CMS was working to prevent future breaches.

Information Source:  
PHIprivacy.net  
records from this breach used in our total: 0

October 11, 2012  PST Services, Inc., Litton and Giddings Radiological Associates, P.C.  
Springfield, Montana  
MED  PHYS  Unknown

Litton and Giddings' janitorial service, PST Services, failed to shred patient billing records before sending them to a Springfield recycling company. The records may have been viewed by unauthorized parties before being destroyed at the recycling center.

Information Source:  
PHIprivacy.net  
records from this breach used in our total: 0
An internal review revealed a hack of Northwest College servers. One or more hackers accessed at least one folder in the server between May 21, 2012 and September 24, 2012. Over 3,000 employees, 76,000 Northwest College student records, and 200,000 students eligible for Bright Future scholarships in 2005-06 and 2006-07 were affected. Bright Future scholarship data included names, Social Security numbers, dates of birth, ethnicity, and genders. Current and former employees that have used direct deposit anytime since 2002 may have had some information exposed. At least 50 employees had enough information in the folder to be at risk for identity theft.

Information Source: Databreaches.net

records from this breach used in our total: 200,050

October 10, 2012 PlaySpan Foster City, California

A hacker or hackers accessed PlaySpans computer system. User IDs, encrypted passwords, and email addresses of online players were exposed. Users are advised to immediately change their passwords and also any similar passwords for other logins associated with compromised email addresses. PlaySpan Marketplace may have also been affected and could be linked to user financial information.

Information Source: Media

records from this breach used in our total: 0

October 10, 2012 Equifax Atlanta, Georgia

Equifax settled charges with the Federal Trade Commission after it was discovered that Equifax Information Services improperly sold lists of consumer data. People who were late on their mortgage payments had their information sold to firms that should not have received the information and subsequently resold it to other firms. Equifax agreed to pay nearly $1.6 million to resolve charges that it violated the FTC and Fair Credit Reporting Acts. The settlement prohibits Equifax from providing prescreened lists to unauthorized parties, having poor procedures for releasing prescreened lists, and selling prescreened lists in certain circumstances.

Information Source: Media

records from this breach used in our total: 17,000

October 8, 2012 TD Bank Cherry Hill, New Jersey

Two data backup tapes were lost during shipping in late March 2012. The tapes included customer names, Social Security numbers, addresses, account numbers, debit card numbers, and credit card numbers.

UPDATE (10/13/2012): A total of 260,000 customers from Maine to Florida were notified.

UPDATE (10/15/2014): "TD Bank NA has agreed to pay $850,000 to settle a multistate probe into the security breach, New York's attorney general said".


UPDATE (12/10/2014): TD Bank has settled with the state of Massachusetts for $625,000, separate from the above previous settlement deals the bank made with other states.


Information Source: California Attorney General

records from this breach used in our total: 260,000

October 8, 2012 GreenStone Homes Columbus, Ohio

A pile of thousands of documents were found in the street. Two bags were stuffed with financial information such as tax returns with Social Security numbers. The information was found in the driveway of a model home that had been foreclosed in July 2011.

Information Source: Databreaches.net

records from this breach used in our total: 0

263
There is no specific location for this breach.

The University of Texas, University of Colorado, University of Pennsylvania, Duke University, Rutgers University, University of Pittsburgh, University of Florida, Case Western Reserve University, Texas A&M University, Boston University, Purdue University, University of Arizona, Arizona State University, University of Utah, Ohio State College of Dentistry, and additional universities were affected. Universities outside of the United States were also affected.

Each affected university is listed here: http://pastebin.com/AQWhu8Ek

A hacking group called Team GhostShell targeted universities around the world. A total of 53 universities were affected. Most of the data exposed was publicly available, but student, staff, and faculty usernames and passwords were also exposed. It is unclear if any financial information or Social Security numbers were taken from universities.

Information
Source: www.naperville.il.us
Naperville, Illinois

October 8, 2012

A cyber intruder injected a virus into the website of the city of Naperville. City officials claim that no resident credit card information was compromised. There is no evidence that any type of information was stolen from the website.

Information
Source: Dataloss DB

October 4, 2012

Monterey Institute of International Studies, Middlebury College
Monterey, California

EDU PORT Unknown

A September 14, 2012 home burglary resulted in the theft of a laptop. The laptop was password-protected and was stolen along with other items. Student names and Social Security numbers were on the laptop.

Information
Source: California Attorney General

October 2, 2012

Town Council of Chapel Hill
Chapel Hill, North Carolina

GOV DISC 12

A licensed clinical social worked accidentally attached confidential client information to an email that was forwarded to town council colleagues. A copy of her and her husband’s 2011 income tax returns was also in the email. The email automatically became available to the public and the error was noticed nearly a week later. Unfortunately, the email was also forwarded a second time to a public account. Consequently, the information was publicly available for a week.

Many of the affected clients were University of North Carolina students. Names, Social Security numbers, clinical notes about client mental health, payment amounts, and insurance forms were exposed.

Information
Source: PHIPrivacy.net

October 2, 2012

Robeson County Board of Elections
Lumberton, North Carolina

GOV PORT 71,000 (Partial SSNs exposed)

Five password-protected laptop computers that contained personal information of registered voters in Robeson County were discovered stolen in September. Voters had their names, addresses, dates of birth, and the last four digits of their Social Security numbers exposed. The computers went missing between July 18 and September 4. They were most likely taken while outside of their normally secured area and left with unsupervised community volunteers. Driver’s license numbers may have also been exposed. Those who were affected were mailed letters on September 12.

Information
Source: Databreaches.net

October 1, 2012

San Mateo Union High School District
San Mateo, California

EDU HACK Unknown

Hackers accessed San Mateo Union High School District’s computer system and attempted to use it to infiltrate FBI and CIA electronic systems. The District became aware of the problem when United States Naval Intelligence informed them that the District’s servers had been compromised. The hackers appear to have used additional organizations in their scheme.

Information
Source: Databreaches.net

September 29, 2012

Health and Sports Rehab, Inc.
Dorchester, Massachusetts

MED INSD Unknown
A dishonest intern stole personal information while working at the clinic. The information was used to create and cash fraudulent checks and the dishonest intern pled guilty.

Information Source: PHIPrivacy.net records from this breach used in our total: 0

September 28, 2012 University of Chicago Chicago, Illinois EDU DISC 9,100

A postcard mailed to University of Chicago employees contained their Social Security numbers. The cards were mailed on September 24 to remind employees about open enrollment, but also had Social Security numbers printed on the outside.

Information Source: Databreaches.net records from this breach used in our total: 9,100

September 28, 2012 Brightline Interactive, Army Chief of Public Affairs Alexandria, Virginia GOV DISC 518 (31 SSNs reported)

An army awards database was found to be available online. The database was being handled by the defense contractor Brightline Interactive and was mistakenly uploaded to a public server at an unknown time. Those who received awards for actions since September 11, 2001 were affected.

Information Source: Databreaches.net records from this breach used in our total: 31

September 27, 2012 Apex Laboratory Farmingdale, New York MED HACK Unknown

Apex Laboratory learned from law enforcement investigators on July 30 that an unauthorized party or parties accessed their computer systems. Patients may have had their names, Social Security numbers, addresses, phone numbers, dates of birth, gender, and insurance identification numbers were exposed.

Information Source: PHIPrivacy.net records from this breach used in our total: 0

September 27, 2012 Rite Aid Corporation Camp Hill, Pennsylvania BSR DISC Unknown

A customer using RiteAid’s mobile app to check a prescription noticed that he was able to access the names, addresses, and prescription records of other customers. The customer was able to identify some of the problems by using his computer science background. He noticed there was no secure login tied to web service calls made from the smartphone application. The customer was able to correspond with several RiteAid representatives and RiteAid began to address some of the security concerns.

Information Source: PHIPrivacy.net records from this breach used in our total: 0

September 27, 2012 Medical Solutions Management, Inc. Hicksville, New York MED PHYS 1,000

The owner of Medical Solutions Management, Inc. was convicted of wrongful disclosure of private patient information and Medicare fraud. The owner stole private patient information from nursing homes in Long Island and used the information to submit fraudulent claims to Medicare over the course of four and a half years. Over 1,000 people were affected. She faces a sentence of up to 10 years per count and could be fined up to $250,000 for each conviction count.

UPDATE (04/11/2013): The dishonest owner was sentenced to 12 years in prison. A total of 1.3 million dollars was seized from the owner and she was ordered to forfeit it at her sentencing. She had submitted 10 million dollars in fraudulent Medicare billings.

Information Source: PHIPrivacy.net records from this breach used in our total: 1,000

September 27, 2012 Center 4 Health Enlightenment Enrichment Empowerment Renewal Services (CHEERS) Phoenix, Arizona NGO INSD 180

A dishonest employee accessed and misused CHEERS client names, Social Security numbers, and birth dates. She, her sister, and her husband filed 180 tax returns under stolen identities and claimed over $1 million in tax refunds. The three face between three years and five years in prison.

Information Source: Databreaches.net records from this breach used in our total: 180

September 26, 2012 American Heart Association, Olive Crest Las Vegas, Nevada NGO PORT Unknown
An office burglary resulted in the exposure of personal information. Two or more laptops with donor information and a docking station were stolen.

Information
Source: Databreaches.net

September 24, 2012  City of Tulsa, Oklahoma
Tulsa, Oklahoma

GOV  HACK  Unknown

Those with questions may call (918) 596-2699.

A hacker or hackers managed to infiltrate and bring down the City of Tulsa's website. It is unclear if any information was accessed, but notifications were sent to people who applied online for jobs or submitted online police reports. Names, Social Security numbers, addresses, and driver's license numbers may have been exposed.

UPDATE (10/01/2012): A member or members of the IT department used a third-party firm to test the City's computer system. There was no unauthorized access.

Information
Source: Media

September 23, 2012  Town of Willimantic, Connecticut
Willimantic, Connecticut

GOV  PORT  Unknown

An employee's laptop was stolen from his unattended office between 10 a.m. and noon on September 17. The laptop was password-protected. It contained the information of town employees. Social Security and bank account numbers may have been exposed.

Information
Source: Media

September 21, 2012  Central States Southeast and Southwest Areas Health and Welfare Fund
Des Plaines, Illinois

NGO  PHYS  754 (No SSNs or financial information reported)

An incident occurred on July 31 that may have caused sensitive health information to be exposed. The information was in the form of paper records that were exposed in some undisclosed way.

Information
Source: HHS via PHIPrivacy.net

September 21, 2012  Library Resources, Inc. (LRI)
Philadelphia, Pennsylvania

MED  PORT  3,183 (No SSNs or financial information reported)

Consumers with questions may call LRI’s Quality Management Hotline at 1-888-634-2155 ext. 629.

The August 4th theft of a laptop resulted in the exposure of sensitive information. The laptop contained names, Medicaid numbers, and short summary information used for administrative purposes.

Information
Source: HHS via PHIPrivacy.net

September 21, 2012  Lana Medical Care
Ormond Beach, Florida

MED  PORT  500 (No SSNs or financial information reported)

The August 18th theft of a laptop resulted in the exposure of patient information.

Information
Source: HHS via PHIPrivacy.net

September 21, 2012  Office of Dr. Clark-Neitzel
Olympia, Washington

MED  PORT  942

A July 24 office burglary resulted in the theft of medical bags and a laptop. Affected patients were mailed notification letters on September 7. Patient names, Social Security numbers, addresses, dates of birth, and medical information was exposed.
September 21, 2012  
**Tricounty Behavioral Health Clinic**  
**Acworth, Georgia**  
**MED**  
**PORT**  
4,000 (No SSNs or financial information reported)

Those with questions may call 888-261-6360.

An August 26 office theft of a laptop resulted in the exposure of patient information.

September 20, 2012  
**Transcend Capital**  
**Austin, Texas**  
**BSF**  
**HACK**  
236

A hacker breached a data server located at a Transcend Capital branch during the week of August 20. Client names, Social Security numbers, addresses, account numbers, telephone numbers, email addresses, security positions, and cash positions may have been exposed. Clients were encouraged to change their passwords. A total of 236 clients who are California residents were affected, but the total number of clients affected nationwide was not disclosed.

September 19, 2012  
**United States Navy, Smart Web Move**  
**Washington, District Of Columbia**  
**GOV**  
**HACK**  
200,000 (No SSNs or financial information reported)

A hacker or hackers accessed sensitive information and posted it online. Former and current Navy personnel who used Smart Web Move to arrange household moves could have been affected. The compromised database stored 11 years of private information, but only 20 people had their information publicly posted. Usernames, email addresses, security questions and corresponding answers were exposed.

September 19, 2012  
**Cabinet for Health and Family Services**  
**Frankfort, Kentucky**  
**MED**  
**HACK**  
2,500 (No SSNs or financial information reported)


An employee was the victim of a phishing attack via email sent by a hacker. The employee's account was then compromised. Unauthorized activity was identified on the account within half an hour and the account was immediately disabled.

September 19, 2012  
**Blue Cross Blue Shield of Massachusetts (BCBS)**  
**Boston, Massachusetts**  
**MED**  
**INSD**  
15,000

A BCBS vendor misused BCBS employee information. The misuse appears to have been limited to one instance. Names, Social Security numbers, dates of birth, compensation information, and bank account information may have been exposed.

September 18, 2012  
**Northstar Healthcare**  
**Chicago, Illinois**  
**MED**  
**DISC**  
170 (No SSNs or financial information reported)

An email that was sent to patients displayed the names of all patients who received the email. The email was sent to
An email that was sent to patients displayed the names of all patients who received the email. The email was sent to patients being treated for HIV or AIDS and inadvertently revealed names and HIV status.

Information
Source: PHIPrivacy.net
September 17, 2012
St. Therese Medical Group
Bakersfield, California
MED STAT Unknown

A July 22 Saint Therese office theft of a computer resulted in the exposure of patient information. The computer was unencrypted; however, it was password protected. Names, Social Security numbers, dates of birth, health insurer names, dates of treatment, amount billed, and account balances were exposed. Notifications were sent on September 17.

Information
Source: California Attorney General
September 16, 2012
Quest Diagnostics
Madison, New Jersey
MED INSD Unknown

A dishonest employee was discovered to have forwarded emails that contained sensitive personal information in late July. The emails included names, Social Security numbers, addresses, dates of birth, driver's license numbers, financial account information, and medical/health insurance information.

Information
Source: PHIPrivacy.net
September 16, 2012
Lahey Clinic
Burlington, Massachusetts
MED PORT Unknown

The loss of a physician's unencrypted, password-free Blackberry at an airport on July 1 resulted in the exposure of patient names, dates of birth, medical record numbers, diagnosis information, procedure names, and test results. Lahey Clinic was able to remove all data from the device remotely on July 6. Affected patients were notified in late August.

Information
Source: PHIPrivacy.net
September 16, 2012
Lincoln Financial Securities Corporation, Red Boat Advisor Resources
Concord, New Hampshire
BSF HACK 4,657

A server that held TIFF images of customer financial applications was accessed by an unauthorized party between January and early April of 2012. Customers who applied for brokerage accounts, life insurance and annuities, and provided other financial applications may have had their names, Social Security numbers, addresses, email addresses, government issued identification numbers, and financial account information exposed. Named beneficiaries and other family members may have also had their information exposed.

Information
Source: PHIPrivacy.net
September 14, 2012
Feinstein Institute for Medical Research
Manhasset,
MED PORT 13,000

Those with questions may call 888-591-3911.

A laptop stolen on or around September 2, 2012 contained current and former patient names, Social Security numbers, and other personal information. The laptop was taken from the car of a contractor or employee and may have also contained current and former patient mailing addresses, dates of birth, and medical information. Participants in about 50 different research studies that date back an unknown number of years were affected.

Information
Source: PHIPrivacy.net
September 14, 2012
U.S. Postal Service
Miami, Florida
GOV PHYS Unknown

A man shot and killed a postal worker in December of 2010 in order to steal his master key. The key was then used by the man and his partner to access apartment complex mailboxes in the North Miami-Dade area. An unknown number of people then became victims of tax refund fraud.

The man was found guilty of 14 counts of homicide, carjacking, robbery, possession of a firearm, and aggravated identity theft in September of 2012. He faces a sentence of up to life in prison.

Information
Source: Databreaches.net
September 14, 2012
Wounded Warrior Project
Jacksonville, Florida
NGO PORT Unknown
A July 25 office burglary resulted in the theft of at least 33 laptops and iPads. The personal information of an unspecified number of former employees may have been affected.

**UPDATE (11/28/2012):** The laptops contained employee names, Social Security numbers, addresses, dates of birth, passport numbers, credit card information, bank account numbers, and possibly life insurance dependent information. The IT department remotely locked access to the devices after discovering they had been stolen earlier in the same day.

**Information Source:** Databreaches.net

**September 14, 2012**

**Lucille Hendricks Elementary School**

**McAllen, Texas**

EDU  PHYS  20

A local news team was contacted when a concerned citizen noticed folders with student information in a dumpster. Former student names, Social Security numbers, dates of birth, addresses, and phone numbers were exposed. McAllen School District launched an investigation. The news team held the folders and decided to forward them to the Texas Attorney General’s office.

**Information Source:** Databreaches.net

**September 12, 2012**

**Education Resources Information Center (ERIC)**

**Washington, District Of Columbia**

NGO  DISC  Unknown

An official notice was posted here: http://www.eric.ed.gov/pdf_availability.html

Those wishing to access a specific PDF should email ERICRequests@ed.gov.

ERIC began an effort to remove personally identifiable information from their full text documents in August of 2012. The information had been publicly available through other means, but it was appearing more frequently in internet searches and becoming easier to access because of web advances. Access to many full text documents on ERIC’s database was temporarily disabled. Every document will be checked for personally identifiable information before being restored.

**Information Source:** Databreaches.net

**September 11, 2012**

**WhatGreatSkin.com (Healing Touch Day Spa Inc.)**

**Nipomo, California**

BSR  HACK  Unknown

The WhatGreatSkin.com servers were hit by an organized attack on the afternoon of August 28. Hackers may have accessed customer names, addresses, and credit card details. Customers were warned to be cautious of phishing attempts for Social Security numbers, credit card information, or any other personal information.

**Information Source:** California Attorney General

**September 11, 2012**

**Carmichael Company**

**Vallejo, California**

BSF  PORT  Unknown

Those with questions may call 707-643-1745.

An electronic filing report was found during a raid. The report contained tax return information such as Social Security numbers.

**Information Source:** California Attorney General

**September 11, 2012**

**Local 2/Hospitality Industry Child & Elder Care Plan**

**San Francisco, California**

MED  PORT  Unknown

A USB drive was determined to be lost on August 13, 2012. Information from the non-medical program within the SF Culinary, Bartetenders, and Service Employees Welfare Plan was on the flash drive. People who participated in the Child and Elder Care Plan may have had their names, Social Security numbers, and addresses exposed.

**Information Source:** California Attorney General

**September 11, 2012**

**Northwestern Mutual and One America - American United Life**

**Indianapolis, Indiana**

BSF  INSD  3,000

A former financial planner stole sensitive information from approximately 3,000 clients and used it to open new accounts, make purchases, receive cash advances, and reroute client mail until his arrest in August of 2011. Client names, Social Security numbers, contact information, and financial account information were exposed. He was sentenced to two years
in prison and three years of probation. He will also have to pay $48,488.66 in restitution.

Around 180 people who were arrested between August 27 and September 4 of 2012 had their Social Security numbers exposed by an administrative error. A new software update intended to automatically post regular arrest lists on the department’s Facebook page and distribute them to media outlets also released Social Security numbers of those who were arrested. The error was discovered within 45 minutes, but between 70 and 50 individuals accessed the information during that time.

Two University of Miami Hospital employees were using patient registration sheets to inappropriately access patient information. Anyone who was seen at University of Miami Hospital between October 2010 and July 2012 may have been affected. Patient names, addresses, dates of birth, insurance policy numbers, and reasons for visits were exposed. The last four digits of patients’ Social Security numbers, were exposed in many cases and full Social Security numbers were exposed in some cases. The dishonest employees were terminated immediately and may have sold some of the information to unauthorized parties.

A contractor working for Boston Water and Sewer Commission misplaced a hard drive. The hard drive may have contained customer names, account numbers, meter numbers, phone numbers, addresses, and other information the utility organization recorded. Residents were also warned to be aware of possible calls from people pretending to be from the Commission.

TwinSpires.com computer records were breached on August 3, 2012. Customer names, cryptographically hashed Social Security numbers, dates of birth, and email addresses may have been exposed.

A hacker accessed the company’s banking system and issued separate payments totalling $190,000 to banks in Virginia. It is likely that the hacker placed malware in the system in order to make the withdrawal. The malware has yet to be discovered and it is unclear how long ago the hacker first breached the system.

Hackers associating themselves with Anonymous claim to have obtained 12 million Apple Unique Device Identifiers (UDIDs) by hacking an FBI agent’s laptop. The hackers offered proof of the breach by posting over one million UDIDs. However, both Apple and the FBI are denying that an FBI agent would have access to that information and keep it on a laptop. The hack occurred in March. Apple replaced the types of identifiers the hackers appear to have obtained and will discontinue their use.
A staff member found that a cable line hooked to the computers used by inmates had been connected to a line connecting to the entire Concord prison computer system. This may have allowed one or more prisoners to view, steal, or change sensitive records. The network is used to track invoiced and billing for Correctional Industries contracts. Information from the offender management database system "Corrections Offender Records and Information System" may have been compromised as well.

Information Source: Databreaches.net

Concerned patients may call 888-633-6122.

The July 3 office theft of a computer from the Radiology Department resulted in the exposure of patient information. The computer was used to store CT examination images taken between January 1, 2012 and July 2, 2012. It contained pictures of CT scans performed, reasons for the scans, patient names, ordering doctors' names, and patient hospital account numbers.

Information Source: PHIprivacy.net

The laptop of an employee who works for a BMO Harris Bank vendor was stolen. It contained customer names, addresses, and dates of birth. BMO learned of the breach on June 20.

Information Source: Databreaches.net

The Harris County Hospital District was alerted to an issue when they received a grand jury subpoena on February 11, 2011. A dishonest employee was immediately fired for viewing and possibly sharing patient names, Social Security and member numbers, medical record numbers, addresses, phone numbers, dates of birth, sexes, emergency contact information, payer information, and other medical care information. The Harris County Hospital District decided to send patients notifications on July 20, 2012 after receiving additional information about the breach. The former employee was indicted and will be tried on criminal charges related to the stolen and misused information on September 24, 2012.

Information Source: PHIprivacy.net

A dishonest employee was arrested for using a skimming device to steal customer credit card numbers at Chili's. Investigators were able to link another fraudulent credit card crime to a credit card stored in the dishonest employee's skimmer. This led to the discovery of a credit card making machine, a credit card skimmer, laptops, blank credit cards, and pages of names, Social Security numbers, and dates of birth at a separate residence.

Information Source: Databreaches.net

Documents dating from 1996 to 2007 were found in a recycling bin by a student. Del Mar employee and student names, Social Security numbers, and mailing addresses were exposed. The student reported the discovery immediately and campus officials began an investigation.

Information Source: Databreaches.net
A dishonest employee obtained and misused the personal information of patients during her employment. She pleaded guilty to one count of aggravated identity and will be sentenced in October. She faces between two and 8.75 years in prison for using the credit card information of cancer patients to make fraudulent purchases.

Information Source: PHIPrivacy.net

August 28, 2012 Cancer Care Group
Indianapolis, Indiana

An employee’s computer bag was stolen on July 19. The bag contained a computer server back-up that had patient and employee names, Social Security numbers, dates of birth, insurance information, medical record numbers, limited clinical information, and addresses.

Information Source: PHIPrivacy.net

August 28, 2012 Wilkinson County Schools
Irwinton, Georgia

A student was able to access and distribute information from a classroom management system called PowerTeacher. The student used user names and passwords to access grades, demographics, Social Security numbers, and other personal information. Some parents reported receiving strange calls that disclosed personal information.

Information Source: Databreaches.net

August 28, 2012 Charter One, Dollar Bank, Fifth Third, FirstMerit, Key, PNC, Total Merchant Services
Cleveland, Ohio

Ten people consisting of assistant managers, sales representatives, and other employees of banks were arrested for participating in an identity theft ring. Information was stolen and misused between November 2011 and February 2012.

Information Source: Databreaches.net

August 27, 2012 University of Rhode Island
Kingston, Rhode Island

The University of Rhode Island released a notice on their website here: http://www.uri.edu/datanotice/

Students and faculty who were associated with the University of Rhode Island after April of 2007 may have had their personal information exposed. The information was placed on a server that was not set-up or intended to be used for storing sensitive information. The information was on the College of Business Administration’s computer server and included names, Social Security numbers, dates of birth, hire year, rank, and limited compensation information. The information was discovered to be publicly accessible on July 31. It is unclear how long the information was available, but unauthorized access had occurred sometime while the information was exposed.

Information Source: Databreaches.net

August 24, 2012 Main Street Pharmacy
Corona, California

A doctor was convicted of prescription drug fraud, identity theft, illegal possession of controlled substances, and burglary. She was arrested in January 2009 following a yearlong narcotics investigation and subsequently pleaded guilty to 272 felony counts. The doctor had a drug addiction. She forged the signatures of several doctors and stole the identity of at least 15 patients in order to maintain her drug habit. She was sentenced to a year in jail, five years of probation, completion of a drug rehabilitation program, and completion of 1,000 hours of community service. The dishonest doctor’s license was also permanently revoked.

Information Source: PHIPrivacy.net

August 23, 2012 State Farm Insurance
Bloomington, Illinois

An employee was caught misusing customer information on July 28. The dishonest employee had been improperly using customer names, Social Security numbers, addresses, dates of birth, and credit card numbers for at least two months. An unspecified number of customers had fraudulent online purchases made in their names.

Information Source: California Attorney General

August 23, 2012 John Stewart Company (JSCo)
August 23, 2012  San Francisco, California

A set of internal emails were sent to various JSCo employees on August 7 and August 13. The emails contained the names, Social Security numbers, and in some cases, dates of birth of other employees. Employees were instructed to delete the email upon discovery.

Information Source: California Attorney General

August 22, 2012  South Bend Community School Corporation
South Bend, Indiana

A computer glitch that occurred when the district changed its student management systems caused some employee Social Security numbers to be exposed. The numbers could only be seen by other employees who were being trained on the new computer program. Employees were notified of the breach.

Information Source: Databreaches.net

August 21, 2012  Bellacor.com, Inc.
Mendota Heights, Minnesota

A breach by an unauthorized party was discovered and contained on July 26. The unauthorized party injected malicious code into the Bellacor website on June 7. Temporary files including customer names, addresses, phone numbers, and encrypted credit card information may have been exposed.

Information Source: California Attorney General

August 21, 2012  Colorado State University - Pueblo
Pueblo, Colorado

A few students accidentally gained access to sensitive student files. It is not clear if the files were physical or electronic. The students notified school authorities immediately and the problem was fixed. It is not clear what types of student information were exposed.

Information Source: Databreaches.net

August 20, 2012  U.S. District Court, Los Angeles California
Los Angeles, California

A Los Angeles federal court clerk was identified as the source of leaked confidential information. The clerk was married to a convicted felon who then sold the information from sealed criminal case documents to an identity theft ring. The federal court clerk, her husband, and at least 60 others from the theft ring were caught by an FBI investigation.

Information Source: Databreaches.net

August 17, 2012  University of Texas M.D. Anderson Cancer Center (M.D. Anderson)
Houston, Texas

An unencrypted flash drive was discovered missing. It had last been seen on an employee shuttle bus on July 13. It contained patient names, dates of birth, medical record number, diagnoses and treatment information, and research information.

Information Source: PHIPrivacy.net

August 17, 2012  Wright-Patterson Medical Center
Dayton, Ohio

A notebook containing names and Social Security numbers was misplaced after a blood drive. It was left in a limited-use conference room late in the afternoon and recovered the next morning behind a chair.

Information Source: PHIPrivacy.net

records from this breach used in our total: 0

records from this breach used in our total: 0

records from this breach used in our total: 0

records from this breach used in our total: 0

records from this breach used in our total: 0

records from this breach used in our total: 3,800
August 17, 2012  Discover Financial Services  
Riverwoods, Illinois  
BSF  UNKN  Unknown

An unspecified number of Discover customers had their account numbers changed and were issued a new card. It is unclear what type of security breach prompted the notification and when it may have occurred. Several customers in California received the notification letter; residents of other states may have been notified as well.

Information  
Source: California Attorney General

August 16, 2012  Kindred Healthcare Inc. (Kindred Transitional Care and Rehabilitation)  
 Sellersburg, Indiana  
MED  PHYS  1,504

An office burglary sometime around June 4 resulted in the theft of a safe. The safe held tapes used for backing up Kindred data related to past, present, and prospective patients. Diagnosis information, Social Security numbers, clinical information, bank account and other financial information, addresses, dates of birth, insurance numbers, dates that services were received from Kindred, discharge locations, daily activities, collections letters, and medications received may have been exposed. People admitted between 2009 and 2012 may have been exposed.

Information  
Source: PHIPrivacy.net

August 16, 2012  Office of Dr. Jeffrey Paul Edelstein  
 Chandler, Arizona  
MED  STAT  4,800

Those with questions may call 1-877-615-3743.

Someone who had key access to a building containing a computer server stole the server on May 28. Patient data including names, Social Security numbers, dates of birth, addresses, telephone numbers, account numbers, and diagnoses were on the server. The server contained multiple layers of password protection.

Information  
Source: PHIPrivacy.net

August 14, 2012  First Republic Bank  
San Francisco, California  
BSF  PHYS  Unknown

Sensitive information that may have been in the form of paper records was improperly disposed of on August 2. Client names, account types, account numbers, tax payer identification numbers, and Social Security numbers may have been exposed.

Information  
Source: California Attorney General

August 14, 2012  Creative Croissants  
San Jose, California  
BSR  UNKN  Unknown

A breach at Creative Croissants results in the exposure of customer credit card information. It is unclear how the breach occurred and the date of the breach was March 2, 2012.

Information  
Source: California Attorney General

August 13, 2012  Employee Benefits, Atlanta Police, MARTA Police, Atlanta Fire Department  
Atlanta, Georgia  
GOV  DISC  39

Two representatives of Employee Benefits attempted to gather sensitive information from employees of Atlanta Police, MARTA Police, and Atlanta fire department employees. They visited several locations and offered upgraded insurance and benefits packages through AFLAC insurance. Employee Benefits is a legitimate provider of insurance, but not of AFLAC insurance. The representatives handed out business cards and their supervisor was called when a police lieutenant noticed that the representatives appeared to be frauds. They were arrested and at least 39 information packets that contain sensitive information were recovered. The two representatives face multiple counts of identity theft and racketeering.

Information  
Source: Databreaches.net

August 13, 2012  Apria  
Phoenix, Arizona  
MED  PORT  65,700

An employee’s laptop was stolen from a locked vehicle in June. It contained billing information about Apria patients in California, Arizona, New Mexico, and Nevada. Patient names, Social Security numbers, dates of birth, and other personal or health information may have been exposed.
UPDATE (09/29/2012): The laptop was stolen on June 14 and was password-protected. Current and past patients were affected.

UPDATE (04/03/2013): Billing information for 65,700 patients was stored on the laptop.

Office of Peggy Garland-Coleman
Spartanburg, South Carolina

The owner of a tax preparation business that closed three years ago accidentally discarded several boxes of sensitive records. The records had been picked over before tossed, but sensitive information still ended up in a public dumpster. A concerned citizen found them in a recycling bin in an old supermarket lot. Names, Social Security numbers, dates of birth, and invoices were exposed.

CQ Roll Call, The Economist Group, Bloomberg
Washington, District Of Columbia

A group of former CQ employees were able to continue using log-ins and passwords to access sensitive information from The Economist Group after they left. CQ Roll Call is owned by The Economist Group. Many or all of the former CQ employees accessed the information while employed at Bloomberg. Bloomberg has already paid an unspecified amount to The Economist Group as compensation for the unauthorized access incident or incidents. It is not clear what type of information was exposed.

A dishonest employee faces six charges of fraudulently using a credit card and 59 counts of identity theft. The former employee apparently used customer credit card numbers to pay tuition and insurance bills.

BNSF Railway Company
Fort Worth, Texas

Around 100 BNSF Railway employees in North Dakota and adjacent states have reported fraudulent Paypal accounts and credit cards being opened in their names. It is unclear how long this issue has been occurring, what sensitive employee information may have been accessed, and how the information was accessed.

Blizzard Entertainment
Irvine, California

There is an official Battle.net FAQ page here: http://us.battle.net/support/en/article/important-security-update-faq

Blizzard's security team found an unauthorized party or parties had accessed the Blizzard internal network. Blizzard immediately addressed the security issue and found no evidence that credit card, billing address, or name information had been accessed. Players using North American servers may have had scrambled versions of Battle.net passwords, answers to personal security questions, and information relating to Mobile and Dial-In Authenticators accessed. Users are encouraged to change their passwords immediately and to change the passwords of other accounts if they are similar to the compromised Battle.net passwords. A list of email addresses for global Battle.net users outside of China was also accessed.

UPDATE (11/12/2012): Two people have filed a suit alleging that Blizzard's $6.50 protection charge is inadequate and that Blizzard did not take the necessary measures to secure the private information of customers that was stored online. The lawsuit also alleges that Blizzard continues to fail to disclose to consumers that additional security products must be acquired after buying games in order to ensure that information stored in online accounts is secured.

UPDATE (07/11/2013): The U.S. District Court for the Central District of California dismissed most of the claims that were brought against Blizzard Entertainment.

UPDATE (08/23/2013): At least six out of eight claims from the lawsuit against Blizzard have been dismissed. Blizzard still faces litigation for failing to fully disclose the importance of an authenticator to users.
An employee was fired after an investigation revealed that patient records were accessed without legitimate cause. The breach was discovered during a routine audit.

Information Source: PHIPrivacy.net

Records from this breach used in our total: 102

August 8, 2012 University of Arizona (UA)
Tucson, Arizona

EDU DISC 7,700

Those with questions may call UA's incident contact line at 520-621-4746.

A UA student ran a Google search and found her private information posted publicly. The data belonged to several thousand people who had submitted their names and tax ID numbers to UA in order to receive payments or reimbursements. Vendors, consultants, guest speakers, and UA students had their names and tax ID numbers exposed in February and early March. Some people had their Social Security numbers exposed in lieu of tax ID numbers. The sensitive data was embedded within a larger set of files being transferred to the UA new financial system. The files were thought to only contain public information.

Information Source: Databreaches.net

Records from this breach used in our total: 7,700

August 7, 2012 Nordstrom Bank, Nordstrom fsb
Centennial, Colorado

BSF DISC 2,457

Those who wish to receive a new account number may call 1-800-749-9733.

A total of 2,457 Nordstrom fsb customers in California were affected by a mailing error caused by an administrative error. Cardholder statements, replacement credit cards, or other correspondence were mistakenly sent to addresses other than those of intended cardholders. The issue was discovered on June 7 and was the result of an attempt to reformat addresses to U.S. Postal Service standards. Those who were affected were notified in June and July.

Information Source: California Attorney General

Records from this breach used in our total: 2,457

August 7, 2012 California Correctional Health Care Services (CCHCS) Regional Administration
Fresno, California

MED PHYS Unknown

A June 11 theft of materials inside of a kiosk mailbox located outside of the CCHCS Regional Administration building may have resulted in the exposure of sensitive information. Documents that included prospective employment candidate responses to employment inquiries with personally identifiable information may have been in the mailbox. California State Employment Application forms and applicable documents include names, Social Security numbers, driver's license numbers, residential addresses, dates of birth, telephone numbers, email addresses, employment histories, education histories, and other employment information of prospective candidates.

Information Source: California Attorney General

Records from this breach used in our total: 0

August 6, 2012 Steamboat Ski and Resort Corp.
Steamboat Springs, Colorado

BSO DISC Unknown

A former employee received W-2 information of current and former employees. Names, Social Security numbers, addresses, payroll information, and other W-2 information were accidentally emailed to the former employee. The former employee immediately notified the human resources department and confirmed that the information had not been mishandled.

Information Source: Databreaches.net

Records from this breach used in our total: 0

August 6, 2012 City of Ocoee
Ocoee, Florida

GOV DISC 350

Over 350 city workers had their information posted on a public server in January. An employee inadvertently uploaded the sensitive information to a public domain server as part of an annual audit. Names, Social Security numbers, salaries, and addresses were exposed.

Information Source: Media

Records from this breach used in our total: 350

August 3, 2012 University of Kentucky HealthCare
Lexington, Kentucky

MED PORT 4,490 (No SSNs or financial information reported)
Those with questions may call either 859-323-6044 or 1-877-528-3970 or email privacy@uky.edu.

The May first theft of an employee’s password-protected laptop resulted in the possible exposure of protected health information. Patient medical records, reasons for visits, and dates of visits may have been exposed. A notification was placed on the UKHealthCare website on June 21.

**Information**

**Source:**
- HHS via PHIPrivacy.net

**Records from this breach used in our total:** 0

**Date:** August 3, 2012
- **Office of Dr. Sharon L. Rogers**
  - **Corpus Christi, Texas**

The June 16 theft of a laptop may have resulted in the exposure of protected health information from psychology patients. The incident was reported on the HHS website on July 27, 2012.

**Information**

**Source:**
- HHS via PHIPrivacy.net

**Records from this breach used in our total:** 0

**Date:** August 3, 2012
- **Wolf & Yun**
  - **Elizabethtown, Kentucky**

The April 24 office theft of a laptop resulted in the exposure of patient information. The laptop contained names, dates of birth, and auditory testing data. A public notice was posted on July 20.

**Information**

**Source:**
- HHS via PHIPrivacy.net

**Records from this breach used in our total:** 0

**Date:** August 3, 2012
- **Memorial Healthcare System (MHS)**

MHS discovered a second breach during the process of investigating a dishonest employee’s misuse of patient data in January of 2012. Employees of affiliated physicians’ offices may have improperly accessed patient information through a web portal used by physicians who provide care and treatment at MHS. Patient names, Social security numbers, and dates of birth may have been accessed during the period between January 1, 2011 and July 5, 2012.

**Information**

**Source:**
- HHS via PHIPrivacy.net

**Records from this breach used in our total:** 102,153

**Date:** August 3, 2012
- **Pamlico Medical Equipment, LLC (Now Vidant Internal Medicine)**
  - **Washington, North Carolina**

Those with questions may call 800-678-0697.

A flash drive was lost during transit on or around May 16. Patient names, Social Security numbers, Medicaid numbers, insurance carrier contact information, medical equipment being provided by Pamlico Medical Equipment, service date, price of the equipment rental, and other miscellaneous billing information may have been on the flash drive. The flash drive is believed to have been placed with compacted trash that was transported to a landfill.

**Information**

**Source:**
- HHS via PHIPrivacy.net

**Records from this breach used in our total:** 2,917

**Date:** August 3, 2012
- **The Surgeons of Lake County, LLC**
  - **Libertyville, Illinois**

A hacker or hackers accessed and encrypted the computer server of The Surgeons of Lake County. The incident occurred between June 22 and June 25 and was an attempt to force payment from The Surgeons of Lake County in exchange for the password needed to regain access to the server. The unauthorized user or users had access to names, Social Security numbers, addresses, credit card numbers, and medical information.

**Information**

**Source:**
- HHS via PHIPrivacy.net

**Records from this breach used in our total:** 7,067

**Date:** August 3, 2012
- **Adult and Child Care Center, Choices, Inc., Diversified Support Services**
  - **1945 (No SSNs or financial information reported)**
A hacking incident that occurred on or around May 10 may have exposed the protected health information of patients. The incident was reported by HHS on July 27.

**UPDATE** (08/16/2012): A total of 505 clients and family members of clients of Diversified Support Services and 890 clients and family members of clients of Midtown Mental Health Center were affected. Social Security numbers, private health information, and demographic information were exposed.

**Information Source:**
HHS via PHIprivacy.net

**August 3, 2012**
**Palm Beach County Health Department**
Palm Beach, Florida

Those with questions may call 561-671-4014.

An employee was fired in May for creating and attempting to mail a list of names and Social Security numbers for purposes of identity fraud. It is unclear if the dishonest employee disclosed the information of other people before being caught. Some patients had already experienced fraudulent activity. People who may have been a patient in one of the Health Department Health Centers could have been affected.

**UPDATE** (01/09/2013): The employee worked as a records clerk and was arrested on January 5, 2013. She had worked for Palm Beach County Health Department since 2006 and was charged with several counts of fraud.

**Information Source:**
PHIprivacy.net

**August 3, 2012**
**Stanford University Medical Center, Stanford Hospital and Clinics, Stanford School of Medicine**
Stanford, California

Those with questions may call 855-731-6016.

A burglary sometime around July 15 resulted in the theft of a computer from a Stanford faculty member's locked office. The computer contained patient information. No medical records or health histories were stored on the computer, but it may have held the Social security numbers of some patients. The computer was outfitted with security software that would detect when and where the computer connected to the internet.

**UPDATE** (08/13/2012): The stolen computer was also password-protected. It may have contained medical record numbers, dates of service, and the names of providers and clinics relating to care provided at Stanford Hospital and Clinics or research conducted by the Stanford School of Medicine.

**Information Source:**
PHIprivacy.net

**August 3, 2012**
**General Motors Co.**
Detroit, Michigan

It was determined that an employee who retired in May copied two electronic spreadsheets with names and Social Security numbers of active and retired GM workers. The file was found on the former employee's computer. It is unclear if the information was misused or if the former employee acted with malicious intent.

**Information Source:**
Dataloss DB

**August 2, 2012**
**Environmental Protection Agency**
Washington, District Of Columbia

A computer security breach resulted in the exposure of Social Security numbers, bank routing numbers, and home addresses. A total of 5,100 current employees and 2,700 other individuals had their information exposed by the unspecified computer breach that occurred in March. Notification was sent around the end of July.

**UPDATE** (10/28/2013): An England national was charged in New Jersey with one count of accessing a U.S. department or agency computer without authorization and one count of conspiring to access a U.S. department or agency computer without authorization. He is being investigated for illegally accessing U.S. government computer systems associated with the U.S. Army, U.S. Missile Defense Agency, Environmental Protection Agency, and National Aeronautics and Space Administration.

**Information Source:**
Databreaches.net

**August 1, 2012**
**Office of the Circuit Clerk of Madison County, Illinois**
Edwardsville, Illinois

A hacking incident that occurred on or around May 10 may have exposed the protected health information of patients. The incident was reported by HHS on July 27.

**UPDATE** (08/16/2012): A total of 505 clients and family members of clients of Diversified Support Services and 890 clients and family members of clients of Midtown Mental Health Center were affected. Social Security numbers, private health information, and demographic information were exposed.

**Information Source:**
HHS via PHIprivacy.net

**August 3, 2012**
**Midtown Mental Health Center**
Indianapolis, Indiana

A hacking incident that occurred on or around May 10 may have exposed the protected health information of patients. The incident was reported by HHS on July 27.

**UPDATE** (08/16/2012): A total of 505 clients and family members of clients of Diversified Support Services and 890 clients and family members of clients of Midtown Mental Health Center were affected. Social Security numbers, private health information, and demographic information were exposed.

**Information Source:**
HHS via PHIprivacy.net
Sensitive court documents remained in a recycling dumpster for two weeks because of a missed scheduled pick-up. The court respondent documents included Social Security numbers, dates of birth, addresses, telephone numbers, and detailed accounts of why an order of protection was needed. They were removed upon discovery. Some files were from 2007, though the exact group of people who may have been affected is unclear. The information was from closed cases and could be found in the public record.

Information Source: Databreaches.net

August 1, 2012  Queens College New York, New York EDU HACK 15 (No SSNs or financial information reported)

A hacker or hackers accessed and posted sensitive information online. A total of 15 administrator user names and encrypted passwords were exposed. Three email addresses were also posted.

Information Source: Dataloss DB

August 1, 2012  Tarleton State University Stephenville, Texas EDU PHYS Unknown

Financial aid documents with student information were found scattered in the street. It is unclear how the documents got there. Hundreds of current and former students who applied for or received financial aid during 1997 and 1998 may have had their Social Security numbers, dates of birth, federal Pell grant disbursements, and other personal information exposed.

Information Source: Databreaches.net

August 1, 2012  Marquette University Milwaukee, Wisconsin EDU HACK 15 (No SSNs or financial information reported)

A hacker or hackers accessed and posted sensitive Marquette University information online. Fifteen names, addresses, email addresses, and passwords were exposed.

Information Source: Dataloss DB

July 31, 2012  Massachusetts Mutual Life Insurance Company (MassMutual) Springfield, Massachusetts BSF HACK Unknown

On July 13, MassMutual inadvertently sent a report via secure email that included client information to an incorrect retirement Plan Sponsor. Client names, Social Security numbers, and 401(k) balance information were exposed. The individual who received the plan information informed MassMutual of the error immediately and claimed to have deleted the information without storing or printing it.

Information Source: California Attorney General

July 31, 2012  Oregon Health and Science University Hospital (OHSU) Portland, Oregon MED PORT 14,495 (195 SSNs reported)

OHSU posted an official notice here: http://www.ohsu.edu/xd/about/news_events/news/2012/07-31-ohsu-contacts-p...

The July 4 or 5 burglary of an OHSU employee’s home resulted in the theft of a briefcase, a thumb drive, and several other items. The thumb drive was used to back up data from OHSU computer systems and would normally be locked in a secure location on campus. Pediatric patient information such as name, date of birth, phone number, address, OHSU medical record number, patient medical condition code, or family medical history was exposed. A total of 702 patients had additional information exposed that was more sensitive. The thumb drive also contained a database of OHSU staff information that included names, Social Security numbers, addresses, and employment-related vaccination information of 195 OHSU employees.

Information Source: PHIprivacy.net

July 30, 2012  Hartford Hospital, VNA HealthCare, Greenplum San Mateo, California MED PORT 9,558

The location of the breach is listed as Greenplum’s headquarters.
An employee of Greenplum was robbed of a laptop during a home burglary on or around June 26. Greenplum is a subsidiary of a hospital vendor known as EMC Corp. The laptop contained the information of 7,461 VNA HealthCare patients and 2,097 Hartford Hospital patients. Patients had their names, Social Security numbers, addresses, dates of birth, marital status, Medicaid and Medicare numbers, medical record numbers, and certain diagnosis and treatment information exposed.

**Information Source:**
PHIPrivacy.net

**July 30, 2012**
**Neurocare, Inc.**
**Newton, Massachusetts**
MED HACK Unknown

A malware attack on a Neurocare CPU resulted in unauthorized intrusion into Neurocare's computer systems. The attack compromised Neurocare's credentials for accessing a third party payroll processor. Unauthorized access to Neurocare's payroll system occurred sometime around June 26, but Neurocare's payroll processor immediately noticed the suspicious account activity and addressed the issue. Neurocare was notified and immediately changed system passwords, sent notifications, and began investigations. A total of 19 employees had their personal information accessed, but all Neurocare employees may have been affected.

**Information Source:**
Media

**July 27, 2012**
**Northwestern Memorial Hospital Home Hospice**
**Chicago, Illinois**
MED PORT Unknown

Those with questions may call (855) 755-8480 and use the reference number 6963071312.

A June 11 office burglary resulted in the theft of six laptops and a tablet. One or more of the computer devices included the personal health information of current and former Home Health patients. Information included names, Social Security numbers, addresses, dates of birth, demographics, patient medical treatment profiles, diagnoses, symptoms, medications, treatment notes, and health insurance information. The standard laptop security controls had been temporarily suspended on the devices since they were undergoing a software upgrade.

**Information Source:**
PHIPrivacy.net

**July 27, 2012**
**Upper Valley Medical Center, Data Image**
**Troy, Ohio**
MED UNKN 15,000 (No SSNs or financial information reported)

A data breach of Data Image's online billing system may have exposed the private information of Upper Valley Medical Center patients. Names, addresses, hospital account numbers, and balances owed could have been obtained during an 18-month period. Current and former patients were notified that the breach was discovered on March 21, 2012, but could have occurred as early as October 1, 2010.

**Information Source:**
PHIPrivacy.net

**July 27, 2012**
**Upper Valley Medical Center**
**Troy, Ohio**
MED PORT Unknown

The May 16 office theft of a hard drive resulted in the exposure of patient information. The theft was discovered the next day and a suspect was caught on tape. Upper Valley Medical Center does not believe any patient information was contained on the hard drive.

**Information Source:**
PHIPrivacy.net

**July 26, 2012**
**Petco Animal Supplies, Inc.**
**Chanhassen, Minnesota**
BSR PORT Unknown

Five laptops were stolen from an unnamed auditor of Petco’s 401(k) Plan between May 18 and May 20. The auditor informed Petco on July3. Current and former employee names, Social Security numbers, and other 401(k) account information may have been exposed. Anyone who was issued a Petco paycheck in 2010, had a 401(k) account and received a distribution, or had a fee deducted from their account in 2011 may have been affected.

**Information Source:**
California Attorney General

**July 26, 2012**
**Hillsborough Health Department**
**Tampa, Florida**
GOV INSD 291

An employee printed and removed sensitive client information for unknown purposes. The employee was dismissed and
steps were taken to reduce the risk of similar employee thefts occurring. The employee removed the documents on February 15, 2012 and was not discovered until Hillsborough County Health Department was notified on May 25. Client names, Social Security numbers, dates of birth, phone numbers, patient identification numbers, type of visit, and other protected health information were exposed.

**Information**  
**Source:** PHIPrivacy.net

**July 26, 2012**  
**Natural Provisions Market**  
Williston, Vermont

BSR  HACK  350

Investigators are fairly certain that people who used their credit or debit cards at Natural Provisions Market may be the targets of payment card fraud. Anyone who used a debit or credit card at the store before July 2, and possibly as early as January 2012, should check their bank statements for phony charges. It appears that hackers accessed Natural Provisions’ credit card processors.

**UPDATE (09/11/2013):** The Attorney General of Vermont reached a settlement with Natural Provisions. The store will pay $15,000 to the state and agreed to spend $15,000 to upgrade its computer security system.

**Information**  
**Source:** Databreaches.net

**July 25, 2012**  
**Oregon State University**  
Corvallis, Oregon

EDU  INSD  21,000

An unnamed check printing vendor for the University copied data from the University’s cashier’s office during software upgrades. The information included 30,000 to 40,000 checks that contained student and employee names, University IDs, check numbers, and check amounts. Current and former student, faculty, and staff records older than 2004 may have included Social Security numbers. it does not appear that the vendor acted with malicious intent.

**Information**  
**Source:** Media

**July 24, 2012**  
**Wisconsin Department of Revenue**  
Madison, Wisconsin

GOV  DISC  110,795

An annual sales report contained the Social Security and tax identification numbers of people and businesses who sold property in Wisconsin in 2011. The report was available online between April 5, 2012 and July 23, 2012 and meant for real estate professionals. The report was accessed a total of 138 times before being taken down. Sensitive seller information was in an an embedded file included in an Microsoft Access file which showed sales data. A total of 110,795 sales were made in Wisconsin in 2011, but not everyone who made a sale provided their Social Security or tax identification number for the paperwork.

**Information**  
**Source:** Media

**July 24, 2012**  
**New York University Langone Medical Center, Office of Dr. Eric C. Parker,**  
**Office of Dr. Patrick J. Kelly**  
New York, New York

MED  STAT  8,400 (5,000 SSNs reported)

Those with questions may call (877) 615-3775.

The May 23 office theft of a desktop computer resulted in the exposure of patient information. The computer was password protected and had security software, but was not encrypted. Patient names, addresses, dates of birth, telephone numbers, insurance information, and clinical information may have been exposed. Additionally, approximately 5,000 patients had their Social Security numbers exposed.

**Information**  
**Source:** PHIPrivacy.net

**July 23, 2012**  
**Gamigo**  
Hamburg,

BSR  HACK  3 million American accounts (No SSNs or financial information reported)

Hackers were able to access Gamigo’s server in February of 2012. Notification of the breach was sent on March 1. Gamigo warned users and advised that they change any passwords for emails associated with Gamigo. The hacked information was released on July 6. A total of 8,243,809 user email addresses and encrypted passwords were posted online.

**Information**  
**Source:** Media

**July 23, 2012**  
**Gamigo**  
Hamburg,

BSR  HACK  3 million American accounts (No SSNs or financial information reported)
July 23, 2012  Office of Dr. Luz Colon, DPM Podiatry  Miami, Florida  MED PORT 1,137 (No SSNs or financial information reported)

The theft or loss of a laptop or laptops resulted in the exposure of protected health information. The data breach occurred sometime around March 20, 2012, and was reported on July 3, 2012.

Information Source: HHS via PHIPrivacy.net

July 23, 2012  Independence Physical Therapy  Mystic, Connecticut  MED STAT 925 (No SSNs or financial information reported)

A desktop computer was stolen or discovered stolen on August 1, 2011. It contained protected health information. The incident was disclosed on July 3.

Information Source: HHS via PHIPrivacy.net

July 23, 2012  Titus Regional Medical Center (TRMC)  Mount Pleasant, Texas  MED PORT 500

The official TRMC notice can be found here: http://www.titusregional.com/PublicNotices.htm

The March 28, 2012 loss of a laptop during a routine patient transportation resulted in the exposure of protected health information. It was encrypted and password protected. The laptop was most likely let on the fender of an ambulance and lost during a route. Patient names, Social Security numbers, addresses, and medical data related to services provided by the EMS department may have been on the laptop. Notice of the breach was given on May 24.

Information Source: HHS via PHIPrivacy.net

July 23, 2012  Titus Regional Medical Center (TRMC)  Mount Pleasant, Texas  MED PHYS Unknown

The March 29 theft of an unknown number of x-ray films resulted in the exposure of protected health information. Thieves were able to access the secured storage location that contained the old x-ray films. These thefts usually occur for the purpose of extracting valuable precious metals from the films by destroying them. Most of the information on the films was more than five years old. It is unclear what type of patient information the x-ray films contained, but they did not include Social Security numbers. Notice of the breach was given on May 24.

Information Source: PHIPrivacy.net

July 23, 2012  Lutheran Community Services Northwest  Bremerton, Washington  MED STAT 756 (3,040 people notified)

An office burglary that occurred on or around March 30, 2012 resulted in the theft of several computers and electronic devices. The computers and devices may have contained the names, Social Security numbers, addresses, phone numbers, email addresses, dates of birth, driver’s license numbers, Washington state ID numbers, income or payment information about services, conditions, treatments, or diagnosis information about clients, volunteers, and staff.

Information Source: HHS via PHIPrivacy.net

July 23, 2012  West Dermatology  Redlands, California  MED UNKN 1,900 (No SSNs or financial information reported)

A theft that occurred sometime around April 22, 2012 resulted in the exposure of protected health information. The breach was posted on the HHS website on July 3.

Information Source: HHS via PHIPrivacy.net
An office burglary was discovered on March 26. The theft of lab requisition forms that were kept in a locked cabinet resulted in the exposure of information of patients who received laboratory services between February 1 and March 23. Patient names, addresses, phone numbers, dates of birth, insurance information, ordering practitioner's name, and types of laboratory tests ordered may have been accessed.

Information Source: HHS via PHIPrivacy.net

Envelopes containing BlueCare member protected health information were damaged while being sent to Comprehensive Counseling Network. Lists of claims containing patient protected health information became separated from the envelopes and were lost. Patient names, BlueCare ID numbers, dates of services, procedure codes, claim numbers, totals charged, amounts paid, provider names and provider addresses may have been exposed. The envelopes also contained check to pay for medical visits that were listed on the claims, but the checks were not lost.

Information Source: HHS via PHIPrivacy.net

The May 22 office theft of a physician's laptop resulted in the exposure of patient information. It is unclear what type of information was on the laptop, but the chief information officer said that "nothing that would be used from an identity theft perspective" was on the laptop.

Information Source: PHIPrivacy.net

A customer notified Mission Linen Supply of unauthorized charges on the credit cards of several other customers. Mission Linen Supply discovered that the third party vendor who stores and maintains information for their web stores had a data breach. The unnamed vendor experienced an unauthorized access of their file servers. Customers who made online purchases may have had their credit or debit card numbers, expiration dates, and possibly name and other payment card information compromised. The customer contacted Mission Linen Supply on June 29, but it is unclear when the vendor experienced the data breach.

Information Source: California Attorney General

A hacker or hackers accessed and posted sensitive information online. A total of 1,313 user names and passwords were posted publicly. The account details and name of one administrator were also posted.

Information Source: Dataloss DB

A computer system glitch caused the personal information of public assistance applicants to be sent to random addresses in the department’s system. The error occurred in December, but was not noticed until June. Multiple rounds of forms had been mailed out by that time. A total of 31 forms contained the Social Security numbers, bank account numbers, and other information of 79 household members.

Information Source: Department of Health and Human Services Maine
<table>
<thead>
<tr>
<th>Date</th>
<th>Organization</th>
<th>Location</th>
<th>Sector</th>
<th>Hack Type</th>
<th>Affected Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 19, 2012</td>
<td>Yale University</td>
<td>New Haven, Connecticut</td>
<td>EDU</td>
<td>HACK</td>
<td>1,200 (Unknown number of SSNs)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hackers accessed at least one Yale database and obtained the details of 1,200 students and staff. Hackers may have obtained names, Social Security numbers, addresses, and phone numbers. Additionally, usernames, passwords, and email addresses were published as proof of the hack.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>July 18, 2012</td>
<td>ITWallStreet.com</td>
<td>New York, New York</td>
<td>BSO</td>
<td>HACK</td>
<td>50,000 (No SSNs or financial information reported)</td>
</tr>
<tr>
<td></td>
<td>A hacker may have accessed as many as 12 data files containing detailed information on IT professionals searching for work with Wall Street. First and last names, mailing addresses, email addresses, usernames, hashed passwords, and phone numbers were posted online. Many of the passwords were decrypted and displayed in plain-text. Past salaries, salary expectations, contact information for references, and other types of job search information were also exposed.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>July 17, 2012</td>
<td>Awklein</td>
<td>California</td>
<td>MED</td>
<td>PHYS</td>
<td>2,000 (No SSNs or financial information reported)</td>
</tr>
<tr>
<td></td>
<td>The city where the incident occurred was not reported.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sensitive health information in an unspecified format was stolen or discovered stolen on or around February 1, 2011. The incident was posted on the HHS website on June 8.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>July 17, 2012</td>
<td>Office of Dr. Stephen Haggard, DPM Podiatry</td>
<td>Federal Way, Washington</td>
<td>MED</td>
<td>STAT</td>
<td>1,597 (No SSNs or financial information reported)</td>
</tr>
<tr>
<td></td>
<td>A theft, possibly of a network server, resulted in the exposure of sensitive patient health information. The theft occurred on or around March 4, 2012 and notifications were available for a limited time after April 22. The incident was posted on the HHS website on June 8.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>July 17, 2012</td>
<td>Safe Ride Services, Inc.</td>
<td>Phoenix, Arizona</td>
<td>MED</td>
<td>INSD</td>
<td>42,000 (No SSNs or financial information reported)</td>
</tr>
<tr>
<td></td>
<td>A former employee may have accessed computer systems without authorization and accessed service files. The incident or incidents occurred between August 31, 2011 and January 31, 2012. Employee personal information as well as patient demographic and insurance information were exposed. It is unclear if the former employee was currently employed at the time of the incidents. The incident was posted on the HHS website on June 8.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>July 17, 2012</td>
<td>SHIELDS For Families</td>
<td>Los Angeles, California</td>
<td>MED</td>
<td>STAT</td>
<td>961 (No SSNs or financial information reported)</td>
</tr>
<tr>
<td></td>
<td>records from this breach used in our total: 79</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
A February 27 office burglary resulted in the theft of a computer server. Sensitive client health information such as dates of birth, addresses, treatment plans, and other types of personal information were exposed. The server was not recovered, but the theft was discovered the next morning and a police report was filed. The incident was posted on the HHS website on June 8.

**Information**
**Source:**
HHS via PHIPrivacy.net

**July 17, 2012**  
**Hogan Services Inc.**  
Saint Louis, Missouri  
BSO  
HACK  
1,134 (No SSNS or financial information reported)

An email or emails with sensitive health information related to a health care premium plan was mistakenly emailed to or accessed by unauthorized people. The incident occurred or was discovered sometime around March 30, 2012. The incident was posted on the HHS website on June 8.

**Information**
**Source:**
HHS via PHIPrivacy.net

**July 17, 2012**  
**Ameritas Life Insurance Corp.**  
Lincoln, Nebraska  
MED  
PORT  
3,000

A laptop was stolen or discovered stolen sometime around March 21, 2012. It contained the sensitive health information of 3,000 people. The incident was posted on the HHS website on June 8.

**UPDATE** (08/03/2012): An official notice states that an employee notified Ameritas that their laptop and other items were stolen from their car on March 21. The laptop contained information used to provide group dental and vision quotes, as well as individual member enrollment information for employer-sponsored group health plans. The laptop was password protected but not encrypted. Names, Social Security numbers, addresses, dates of birth, and places of employment may have been exposed.

**Information**
**Source:**
HHS via PHIPrivacy.net

**July 17, 2012**  
**St. Mary Medical Center**  
California  
MED  
PORT  
3,900

A notice can be found [here](http://www.stmarymedicalcenter.org/stellent/groups/public/@xinternet_con_sml/documents/webcontent/smmc-lb-security-breach-2012-0.pdf)

An unencrypted thumb drive was lost on May 7 and discovered missing on May 8. It contained the names, account numbers, diagnoses, dates of admission and discharge, physician’s name, account numbers, and medical record numbers of patients. It is unclear if only one Saint Mary Medical Center in California was affected, and if so, which one. The incident was posted on the HHS website on June 8.

**Information**
**Source:**
HHS via PHIPrivacy.net

**July 17, 2012**  
**Patterson Dental, River Arch Dental, Hamner Square Dental**  
Ontario, California  
MED  
PORT  
3,645

An unencrypted USB memory chip was shipped against company policy. The envelope that contained it arrived at its destination on May 14 with a tear and missing the USB memory chip. Names, home addresses, telephone numbers, email addresses, ID numbers, dates of birth, driver’s license numbers, Social Security numbers, dental information, and dental insurance information of patients was exposed.

**UPDATE** (08/03/2012): A total of 1,112 Hamner Square Dental patients and 2,533 River Arch Dental patients were affected.

**Information**
**Source:**
California Attorney General

**July 17, 2012**  
**Dropbox**  
San Francisco, California  
BSR  
UNKN  
Unknown

Dropbox users began receiving spam from email sources posing as Dropbox. Many users claim that Dropbox must have suffered a breach because email addresses they used specifically and solely for Dropbox were compromised.
UPDATE (07/20/2012): Dropbox investigated customer concerns of a data breach but could not find any evidence of an unauthorized intrusion or activity as of July 20.

UPDATE (07/31/2012): Dropbox has confirmed that some accounts were accessed by hackers. One of the compromised accounts was that of a Dropbox employee. The employee's account contained a project document of user email addresses. Dropbox required some users to change their passwords and increased their security by adding a two-factor authentication system, new automated mechanisms to help identify suspicious activity, and a page that allows users to monitor active logins to their accounts.

Information Source: Media

July 16, 2012 Pulaski Bank, Pulaski Financial Creve Couer, Missouri BSF INSD Unknown

Three former Pulaski employees are accused of accessing and exporting the mortgage data of customers. A former loan officer emailed a large file to an outside email account a month before leaving Pulaski. A former closing supervisor also allegedly transferred documents onto a portable electronic storage device before resigning. The data appears to have been taken to a competitor. Pulaski Financial filed a lawsuit against three former employees and their possible new employer, First State Bank of St. Charles, Missouri.

Information Source: Databreaches.net

July 15, 2012 High Tech Crime Solutions Atlanta, Georgia BSO HACK 32,000 (No SSNs or financial information reported)

A hacker or hackers accessed and posted information from High Tech Crime Solutions Inc.'s website by using an SQL injection cyber attack. A total of 8,900 names and phone numbers were posted online. Over 32,000 private messages were also exposed.

Information Source: Dataloss DB

July 14, 2012 Orcutt Burger Restaurant Orcutt, California BSR CARD Unknown

People who used debit cards to make purchases at Orcutt Burgers may have had their information stolen. Coast Hills Federal Credit Union sent out an alert to clients and reissued an unspecified number of debit cards. It is unclear how the debit card data was accessed and how long the information was at risk. It is also unclear if credit cards were also compromised.

Information Source: Databreaches.net

July 13, 2012 American Express Travel Related Services Company, Inc. (AXP) Los Angeles, California BSF CARD 27,257

A man was arrested in his Los Angeles home for allegedly purchasing and using stolen payment card numbers. The credit and debit card numbers from American Express, Visa, MasterCard, and Discover were in the man's possession between January 11, 2012 and February 26, 2012. The payment card numbers came from hacking the computer systems of a restaurant and a restaurant supply business in the Seattle area. Two people who were associated with the hacking incidents had already been arrested. The man who purchased the payment card numbers is charged with conspiracy to access protected computers to further fraud, to commit access device fraud, and to commit bank fraud; eight counts of bank fraud; six counts of access device fraud; five counts of aggravated identity theft; and two counts of accessing a protected computer without authorization.

UPDATE (07/20/2012): Customer names and payment card expiration dates were also compromised.

Information Source: Databreaches.net

July 13, 2012 New York State Comptroller's Office, New York State Assembly Albany, New York GOV DISC 300

The New York state Comptroller’s Office accidentally released the personal information of over 300 current and former state lawmakers and their staff. The information was intended to fulfill a reporter’s request for per diem payments collected by lawmakers. The information was posted in a spreadsheet online. The Social Security numbers were accessible on hidden pages within the spreadsheet; though they were initially believed to be hidden from public view. The private information was available for less than a day.

Information Source: Media
### Security Breaches

<table>
<thead>
<tr>
<th>Date</th>
<th>Company</th>
<th>Location</th>
<th>Type</th>
<th>Source</th>
<th>Affected Users</th>
<th>Sensitive Info Reported</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 13, 2012</td>
<td><strong>Nvidia</strong></td>
<td>Santa Clara, California</td>
<td>BSR HACK</td>
<td>Media</td>
<td>400,000</td>
<td>No SSNs or financial info reported</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>UPDATE</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>(07/13/2012)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A security breach affected Nvidia's developer forums. Hashed passwords and other sensitive information may have been obtained. Public information such as birthdays, gender, and location may have been exposed. People who used the forums were given temporary passwords and instructed to choose a new forum password.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>UPDATE</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>(07/13/2012)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A Nvidia representative said that its forum has 290,000 registered accounts, its DevZone site has 100,000 accounts, and its research site has 1,200 accounts.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>July 12, 2012</td>
<td><strong>Scripps College Financial Aid Office</strong></td>
<td>Claremont, California</td>
<td>EDU INSD Unknown</td>
<td>Media</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>UPDATE</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>(07/12/2012)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A former employee of Scripps College allowed a personal contact outside of the College to access financial aid application information. The issue was discovered during a review of Scripps College Financial Aid Office processes. It appears that the former employee shared the information to obtain assistance in evaluating applications and preparing potential aid packages. Names, Social Security numbers, dates of birth, and other financial information may have been exposed at various times between 2008 and 2012.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>July 12, 2012</td>
<td><strong>SwedishAmerican Hospital</strong></td>
<td>Rockford, Illinois</td>
<td>MED PHYS Unknown</td>
<td>Media</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>UPDATE</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>(07/12/2012)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Around 1,500 X-ray films were stolen from SwedishAmerican Hospital on May 31. Someone claiming to be the person responsible for picking up and destroying the films was able to steal them. Patient names, medical record numbers, dates of service, and dates of birth were exposed. Representatives believe the risk of identity theft is low since extracting the silver from X-ray films is usually the motive for similar thefts.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>July 12, 2012</td>
<td><strong>Yahoo! Voices</strong></td>
<td>Sunnyvale, California</td>
<td>BSO HACK</td>
<td>Databreaches.net</td>
<td>453,492</td>
<td>No SSNs or financial info reported</td>
</tr>
<tr>
<td></td>
<td><strong>UPDATE</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>(08/02/2012)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A hacker or hackers used an SQL injection technique to access the plain-text passwords of over 450,000 Yahoo! Voices (formerly known as Associated Content) users. The information was then posted online. Yahoo! Voice users are encouraged to change their Yahoo! passwords immediately. Users from as far back as 2006 or earlier may have had their passwords exposed.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>UPDATE</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>(08/02/2012)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A Yahoo! user is suing Yahoo! Inc. for negligence. The user claims that Yahoo!’s failure to adequately safeguard his personal information should result in compensation for himself and other users who experienced account fraud and had to take measures to protect accounts put at risk by the Yahoo! breach.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>July 11, 2012</td>
<td><strong>Formspring</strong></td>
<td>San Francisco, California</td>
<td>BSO HACK</td>
<td>Databreaches.net</td>
<td>420,000</td>
<td>No SSNs or financial info revealed</td>
</tr>
<tr>
<td></td>
<td><strong>UPDATE</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>(07/11/2012)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A hacker or hackers accessed Formspring's development server and posted the password hashes of 420,000 users online. Formspring immediately reset all 28 million user passwords and addressed the security issues upon confirming that a breach had occurred.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>July 10, 2012</td>
<td><strong>Puerta Grande</strong></td>
<td>Winchester, Kentucky</td>
<td>BSR HACK</td>
<td>Databreaches.net</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>UPDATE</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>(07/10/2012)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Customers who used their debit and credit cards at Puerta Grande may have had their payment card information stolen by</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
hackers. Between 50 and 100 people reported fraudulent activity on their payment cards after visiting the restaurant. The restaurant stopped accepting payment cards until a new and secure system could be installed. Only one of the three Puerta Grande restaurants in Winchester were affected.

Information Source: Databreaches.net
July 10, 2012  Phandroid, Androidforums.com
Inverness, Florida

Phandroid user account details were accessed and posted online by a hacker or hackers. Hackers breached a back end database that powers Androidforums.com. Androidforum usernames, email addresses, hashed passwords, member IP addresses, forum group memberships, and other data may have been accessed.

Information Source: Dataloss DB
July 9, 2012  Acronis
Woburn, Massachusetts

A technical error caused a spreadsheet containing an unspecified number of email addresses and upgrade serial numbers to be indexed by search engines. The email addresses from the spreadsheet were not accompanied with any personal information. The spreadsheet was downloaded by 14 different IP addresses and the owners of those IP addresses were contacted.

Information Source: Dataloss DB
July 4, 2012  North Point Dental Care
Winston Salem, North Carolina

The owner of North Point Dental accused a former colleague of stealing the information of about 10,000 current and former patients. The men worked together on a political campaign and the former colleague used the patient information to call patients for campaign support as part of his role as the campaign manager. The former campaign manager countered that he had received an email from the dentist encouraging him to take information from an office computer and use it to call the patients. Patients had their names, email addresses, treatment dates, and home addresses distributed to third parties. The information was also uploaded to an online data storage service.

Information Source: PHIPrivacy.net
July 3, 2012  Miami Northwestern Senior High School
Miami, Florida

A group of volunteers discovered school materials inside of a public dumpster. There were folders containing sensitive student records among textbooks, novels, and workbooks. The folders contained student Social Security numbers, health records, grade reports, and student education forms. An administrative error meant that custodians discarded obsolete materials that had been stored. The items should have been delivered to the district’s central warehouse or sold to used-book dealers. The items were recovered and transmitted to the correct locations.

Information Source: Dataloss DB
July 3, 2012  Olympic College
Bremerton, Washington

Those who experience an incident are encouraged to contact the college's campus security office at 360-475-7800.

Close to 20 Olympic College students and employees notified college personnel that their credit or debit card numbers were used fraudulently. The payment cards had all been used at Olympic College. The reports began in late June and the exact cause of the breach was not identified. Credit card transaction systems were removed from the main merchant network as a precaution.

Information Source: Dataloss DB
July 2, 2012  Restart Behavioral Health Care
Greenville, North Carolina

Sensitive paperwork was left in a publicly accessible dumpster after Restart Behavioral Health Care moved to a new location. Contact information and financial information such as email addresses, phone numbers, names, and check receipts could be found. Social Security card information and Medicaid numbers were also in the dumpster. A local news team contacted the owner of Restart. He refused to comment on the situation, but demanded the return of the documents.
July 2, 2012  
**Dayton VA Medical Center**
**Dayton, Ohio**

Documents with Social Security numbers, dates of birth, and other sensitive information were found in the home of a deceased VA employee in May. The records were found in a box in the attic of the home. It is unclear why the employee took the information home.

---

July 2, 2012  
**University of Texas M.D. Anderson Cancer Center (M.D. Anderson)**
**Houston, Texas**

A laptop with sensitive patient information was stolen from the home of an M.D. Anderson faculty member on April 30. The laptop was not encrypted and contained patient names, medical record numbers, treatment and/or research information, and in some instances Social Security numbers. Notifications were mailed to patients who were affected on June 28.

---

July 2, 2012  
**San Jose State University (SJSU) Associated Students**
**San Jose, California**

A hacker was able to access SJSU’s Associated Students information. Associated Students is a student-run non-profit that manages and hosts many SJSU campus services, but it’s IT infrastructure is separate from SJSU’s. The hacker claimed to have 10,000 student Social Security numbers and driver’s license numbers, but it is unclear if this information was actually exposed. The hacker claimed to use an SQL injection to access the information. In addition to Social Security numbers and driver’s license numbers, information such as administrative materials, job applications, work schedules, email addresses and passwords from the past 10 years may have been accessed. SJSU denies that information this sensitive was accessed.

---

July 2, 2012  
**University of Florida**
**Gainesville, Florida**

The University of Florida maintains a page with their privacy breach incidents [here](http://privacy.ufl.edu/)

The information of former students and applicants was available online. Former students and applicants who signed up for a roommate service online through Levin College of Law in the early 2000s had their Social Security numbers exposed. The breach was discovered in May of 2012; the College of Law stopped using the software for the roommate service in the mid-2000s. Former students and applicants were mailed notifications on June 25.

---

July 2, 2012  
**Chinese Gourmet Express**
**Roseville, Minnesota**

Police are investigating an identity theft and credit and debit card skimming operation involving a Chinese Gourmet Express. A total of $100,000 in losses caused by fraudulent payment card charges had been reported by financial institutions. At least 300 mall employees and shoppers reported fraudulent transactions between March and June.

---

July 2, 2012  
**Wave House**
**San Diego, California**

A former employee allegedly stole hundreds of applications and contracts while employed between May 2010 and January 2012. He is accused of making at least $40,000 in online purchases and pleaded not guilty to 17 counts of identity theft and one count each of grand theft, false personation, and a drug charge. He faces 15 years and eight months in prison if convicted.

**UPDATE (08/08/2012):** The dishonest employee entered a plea of guilty. He faces at least 180 days and up to one year in jail. He is scheduled to be sentenced on September 6.
July 2, 2012  
**Groupon**  
*Chicago, Illinois*

BSR  
DISC  
170 (No SSNs or financial information reported)

An ongoing flaw in Groupon's email link encryption exposes the emails of some Groupon users when specific terms are added into Google searches of Groupon's site. Groupon believes that the problem is caused by users publicly pasting their Groupon deals online. Groupon is working on a solution to exclude the results.

**Information Source:**  
Databreaches.net

---

June 29, 2012  
**University of Southern California (USC)**  
*Los Angeles, California*

EDU  
HACK  
Unknown

A breach in a third-party software system used to process credit card transactions in some USC dining halls, including Ronald Tutor Campus Center, Seeds, the Lab on Figueroa St., and Starbucks on the Health Sciences Campus resulted in the exposure of credit card numbers. The breach of USC Hospitality most likely occurred from May 21 to June 21, but may have occurred earlier. Names and contact information were not associated with the credit card numbers.

**Information Source:**  
California Attorney General

---

June 29, 2012  
**www.ThePartsBin.com**  
*Ord, Nebraska*

BSR  
HACK  
Unknown

The servers of ThePartsBin.com were hacked between April 9 and June 12, 2012. Customer names and credit card information may have been exposed.

**Information Source:**  
California Attorney General

---

June 25, 2012  
**BlueCross Blue Shield of North Carolina**  
*Durham, North Carolina*

MED  
DISC  
100

A mailing software error caused the private information of current and former Blue Cross Blue Shield members to be mailed to other members. The error was discovered on April 12. The records were more than 10 years old and included patient names, Social Security numbers, type of medical care received, and other protected health information.

**Information Source:**  
PHIPrivacy.net

---

June 25, 2012  
**Towards Employment**  
*Cleveland, Ohio*

NGO  
PORT  
26,000

Those with questions may call 216-297-4470 or go to the Towards Employment website: [towardsemployment.org](http://towardsemployment.org)

The May theft of a laptop that contained Towards Employment client data may have exposed personal information. The laptop was password protected and contained the names, Social Security numbers, and addresses of clients. Towards Employment is altering its policy so that only the last four digits of clients’ Social Security numbers are tracked and used.

**Information Source:**  
Media

---

June 24, 2012  
**Commodity Futures Trading Commission (CFTC)**  
*Washington, District Of Columbia*

GOV  
HACK  
700

A CFTC employee received an email on May 21 that linked to a fraudulent website. The employee failed to recognize the email as a phishing attempt and mistakenly entered information on the website. An unauthorized third party was then able to use the employee’s account information to access emails and attachments that contained sensitive employee information such as names and Social Security numbers. The incident was confirmed by the CTC in mid June.

**Information Source:**  
Media

---

June 22, 2012  
**Minnesota Board of Psychology**  
*Minneapolis, Minnesota*

NGO  
INSD  
42

A dishonest employee working as a receptionist for the Minnesota Board of Psychology was part of a fraud ring that included nearly 30 co-conspirators. The receptionist was employed from December 2006 until May 2011. She pled guilty to conspiracy to commit bank fraud and aggravated identity theft and faces six years in prison. Those convicted in the case will be jointly responsible for $358,780 in restitution to victims.
Fifteen people have pleaded guilty and 10 others have pleaded not guilty in the case. The identity fraud ring was able to make at least $2 million in fraudulent purchases and bank withdrawals. The fraud ring used a variety of methods that included dishonest employees and theft of sensitive information from cars, businesses, trash cans, and mailboxes. 

**Information Source:**
Databreaches.net

**June 20, 2012**
**Delta Dental of Illinois**
**Naperville, Illinois**

A box that contained paper claims information and X-rays was lost during shipping between an unnamed subcontractor and Delta Dental of Illinois. The paperwork included enrollees’ dates of birth, Social Security numbers, and other information that dentists provided on their claims.

**Information Source:**
PHIPrivacy.net

**June 20, 2012**
**Gotickets, Inc.**
**Libertyville, Illinois**

Customers who used a payment card on www.gotickets.com may have had their personal and financial information exposed. An investigation revealed that an unauthorized group accessed shipping, billing, and credit card data related to purchases made through the website between May 22 and May 30, 2012.

**UPDATE (11/30/2012):** At least 105 customers in Maryland may have been affected. It is unclear how many people nationwide are at risk. It appears that GoTickets continued to experience online breaches in July. GoTickets updated their online system to increase password security, reduce the number of administrative accounts used, and took additional precautions against future attacks.

**Information Source:**
California Attorney General

**June 19, 2012**
**ECS Tuning Inc.**
**Wadsworth, Ohio**

An unauthorized person or persons accessed customer personal information between May 6 and May 10, 2012. The information was associated with pending and recently shipped orders. Customer names, addresses, email addresses, phone numbers, ECS customer account passwords, and debit and credit card information may have been exposed. Specifically, credit and debit card expiration dates, security codes, or access codes may have been exposed. ECS Tuning integrated PayPal’s Payflow Pro to add additional security to the ECS checkout process and stopped the storing credit and debit cards for any length of time regardless of order status.

**Information Source:**
California Attorney General

**June 16, 2012**
**Bob Wilson Dodge**
**Tampa, Florida**

Vandals broke into a car dealership that had been closed for four years. Sensitive documents were found scattered all over the parking lot. It appears that the primary purpose of the break in was vandalism, but former customers are being warned to check their credit reports for fraudulent activity.

**Information Source:**
Databreaches.net

**June 16, 2012**
**U.S. Department of the Interior National Business Center**
**Denver, Colorado**

A compact disc was discovered missing on or around May 26. It had been sent to the National Business Center in Denver, but may not have arrived. The data on the CD was encrypted and password-protected. Unspecified types of personal information may have been exposed.

**Information Source:**
Media

**June 15, 2012**
**Atkinson & Company LLP Consultants and Certified Public Accountants, The Public Employees Retirement Association (PERA) of New Mexico**
**Albuquerque, New Mexico**

100,000 (No SSNs or financial information reported)
A computer containing PERA information was stolen from Atkinson & Company. The information was related to a PERA annual audit that Atkinson & Company were hired to perform. PERA current and former members, as well as retirees may have had their personal information on a file on the computer.

UPDATE (06/15/2012): Names, addresses, financial institution routing numbers, account types, account numbers, payment amounts, and PERA identification numbers may have been exposed. Family members of current and former PERA members may have also been affected.

Information Source: Dataloss DB

June 13, 2012 Memorial Sloan-Kettering Cancer Center New York, New York MED DISC 880 (Unknown number of SSNs)

Memorial Sloan-Kettering’s statement about the breach is posted on their website and can be found here.

A routine check for sensitive information by Memorial Sloan-Kettering revealed that a PowerPoint presentation that was posted on two medical professional websites in 2006 contained embedded private information. The information included patient names, phone numbers, addresses, and in some cases, Social Security numbers. Anyone who accessed and manipulated the PowerPoint presentation could have viewed the information that was used to create certain graphs. A total of five PowerPoint files contained sensitive information. The largest file had data from 568 patients from various states; the second largest contained 112. Three others contained the data of 37, 59, and 112 individuals.

Information Source: PHIPrivacy.net

June 13, 2012 Gressler Clinic Winter Haven, Florida MED PHYS 1,400

A May 3 office burglary resulted in the theft of sensitive documents. The stolen documents were charge tickets and contained Social Security numbers, addresses, phone numbers, dates of birth, insurance information, and diagnosis and treatment information.

Information Source: PHIPrivacy.net

June 13, 2012 The Tilted Kilt San Antonio, Texas BSR HACK Unknown

A theft ring hacked into the computer system of a Tilted Kilt restaurant. Customers who used a debit or credit card are encouraged to check their bank statements for suspicious activity such as double billing. Fraudulent charges have already appeared on the statements of some customers. It is unclear when the breach occurred, but the Secret Services alerted the pub of the investigation on June 7.

Information Source: Databreaches.net

June 12, 2012 Bethpage Federal Credit Union Bethpage, New York BSF DISC 86,000

An employee accidentally posted data onto a file transfer protocol site that was not secure on May 3. The data contained customer VISA debit card names, addresses, dates of birth, card expiration dates and checking and savings account numbers. The error was discovered on June 3. The data was accessed, but there was no evidence of identity theft or fraud as of June 12. New cards were issued to 25% of the affected members and the remaining members will have their affected cards deactivated on June 30.

Information Source: Databreaches.net

June 11, 2012 University of North Florida (UNF) Jacksonville, Florida EDU HACK 23,246

UNF Housing has set up a webpage to distribute information about the breach. It can be found here.

UNF became aware of a server breach that exposed Social Security numbers and other sensitive information. Students who submitted housing contracts between 1997 and spring 2011 may have had their information exposed. Multiple servers were affected and secured upon discovery. The information may have been accessed as early as spring of 2011.

Information Source: Databreaches.net

June 11, 2012 Eugene School District 4J Eugene, Oregon EDU HACK 16,000

An unauthorized person accessed confidential files that contained current and former students' personal information. Names, Social Security numbers, Dates of birth, student ID numbers, phone numbers, students' free or reduced-price

292
UPDATE (07/12/2012): A minor was arrested for possible involvement in the breach. It appears that the teenager may have obtained the login credentials of an employee and used them to access the computer system. Records for approximately 16,000 current students, as well as free and reduced-price lunch records from 2007 were exposed.

UPDATE (08/25/2012): The student was released from custody and expelled by North Eugene High School. He also posted hundreds of students’ confidential information on a computer account to taunt district officials. He is on house arrest and his attorney entered not guilty pleas.

Information
Source: Databreaches.net
June 9, 2012 Office of Dr. Robert Witham
Port Angeles, Washington
MED STAT Unknown

An April 16 office burglary resulted in the theft of two computers that contained sensitive patient information. Patient names, Social Security numbers, addresses, medical billings, ICD-9 diagnosis codes, and dates of birth were exposed. It is unclear if patients who saw the doctor as far back as 1979 were affected by the breach. Letters to patients who were affected were mailed on June 7.

Investigators were able to arrest an employee of the New York State Office of Children and Family Services after learning about a case of identity theft. The dishonest employee is accused of selling personal information to an outside person and was arraigned on one felony count of receiving a reward for official misconduct in the second degree. He received $500 for accessing and providing the sensitive information of multiple individuals through his workplace.

Information
Source: PHIprivacy.net
June 9, 2012 New York State Office of Children and Family Services
Albany, New York
GOV INSD Unknown

The FTC fined EPN, Inc. for failing to implement reasonable security measures. The agency charged that the company did not have an appropriate information security plan, failed to assess risks to the consumer information it stored, did not adequately train employees, did not use reasonable measures to ensure compliance with its security policies, and did not use reasonable methods to prevent, detect and investigate unauthorized access to personal information on its networks. The FTC claims that this failure to implement reasonable and appropriate data security measures was an unfair act or practice and violated federal law. EPN’s chief operating office installed peer-to-peer file-sharing software on EPN’s computer system and left patient information vulnerable to unauthorized access. Hospital patient Social Security numbers, health insurance numbers, and medical diagnosis codes were accessible on any computer connected to the peer-to-peer network. EPN was barred from misrepresenting the privacy, security, confidentiality, and integrity of personal information they collected. EPN was also required to undergo data security audits and establish and maintain a comprehensive information security program.

Information
Source: Databreaches.net
June 9, 2012 EPN, Inc.
Provo, Utah
BSF DISC 3,800

The FTC fined Franklin’s Budget Car Sales for compromising consumers’ personal information by allowing peer-to-peer software to be installed on its network. Any computers that were connected to the peer-to-peer network could have accessed Franklin’s network of consumer names, Social Security numbers, addresses, dates of birth, and driver’s license numbers. The FTC claimed that Franklin’s failed to assess risks to the consumer information it collected and stored online and failed to adopt policies to prevent or limit unauthorized disclosure of information. Franklin’s also allegedly failed to prevent, detect and investigate unauthorized access to personal information on its networks, failed to adequately train employees and failed to employ reasonable measures to respond to unauthorized access to personal information. Franklin’s settlement agreement bars Franklin’s from misrepresentations about the privacy, security, confidentiality, and integrity of personal information it collected from consumers. Franklin’s must also establish and maintain a comprehensive information security program and undergo data security audits.

Information
Source: Databreaches.net
June 9, 2012 Franklin’s Budget Car Sales, Inc.
Statesboro, Georgia
BSR DISC 95,000

DocuSign user information was discovered to be accessible through a Google search. The information goes as far back as January 2012, and some information could be even older. It is possible to see private emails, signatures, times, dates, locations, addresses, document names, and email addresses. DocuSign claims that the information is available because a small number of DocuSign users have saved their own personal copies of their signed documents to publicly accessible
and searchable locations outside of DocuSign's secure global network.

**Information**

**Source:** Databreaches.net

**June 8, 2012**  
**City of New Haven, Rent Rebate**  
**New Haven, Connecticut**  
**GOV**  
**PORT**  
**Unknown**

The story is available on the official website of New Haven, Connecticut.

The May 23 theft of an employee's laptop resulted in the loss of sensitive information. The laptop was stolen from the Mitchell Branch Library and contained the personal information of people enrolled in New Haven's Rent Rebate program.

**UPDATE** (09/01/2012): Names, Social Security numbers, addresses, dates of birth, and other personal information was exposed. A total of 21,000 Connecticut Rent Rebate program participants were affected.

**Information**

**Source:** Databreaches.net

**June 7, 2012**  
**eHarmony.com**  
**Santa Monica, California**  
**BSO**  
**HACK**  
**Unknown**

An unspecified number of eHarmony users were found to have had their passwords exposed after eHarmony investigated reports of passwords being posted on a hacker site. Those who were affected had their passwords reset.

**Information**

**Source:** Dataloss DB

**June 7, 2012**  
**Wounded Warrior Project**  
**Jacksonville, Florida**  
**NGO**  
**HACK**  
**22 (No SSNs or financial information exposed)**

Hackers accessed and leaked information from the Wounded Warrior Project website. A total of 22 administrator accounts with encrypted passwords and emails were released. The hackers did not release the full database of thousands of users' information out of respect to the U.S. military.

**Information**

**Source:** Databreaches.net

**June 6, 2012**  
**University of Virginia**  
**Charlottesville, Virginia**  
**EDU**  
**DISC**  
**300 (Unknown number of SSNs)**

Between 300 and 350 transcripts from Summer Language Institute applicants were accessible through the University of Virginia website. The human error was discovered when a student searched Google for an image of himself. Students who applied to the University's program within the last two years may have had their names, transcript information, and Social Security numbers exposed. Technology experts at the University blocked public access to the information and asked Google to remove its cache of the sensitive pages on June 5, 2012. It is unclear how long the information was available.

**Information**

**Source:** Databreaches.net

**June 6, 2012**  
**LinkedIn.com**  
**Mountain View, California**  
**BSO**  
**HACK**  
**6,458,020 (No SSNs or financial information)**

A file containing 6,458,020 encrypted passwords was posted online by a group of hackers. It is unclear what other types of information were taken from LinkedIn users. LinkedIn recommends that users change their passwords.

**UPDATE** (08/30/2012): Four potential class actions against LinkedInCorp. were consolidated. The consolidated suits allege that LinkedIn violated its user agreement and privacy policy by failing to properly safeguard digitally stored user data. LinkedIn is also accused of not publicizing the attack in a timely manner.

**UPDATE** (03/06/2013): A lawsuit that was filed in a federal court in San Jose, California in 2012 was dismissed. The lawsuit was based on negligence claims, California consumer protection statutes, and breach of contract. The judge dismissed the lawsuit because the plaintiffs failed to demonstrate that any alleged misrepresentation by LinkedIn was connected to the harm the plaintiffs suffered.

**UPDATE** (06/17/2013): A second class-action lawsuit against LinkedIn is in the making. LinkedIn is accused of failing to use basic encryption techniques to secure personally identifiable information. LinkedIn is trying to stop the second lawsuit from proceeding in federal court because the lead plaintiff has been able to show that she suffered an injury.
On April 2, 2012, an electronic file was discovered on Next Day Flyer's system. The file was storing transaction information for customers who placed orders through the company’s website between March 23, 2012 and April 2, 2012. It was discovered when the company found out that an unauthorized person was trying to disrupt traffic to Next Day Flyer's website. The file was removed, but customer names, credit card information, email addresses, and postal addresses may have been exposed.

A hacker or hackers accessed and posted sensitive information from the Masons of California. Names, addresses, phone numbers, and Social Security numbers were reported. This breach was reported to the Attorney General of California. Records from this breach used in our total: 0

The theft of a binder from an employee's car resulted in the exposure of sensitive patient information. The binder was stolen on or around May 7 and had information from a survey conducted at the Bakersfield Memorial Hospital. Patient names, dates of birth, ages, medications, room numbers, and medical record numbers were exposed.

Charlie Norwood VA Medical Center, Augusta, Georgia

The March 30 theft of a physician’s laptop resulted in the exposure of personal information. The physician had violated VA policy by placing the personal information on his own laptop. Veterans may have had the last four digits of their Social Security number, discharge date, and medical provider name exposed.

Forty-three restaurants nationwide may have been affected by a data breach involving unauthorized access to credit and debit card information. Customers who used credit or debit cards between early March and the end of April may have had their financial information obtained by unauthorized parties.

UPDATE (06/15/2012): Penn Station updated the number of franchise locations affected. They now claim that 80 restaurants in Illinois, Indiana, Kentucky, Michigan, Missouri, North Carolina, Ohio, Pennsylvania, Tennessee, Virginia, and West Virginia were affected by a point-of-sale processing hack.

A hacker or hackers accessed and posted sensitive information from the Masons of California. Names, addresses, phone numbers, and Social Security numbers were reported. This breach was reported to the Attorney General of California. Records from this breach used in our total: 0
numbers, and emails were exposed.

Information Source: Dataloss DB

June 1, 2012 MOAB Training International Kulpsville, Pennsylvania

A hacker or hackers accessed and publicly posted usernames, email addresses, and encrypted passwords from MOAB. Many law enforcement officials and heads of security were among the users who were affected.

Information Source: Dataloss DB

May 31, 2012 Mount Sinai Hospital Miami Beach, Florida

Eleven computer screen printouts of personal information and seven credit cards of Mount Sinai patients were found in a vehicle that was searched after a motorist was stopped for reckless driving. An employee of Mount Sinai was linked to patient personal information that was found during the traffic stop. She was arrested and accused of accessing and printing the names, Social Security numbers, and dates of birth of 340 patients for identity theft purposes.

Information Source: PHIPrivacy.net

May 31, 2012 Paper Street Media, LLC, Florida

A hacker or hackers accessed Paper Street Media data and posted it online. A total of 6,209 user names and passwords were posted. Additionally, 169 emails were posted.

Information Source: Dataloss DB

May 31, 2012 United States Navy Washington, District Of Columbia

A hacker or hackers accessed the database information of the US Navy and posted the information online. The leaked data included 36 email addresses and passwords.

Information Source: Dataloss DB


A hacker or hackers posted member names, email addresses, and contact information online.

Information Source: Dataloss DB

May 30, 2012 American Pharmacist Association (APhA), Pharmacist.com Washington, District Of Columbia

Hackers associated with the group Anonymous posted donations, emails, personal account information, server information, and other information from APhA’s online database. The hackers also claim to have accessed the records of 16,000 patients by hacking the website, but did not post that information. Anonymous claims that the organization was targeted due to its connection to government officials.

UPDATE (6/09/2012): Some names and addresses were also posted. The data posted included information on over 28,000 visitors, donors, and members.

UPDATE (07/18/2012): The website was defaced on May 28. APhA immediately noticed and shut down the website and related computer servers. However, names, addresses, and credit card information (excluding security codes) stored on computer servers may have been accessed between April 23 and May 28.
May 29, 2012  Investacorp, Inc.  Miami, Florida

MML Investors Services LLC, First Rate Investment Systems, and Massachusetts Mutual Life Insurance Company (MassMutual) were affected by the breach.

A vendor of the broker-dealer, National Financial Services (NFS), used by Investacorp was involved in a data security breach. On or around March 12, 2012, Investacorp learned that an NFS vendor had inadvertently shared electronic files with another federally regulated broker-dealer that also uses NFS’s services. The incident occurred on November 29, 2011 and was first noticed on February 13, 2012. The information included client names, Social Security numbers, and certain types of account data. Five Investacorp clients from California may have been affected, but the total number of affected individuals nationwide was not reported. The vendor responsible for the mistake worked with the other broker-dealer to delete the client files from their system. Investacorp then received an executed affidavit from the broker-dealer certifying the destruction of the electronic files.

May 29, 2012  Alaska Structures  Anchorage, Alaska

A hacker or hackers accessed the website database information of Alaska Structures and defaced the website. Some password information was posted online, but it is unclear how many usernames and passwords were obtained and distributed.

May 26, 2012  Direct TV  Greenwood Village, Colorado

A hacker or hackers accessed the server information of Direct TV and posted the information online. The leaked data included administration account information such as 32 email addresses, usernames, encrypted passwords, and a list of IPs that could belong to Direct TV servers.

May 26, 2012  Gridiron Strategies  North Palm Beach, Florida

A hacker or hackers accessed the database information of Gridiron Strategies and posted the information online. The leaked data included 2,109 email addresses and passwords.

May 25, 2012  Phoebe Putney Memorial Hospital  Albany, Georgia

Those with questions may call 1-855-770-0002.

On April 9, 2012, Phoebe Putney Home Health Care (PPMH) learned from law enforcement officials that a former employee had improperly accessed patient information with the intent to file fraudulent tax returns. The dishonest employee may have accessed the names, Social Security numbers, and dates of birth of patients some time between June 2010 and April 2012. Patients who were treated through PPMH between July 2005 and April 2012 may have been affected.

UPDATE (09/03/2013): The dishonest former employee pleaded guilty to embezzlement of government property and aggravated identity theft on August 23, 2012. She was sentenced to 70 months in prison and ordered to pay $110,431 in restitution to the IRS on August 12, 2013.


On April 9, 2012, Phoebe Putney Home Health Care (PPMH) learned from law enforcement officials that a former employee had improperly accessed patient information with the intent to file fraudulent tax returns. The dishonest employee may have accessed the names, Social Security numbers, and dates of birth of patients some time between June 2010 and April 2012. Patients who were treated through PPMH between July 2005 and April 2012 may have been affected.
One of the computers used by the contractor Serco to support the Federal Retirement Thrift Investment Board (FRTIB) was the target of a sophisticated cyber attack. Thrift Savings Plan participants and others who received TSP payments may have had their information exposed. However, there is no evidence that the entire TSP network of 4.5 million participants was breached. A total of 43,587 participants may have had their Social Security numbers, names, and addresses compromised. An additional 80,000 may have had their Social Security numbers and no other information compromised. The attack appears to have occurred in July of 2011 and was discovered through an FBI investigation in April of 2012.

Information
Source: Databreaches.net

May 25, 2012 University of Nebraska, Nebraska Student Information System, Nebraska College System, Lincoln, Nebraska

EDU HACK 654,000

The University of Nebraska set up a webpage for more information on the breach: http://nebraska.edu/security

A University technical staff member discovered a breach on May 23. Staff took steps to limit the breach and there was no clear evidence that any information was downloaded. The Social Security numbers, addresses, grades, transcripts, housing and financial aid information for current and former University of Nebraska students may have been accessed. The database also included the information of people who applied to the University of Nebraska, but may have not been admitted, and alumni information as far back as Spring of 1985. The University of Nebraska was still investigating the extent of the breach as of May 25, 2012.

UPDATE (05/29/2012): The University of Nebraska created a webpage for information about the breach. Close to 21,000 people had bank account information that was linked to the student information system and exposed. The University of Nebraska's computer database also held 654,000 Social Security numbers, though it is unclear if that number completely overlaps the number of individuals who had their bank account information exposed. Current and former students of the University of Nebraska campuses in Lincoln, Omaha, and Kearney were affected; as well as anyone who applied to the University since 1985.

UPDATE (06/01/2012): The Nebraska College System began using a shared student information system called NeSIS in 2009. This resulted in data from Chadron State, Peru State, and Wayne State colleges being exposed.

UPDATE (09/10/2012): Police seized computers and related equipment belonging to a University of Nebraska-Lincoln (UNL) undergraduate student who is believed to be involved in the incident.

UPDATE (12/11/2012): The former UNL student has been charged with intentionally accessing a protected computer system and causing damage of at least $5,000.

UPDATE (06/22/2013): The hacker now faces an additional nine charges of exceeding his authorized access to a computer and two charges of knowingly transmitting a program that damaged computers owned by the University of Nebraska and Nebraska State College Systems.

UPDATE (12/03/2013): The hacker and former UNL student pleaded guilty to one count of intentionally damaging a protected computer and causing loss in excess of $5,000. His sentencing was scheduled for March 21, 2014.

Information
Source: Databreaches.net

May 25, 2012 Duane Reade
New York, New York

BSR INSD Unknown

Employees at two Duane Reade stores were caught participating in a credit card fraud ring. One employee at each store was found to have used an unauthorized device to scan customer credit cards prior to processing them through the store's system. People who made purchases at the stores between October 1, 2011 and February 16, 2012 may have been affected.

Information
Source: Databreaches.net

May 25, 2012 T&M Protection Resources
New York, New York

BSO HACK 10 (No SSNs or financial information reported)

A hacker or hackers accessed the database information of T&M Protection Resources and posted the information online. The leaked data included 10 usernames and passwords.

Information
Source: Databreaches.net

May 24, 2012 Physicians Automated Laboratory
Bakersfield, California

MED PHYS 745 (No SSNs or financial information reported)

An office burglary on or around March 26 resulted in the exposure of patient information. Patient files containing names,
phone numbers, dates of birth, addresses, and lab work were stolen from a laboratory. It is unclear why affected patients were not notified until two months after the incident.

**Information**

**Source:** PHIPrivacy.net  
**Records from this breach used in our total:** 0

**May 24, 2012**  
**University of California Los Angeles (UCLA) Health System**  
**Los Angeles, California**  
**MED DISC Unknown**

The UCLA Health System placed an audit report on billing practices online in May. It was later discovered that an employee had accidentally attached information containing the first name, last name, and five-digit billing code related to at least one patient’s emergency department visit in May of 2011. It is unclear how many people were affected and if others may have had additional information exposed.

**Information**

**Source:** PHIPrivacy.net  
**Records from this breach used in our total:** 0

**May 24, 2012**  
**Altrec, Inc.**  
**Redmond, Oregon**  
**BSR HACK Unknown**

Altrec discovered a potential information security incident involving the American Express credit cards of people who used the site. Customer information may have been compromised between June 2010 and March 2012. The potential breach was discovered on May 7, but a detailed forensic investigation did not uncover any evidence of a security breach. Customer names, addresses, American Express card account numbers, expiration dates, and four digit security codes were stored in Altrec’s database and could have been exposed if anyone had accessed it.

**Information**

**Source:** California Attorney General  
**Records from this breach used in our total:** 0

**May 24, 2012**  
**General Communication Inc. (GCI)**  
**Anchorage, Alaska**  
**BSR INSD 400**

A former customer service representative gathered account information directly from two customers during telephone calls and later attempted to use the information for personal purchases. GCI decided to notify all other customers who may have been contacted by the dishonest former employee and warn them to check their accounts for any unusual activity.

**Information**

**Source:** Databreaches.net  
**Records from this breach used in our total:** 400

**May 24, 2012**  
**Stanford University**  
**Stanford, California**  
**EDU HACK 1,593 (No SSNs or financial information reported)**

A hacker or hackers accessed the database information of Stanford University and posted the information online. The leaked data included a list of contact information for donors. Names, company association, contact details, and notes about the donors were exposed.

**Information**

**Source:** Dataloss DB  
**Records from this breach used in our total:** 0

**May 23, 2012**  
**Boston Children’s Hospital**  
**Buenos Aires,**  
**MED PORT 2,159 (No SSNs or financial information reported)**

A Boston Children’s Hospital employee misplaced an unencrypted laptop during a conference in Buenos Aires. It contained the names, dates of birth, diagnoses, and treatment information of patients were exposed.

**Information**

**Source:** PHIPrivacy.net  
**Records from this breach used in our total:** 0

**May 23, 2012**  
**U.S. Office of Personnel Management**  
**Washington, District Of Columbia**  
**GOV HACK 37 (No SSNs or financial information reported)**

A hacker or hackers accessed the database information of U.S. Office of Personnel Management and posted the information online. The leaked data included 37 user IDs and plain-text passwords on the internet.
An interesting photo caught the attention of a man passing by a trash container. The photo was among other photos, names, phone numbers, and receipts. The records were tracked to Sears Portrait Studio and the man eventually contacted the local media after failing to get a response from the company. Sears responded to media inquiries and claimed that this was an unusual incident that was against company policy.

Information Source: Dataloss DB

May 22, 2012
Glade County Sheriff's Office
Moore Haven, Florida

Hackers accessed sensitive information from the Glade County Sheriff's Department. Ten names with associated email addresses, plain-text passwords, and usernames were posted online. The information of 192 prisoners was also posted, but most of it could already be found through public records. Prisoner names, genders, birth dates, hair and eye colors, heights, weights, last known addresses, and other details were posted.

Information Source: Databreaches.net

May 22, 2012
United States Bureau of Justice Statistics (BJS)
Washington, District Of Columbia

Hackers from Anonymous claim to have leaked 1.7 gigabytes of data belonging to the United States Bureau of Justice Statistics. The United States Bureau of Justice Statistics is part of the U.S. Department of Justice and analyzes data related to crimes in the U.S. The data file was posted on The Pirate Bay. It contained internal emails and the website's entire database.

Information Source: Dataloss DB

May 22, 2012
Eastern Buffet
West Des Moines, Iowa

Victims who reported fraudulent charges on their debit and credit cards were found to have had their payment cards compromised at the Eastern Buffet. The cards were compromised sometime before May 11. Two employees were fired for their roles in the breach and were found to have been working at the restaurant under fake identities.

Information Source: Dataloss DB

May 20, 2012
Comcast
Philadelphia, Pennsylvania

A hacker or hackers posted email addresses, plain-text passwords, and ID numbers online.

Information Source: Dataloss DB

May 20, 2012
www.SD.gov (South Dakota)
Pierre, South Dakota

A hacker or hackers accessed and posted sensitive information from the South Dakota state website online. Usernames, user IDs, plain-text passwords, and email addresses were exposed.

Information Source: Dataloss DB

May 20, 2012
National Endowment for the Arts
Washington, District Of Columbia

A hacker or hackers accessed and posted sensitive information from the National Endowment for the Arts online. Usernames, user IDs, plain-text passwords, and email addresses were exposed.

Information Source: Dataloss DB
A hacker or hackers accessed the database information of National Endowment for the Arts and posted the information online. The leaked data included 13 names, email addresses, and passwords.

**Information**
**Source:** Dataloss DB

**May 19, 2012**
**Massachusetts Eye and Ear**
**Boston, Massachusetts**


An employee was fired after police informed Massachusetts Eye and Ear that the employee was being investigated for identity theft. The employee had taken and misused patient names, Social Security numbers, and dates of birth. At least four of the employee's victims came from Massachusetts Eye and Ear, but she had access to the information of approximately 3,600 patients.

**Information**
**Source:** PHIPrivacy.net

**May 19, 2012**
**Iwacu Online**
**Baltimore, Maryland**

A hacker or hackers accessed and posted sensitive information from Iwacu Online. Usernames, first names, email addresses, and passwords were exposed.

**Information**
**Source:** Dataloss DB

**May 18, 2012**
**Reading Hospital**
**Reading, Pennsylvania**

A Reading Hospital employee made paper copies of sensitive information and used them for training purposes at an unaffiliated educational facility. The incident was discovered the next day and the employee was fired. Patient medical test results, diagnoses, prescribed medications, Social Security numbers, medical histories, and other personal information were exposed.

**Information**
**Source:** PHIPrivacy.net

**May 18, 2012**
**Lady of the Lake Regional Medical Center**
**Baton Rouge, Louisiana**

A laptop went missing from a physician's office sometime between March 16 and March 20 of 2012. The laptop contained patient outcomes data from patients in the adult ICU from 2000 to 2008. Patient names, race, age, dates of admission and discharge from the Intensive Care Unit, and results of treatment may have been exposed.

**Information**
**Source:** PHIPrivacy.net

**May 18, 2012**
**UnitedHealthcare (United Health Group Plan)**
**Minneapolis, Minnesota**

A dishonest employee used the names, Social Security numbers, addresses, phone numbers, dates of birth, and Medicare Health Insurance Claim Numbers to steal the identities of at least 24 Idaho customers enrolled in UnitedHealthcare Medicare plans. On January 30, 2012, it was discovered that the former employee may have accessed the information in the United Health Care database in a way that was inconsistent with his job duties and possibly for fraud purposes. The information was taken between June 28 and December 12 of 2011. Affected patients were notified on March 30.

**Information**
**Source:** PHIPrivacy.net

**May 18, 2012**
**University of Louisiana Monroe (ULM)**
**Monroe, Louisiana**

Anyone who participated in ULM’s Upward Bound program between 2009 and 2012 should check a special ULM website for information on the breach: [www.ulm.edu/breach](http://www.ulm.edu/breach).
A University of Louisiana Monroe employee's email account was hacked. The hacker or hackers could have accessed the sensitive information of people enrolled in the Upward Bound program. A file in the employee's email included the names, addresses, telephone numbers, and other personal information of 83 high school prospects for the Upward Bound program, two former ULM employees who worked within a related program, a current ULM employee working in a related program, and 35 post-secondary ULM students.

Information
Source: Dataloss DB
May 17, 2012
Experian
Costa Mesa, California
BSF UNKN Unknown

An unauthorized user or users was able to access credit reporting information after managing to pass Experian's authentication process. The unauthorized access incidents took place sometime between October 19, 2011 and February 13, 2012, as well as sometime between November 2010 and March 2012. Consumers may have had their names, addresses, and truncated Social Security numbers, years of birth, and account numbers exposed.

Information
Source: Dataloss DB
May 16, 2012
Chrome Crazy
Park City, Kentucky
BSR HACK 219 (No SSNs or financial information reported)

A hacker or hackers accessed and posted sensitive information from Chrome Crazy online. Customer order details, billing and shipping details, types of motorcycles owned, and email addresses were exposed.

Information
Source: Dataloss DB
May 15, 2012
Howard University Hospital
Washington, District Of Columbia
MED INSD 40

A dishonest employee working as a technician in the surgery department at Howard University Health Sciences sold patient information between August 2010 and December of 2011. The employee was charged with one count of wrongful disclosure of individually identifiable health information. Patient names, Medicare numbers, addresses, and dates of birth may have been exposed.

UPDATE (09/24/2012): The dishonest employee was sentenced to 100 hours of community service and three years of probation. The probation term includes six months in a halfway house followed by six months of home confinement. She was also fined $2,100. Her illegal activities involved taking the records of hospital patients, selling their names, addresses, dates of birth, and medical numbers to an unauthorized party, and providing blank hospital prescription forms as well. The dishonest employee was paid between $500 and $800 in cash for each transaction. The information was used for fraudulent oxycodone prescripitions.

Information
Source: PHIPrivacy.net
May 15, 2012
L-3 Communications Corporation
New York, New York
BSO PORT Unknown

A thumb drive containing information from a small number of current employees, former employees, and applicants was discovered to have been misplaced from the workstation of an employee sometime around April 16. The drive contained names and Social Security numbers. Those who were affected were mailed notifications on May 16.

Information
Source: Dataloss DB
May 15, 2012
Sierra County, California
Downieville, California
GOV HACK 15 (No SSNs or financial information reported)

A hacker or hackers accessed the database information of Sierra County and posted the information online. The leaked data included 15 email addresses and passwords; some of the passwords had been decrypted.

Information
Source: Dataloss DB
May 14, 2012
Northwestern Memorial Hospital
Chicago, Illinois
MED INSD 50

A Northwestern Memorial Hospital employee was charged with one count of aggravated identity and one count of identity theft. The dishonest employee is accused of stealing the identities of patients to pay off personal bills. Paperwork with
the Social Security numbers, credit card numbers, and dates of birth of over 50 patients was found in the employee's home. The dishonest employee's scheme was discovered when suspicious credit card activity related to the opening of utilities in the employee's name.

Information
Source: PHIPrivacy.net

May 14, 2012 York County, South Carolina York, South Carolina

Hackers gained access to York County’s web application server. It contained two databases with the information of 17,000 job applicants and vendors. The first database contained about 12,500 names from as far back as 15 years ago. The second database was newer and contained information that had been collected up until August 29, 2011. The intrusion was discovered by the county on August 29 and no new applicants or vendors were affected by the breach. Those who may have been affected were not notified until after a thorough investigation by York County’s IT department. No definitive evidence was found for a breach after the nine-month investigation.

Information
Source: Dataloss DB

May 13, 2012 University of New Mexico Albuquerque, New Mexico

A hacker or hackers accessed and posted sensitive information from the University of New Mexico’s electrical and computer engineering department. Usernames, emails, and encrypted passwords were exposed.

Information
Source: Dataloss DB

May 12, 2012 Warren County Iowa, Iowa Department of Human Services Indianola, Iowa

Warren County residents had their names, Social Security numbers, addresses, phone numbers, and other information exposed. A fire destroyed a Warren County human services office on December 4, 2011. Records from the location that were due to be shredded were moved to a secure facility owned by warren County. A county maintenance worker mistakenly moved a container full of the damaged sensitive records back to the destroyed building in early February of 2012. The mistake was discovered on March 14 when the department received a call from a resident near the area who found a DHS paper in her yard.

Information
Source: Databreaches.net

May 12, 2012 Hewlett, Packard, California Department of Social Services Riverside, California

Around 700,000 caregivers and care recipients had their information lost or stolen during transit between Hewlett Packard and the State Compensation Insurance Fund in Riverside, California. A package that originally contained microfiche with payroll data entries and possibly other sensitive information arrived via U.S. Postal Service damaged and missing thousands of payroll data entries. Names, wages, Social Security numbers, and state identification numbers were exposed. A total of 375,000 In-Home Supportive Services workers were affected and 326,000 recipients of In-Home Supportive Services care were affected.

UPDATE (05/30/2013): A total of 748,902 elderly home care recipients and their caretakers were affected.

Information
Source: Databreaches.net

May 12, 2012 LA Fitness, Fitness 1 Phoenix, Arizona

A concerned citizen found a dumpster overflowing with old gym memberships. Member credit card information, Social Security numbers, addresses, and other information. The information dates back from the late 1990s and early 2000s. Memberships were originally from Fitness 1, but Fitness 1 sold the location to LA Fitness in 2000. The hundreds of sensitive documents appear to have been abandoned by LA Fitness when it vacated the space. A former Fitness 1 attorney took the exposed documents out of the dumpster after the discovery.

Information
Source: Dataloss DB

May 11, 2012 California Department of Justice, Computer and Technology Crime High-Tech Response Team (CATCH) San Diego, California

In November 2011, hackers accessed and released private email accounts belonging to a retired agent for the Department of Justice. The retired agent was a member of the CATCH. Some of the emails that the hackers released included data
of Justice. The retired agent was a member of the CATCH. Some of the emails that the hackers released included data that contained the names, Social Security numbers, addresses, dates of birth, and other personal information of an unknown number of consumers.

<table>
<thead>
<tr>
<th>Information Source:</th>
<th>California Attorney General</th>
<th>records from this breach used in our total: 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 11, 2012</td>
<td>First Data Corporation</td>
<td>BSF DISC 15,399</td>
</tr>
<tr>
<td></td>
<td>Atlanta, Georgia</td>
<td></td>
</tr>
</tbody>
</table>

On April 25, 2012, First Data learned that certain limited personal information about approximately 108,500 merchants who currently process with First Data or who applied for processing services had been shared outside of the company. The names, addresses, and Social Security numbers of merchants who submitted applications to First Data for merchant processing services were purposely disclosed to an outside party in January and February of 2012. First Data later discovered that this action was not clearly permitted in some merchant contracts.

**UPDATE**: (5/29/2012): Bank of America Merchant Services (BAMS), a joint venture between First Data Corporation and Bank of America, was also involved in the breach. The personal information of 15,399 California residents was involved. Of the 15,399 California residents affected, a total of 4,058 residents were merchant customers of BAMS.

<table>
<thead>
<tr>
<th>Information Source:</th>
<th>California Attorney General</th>
<th>records from this breach used in our total: 15,399</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 10, 2012</td>
<td>The Neighborhood Christian Clinic</td>
<td>MED PORT 9,565 (Unknown number of SSNs)</td>
</tr>
<tr>
<td></td>
<td>Phoenix, Arizona</td>
<td></td>
</tr>
</tbody>
</table>

A portable electronic device was lost or discovered missing sometime around February 7, 2012. It contained sensitive information. The incident was reported on the HHS website.

<table>
<thead>
<tr>
<th>Information Source:</th>
<th>Dataloss DB</th>
<th>records from this breach used in our total: 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 10, 2012</td>
<td>Office of Dr. Roy E. Gondo</td>
<td>MED STAT 2,100 (Unknown number of SSNs)</td>
</tr>
<tr>
<td></td>
<td>Yakima, Washington</td>
<td></td>
</tr>
</tbody>
</table>

A desktop computer and electronic medical records were stolen or discovered stolen sometime around February 21, 2012. They contained sensitive information. The incident was reported on the HHS website.

<table>
<thead>
<tr>
<th>Information Source:</th>
<th>Dataloss DB</th>
<th>records from this breach used in our total: 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 9, 2012</td>
<td>Key Bank</td>
<td>BSF INSD 2,937</td>
</tr>
<tr>
<td></td>
<td>Springfield, Oregon</td>
<td></td>
</tr>
</tbody>
</table>

A former manager of the Thurston Branch of Key Bank pled guilty to charges related to opening a Key Bank account in the name of someone else. He will be sentenced for identity theft and bank fraud. The manager obtained and transferred customer names, Social Security numbers, and dates of birth between January and May of 2007. He eventual threatened and intimidated witnesses in August 2010. Key Bank had a total of $44,937.66 in expenses related to the breach.

<table>
<thead>
<tr>
<th>Information Source:</th>
<th>Databreaches.net</th>
<th>records from this breach used in our total: 2,937</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 9, 2012</td>
<td>Capital One Bank</td>
<td>BSF INSD Unknown</td>
</tr>
<tr>
<td></td>
<td>Houston, Texas</td>
<td></td>
</tr>
</tbody>
</table>

A former employee pled guilty to conspiracy to commit bank fraud and aggravated identity theft. The former employee received $3,000 for his role in the conspiracy and his co-conspirators fraudulently made $84,169.37 from customers.

<table>
<thead>
<tr>
<th>Information Source:</th>
<th>Databreaches.net</th>
<th>records from this breach used in our total: 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 9, 2012</td>
<td>Tarpon Springs High School</td>
<td>EDU DISC 400</td>
</tr>
<tr>
<td></td>
<td>Tarpon Springs, Florida</td>
<td></td>
</tr>
</tbody>
</table>

A guidance counselor accidentally sent an attachment with sensitive information to students via email. The email was sent to members of the senior class and the attachment contained the names and student ID numbers of seniors. Student Social Security numbers were used as student ID numbers in most cases.

<table>
<thead>
<tr>
<th>Information Source:</th>
<th>Dataloss DB</th>
<th>records from this breach used in our total: 400</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 9, 2012</td>
<td>InfoLink, ServerPronto, CloudPronto</td>
<td>BSF HACK 1,926 (1,820 encrypted card)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>304</td>
</tr>
</tbody>
</table>
A hacker or hackers accessed the database information of InfoLink and posted the information online. The intrusion appears to have taken place in November of 2011. The leaked data included 46 administrator names, passwords and email addresses. A total of 1,820 client names, email addresses, passwords, payment methods, card types, last four digits of payment cards, and encrypted full payment card numbers were exposed. ServerPronto and CloudPronto affiliates were also affected.

Information Source: Dataloss DB

May 8, 2012

**IntraCare North Hospital**

*Houston, Texas*

A former employee used patient information to file false income tax returns. The information of 741 patients was accessible in a binder. The employee worked as an intake coordinator at the Hospital from March 15 to August 18 of 2011. The breach was not discovered until April 18 of 2012.

Information Source: PHIPrivacy.net

May 7, 2012

**Lake County Sheriff’s Office**

*Tavares, Florida*

Hackers were able to access and publicly post over 16,000 law enforcement files online. Sensitive 911 calls, witness and victim statements, names of young crime victims, names and personal phone numbers of SWAT team members, a blueprint that could allow sex predators to avoid arrest, and possibly sheriff employee passwords were posted. SWAT team information such as the unit’s operating guide and number of snipers was also posted. Personal information including Swat team member home and cell phone numbers was posted as well. The breach occurred sometime around April 28, 2012.

Information Source: Databreaches.net

May 7, 2012

**Demon Thesis**

*San Francisco, California*

A hacker or hackers accessed and posted sensitive information online. Usernames, email addresses, and MD5 passwords were exposed.

Information Source: Dataloss DB

May 7, 2012

**Friendping.com**

*Denver, Colorado*

A hacker or hackers accessed and posted sensitive information from Friendping.com. Passwords and email addresses were exposed.

Information Source: Dataloss DB

May 7, 2012

**Crowne Plaza**

*Columbus, Ohio*

A hotel employee accidentally downloaded malware to front desk computers. The malware was active for about ten days during the first half of March of 2012. Customer names, addresses, credit card numbers, and credit card expiration dates may have been exposed.

Information Source: Dataloss DB

May 5, 2012

**Ford-Motor Websites (Connect With Fiesta, Unleashfiesta)**

*Dearborn, Michigan*

The location listed is that of Ford’s headquarters.

Hackers targeted various websites owned by Ford and posted sensitive information online. Usernames, passwords, and administrator information may have been exposed.
<table>
<thead>
<tr>
<th>Date</th>
<th>Organization</th>
<th>Location</th>
<th>Type</th>
<th>Hack Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 5, 2012</td>
<td>The Complete Pianist</td>
<td>Tucson, Arizona</td>
<td>BSO HACK</td>
<td>16 (No SSNs or financial information reported)</td>
</tr>
<tr>
<td>May 5, 2012</td>
<td>United States Naval Research Laboratory</td>
<td>Washington, District Of Columbia</td>
<td>GOV HACK</td>
<td>30 (No SSNs or financial information reported)</td>
</tr>
<tr>
<td>May 4, 2012</td>
<td>Booker T. Washington High School</td>
<td>Atlanta, Georgia</td>
<td>EDU HACK</td>
<td>Unknown (18 students requested that their grade be altered)</td>
</tr>
<tr>
<td>May 4, 2012</td>
<td>Boca Ski Club</td>
<td>Palm Beach, Florida</td>
<td>BSR HACK</td>
<td>39 (No SSNs or financial information reported)</td>
</tr>
<tr>
<td>May 4, 2012</td>
<td>Emerson (Funai Corporation)</td>
<td>Torrance, California</td>
<td>BSR HACK</td>
<td>18 (No SSNs or financial information reported)</td>
</tr>
<tr>
<td>May 3, 2012</td>
<td>University of Pittsburgh</td>
<td>Pittsburgh, Pennsylvania</td>
<td>EDU HACK</td>
<td>Unknown</td>
</tr>
</tbody>
</table>
UPDATE (08/28/2012): Two men were arrested for allegedly participating in a hack of University of Pittsburgh. One entered a plea of not guilty.

Information Source: Databreaches.net

May 3, 2012  
Glenn Research Center - National Aeronautics and Space Administration (NASA)  
Cleveland, Ohio

Hackers managed to obtain staff details from Glenn Research Center. Home addresses and telephone numbers of more than 700 US government staff were stolen and published online. Most of the uploaded data was unclassified material such as expense forms and details on flight missions by the US Civil Air Patrol.

Information Source: Databreaches.net

May 2, 2012  
Rackspace, Incorporating Services, Ltd.  
Dover, Delaware

On April 2, 2012, Incorporating Services learned that one of their servers was compromised by a malware attack. Incorporating Services began investigating the breach after being informed by their internet hosting vendor and discovered that malicious software had allowed an unauthorized party to access data stored on the server. Corporate officer Social Security numbers and names may have been exposed.

UPDATE (6/06/2012): Rackspace has been identified as the internet hosting vendor. Social Security numbers, credit card payment information such as expiration date and CVV, and possibly Automatic Clearing House (ACH) payment information were compromised.

Information Source: California Attorney General

May 2, 2012  
Florida Department of Children and Families  
Tallahassee, Florida

The information of Florida child care workers was placed on a state website. The information was not password protected and could have been found through an internet search. An unnamed vendor working for the state of Florida was responsible for placing the information online. Florida daycare workers may have had their dates of birth, names, and Social Security numbers exposed. It is not clear how long the information was exposed.

Information Source: Databreaches.net

May 2, 2012  
Valencia Self Storage  
Valencia, California

Two people were charged with stealing more than $16,000 from 20 businesses and individuals in the Santa Clarita Valley area. The man and woman were able to commit identity theft and run a check counterfeiting operation by retrieving and reassembling shredded checks from the trash bin of Valencia Self Storage. Hundreds of bank account numbers, fake and stolen IDs and identity profiles, check making equipment, and counterfeiting checks were discovered at their residence. A criminal complaint was filed on April 18 alleging felony counts of identity theft, check forgery, commercial burglary, grand theft, false impersonation, receiving stolen property, and unauthorized credit card use.

Information Source: Dataloss DB

May 2, 2012  
Bimbo Bakeries  
Horsham, Pennsylvania

A total of 22 people from New Hampshire were affected. It is unclear how many people were affected nationwide.

The theft of a laptop from the trunk of an employee’s car resulted in the exposure of sensitive information. Current and former associates may have had their names and Social Security numbers on the stolen laptop.

Information Source: Dataloss DB

April 30, 2012  
Volunteer State Community College  
Gallatin, Tennessee

Those with questions may call (615) 230-3390.

The University became aware of an unintended disclosure. Files with the information of current and former faculty and
former students were placed on a web server that was not secure. The information could have been accessed anytime between 2008 and the discovery of the error. Names and Social Security numbers were exposed.

Information Source: Databreaches.net

April 30, 2012  Accurate Accounting  Hesperia, California

A member of law enforcement found a black canvas bag full of payroll files. The bag may have been stolen or misplaced and carried worker names, Social Security numbers, and other personnel information related to taxes. Stacks of files were photographed behind Accurate Accounting. This led to the belief that the files had not been properly stored.

Information Source: Databreaches.net

April 30, 2012  Columbia University  New York, New York

A programmer erroneously saved an internal test file onto a public server in January 2010. Current and former employees had their names, Social Security numbers, addresses, and bank account numbers available on the internet from January 2010 until April of 2012. A total of 3,000 current and former employees were affected, but an additional 500 sole proprietors were also affected. It appears that the file was not accessed at anytime between January 2010 and March 10, 2012.

Information Source: Dataloss DB

April 28, 2012  TwoPlusTwo.com  Henderson, Nevada

A hacker accessed passwords and associated email addresses of users of Two Plus Two Forums. It is unclear what types of data and how much were accessed. Anyone who used the same email and password combination for Two Plus Two Forums and other sites should change their password for Two Plus Two Forums as well as the other sites.

Information Source: Dataloss DB

April 28, 2012  Taco Bell, McDonald’s, Wrigley Field, Ralph Lauren Restaurant (RL Restaurant)  Chicago, Illinois

Six defendants face criminal charges for their roles in a fraud ring that utilized skimming devices in the Chicago area. Some of the defendants were dishonest employees who used a skimming device to read and record customer information as customers made purchases. Others recruited these dishonest employees and some used the card information to make fake cards and fraudulent purchases.

Information Source: Dataloss DB

April 27, 2012  Office of the Texas Attorney General  Austin, Texas

Lawyers responsible for challenging a voter ID law in Texas requested the Texas voter database for analysis. The Texas Attorney General’s office released encrypted discs with the personal records of 13 million Texas voters, but half still contained Social Security numbers. A state police officer was dispatched to New York, Washington D.C., and Boston to retrieve the encrypted discs when the opposing lawyers revealed that a mistake had occurred.

Information Source: Media

April 27, 2012  Minnesota Department of Public Safety Driver and Vehicle Services  St. Paul, Minnesota

An internal audit revealed that an employee at an unnamed Minnesota car dealership allowed an unauthorized friend to use his login information. The login information provided access to a vehicle database for processing consumer sales. Consumer vehicle identification numbers, names, addresses, and dates of birth may have been exposed. The employee’s friend worked at a vehicle repossession company and may have allowed additional individuals to use the login credentials. The employee who revealed his login information may face criminal charges.

Information Source: Dataloss DB
Hackers were able to access the user names and passwords located on the Three Rivers Park District database. Anyone who has ever made a reservation or registered for a program associated with one of the district’s 21 parks was affected. No financial information, names, or addresses was exposed. The breach was discovered on April 19 and immediately addressed.

Information Source: Dataloss DB

An unknown number of customers had their personal information entered into the wrong field in a database. The information should have been encrypted but was not because of the error. Customers may have received mail with their credit card number, driver’s license number, Social Security number, passport number, or any combination of these elements printed on the outside of envelopes. The issue was discovered in late December of 2011.

Information Source: California Attorney General

An April 19 car burglary resulted in the exposure of student information. An external hard drive containing letters associated with students who applied to the North East School of the Arts was stolen from a teacher’s car. The letters contained applicant names, Social Security numbers, dates of birth, home addresses, phone numbers, and previous school district information.

Information Source: Dataloss DB

A CD-ROM disk with IRS W-2 information for Claire’s employees was discovered missing from a designated human resources-only area. Claire employee Social Security numbers, 2011 salary, and other W-2 information were on the disk. A total of 150 New Hampshire residents were notified of the breach, but the total number of affected individuals nationwide was not revealed.

Information Source: Dataloss DB

An April 1, 2012 office burglary resulted in the theft of computer equipment with sensitive information. A server that contained customer names and Social Security numbers or driver’s license numbers was stolen. Additional information related to customer applications was also on the server.

Information Source: California Attorney General

Cryptic Studios detected evidence of unauthorized access to a user database that occurred in December 2010. Users may have had their account names, handles, encrypted versions of their passwords, dates of birth, email addresses, billing addresses, and partial credit card numbers exposed. Some of the passwords that were exposed were decrypted. Cryptic Studios reset all customer passwords that could have been affected after discovering the breach by performing security analysis. Anyone who uses the same password and email combination for other accounts is encouraged to change their password for those accounts as well.

Information Source: Databreaches.net

Former students with questions may call 1-855-822-8510 or email info-help@uab.edu.

People who were undergraduate students at UAB between 1995 and 2006 may have had their information accessed online.
The information included Social Security numbers and academic records. It was accidentally made available on a publicly accessible server for an unspecified amount of time. The breach was discovered on March 27.

Information Source: Dataloss DB

- **April 24, 2012** Oregon State Hospital, Oregon
  - **MED** **PHYS**
  - 550 (No SSNs or financial information reported)

The city where the breach took place was not reported.

The theft of sensitive documents from an Oregon State Hospital supervisor’s car resulted in the exposure of patient information. On Friday, April 13, a printed list of 550 hospital patients that included names, treating physicians, hospital identification numbers, and geographic information was stolen. Additionally, progress notes for 20 patients were stolen that included patient dates of birth, diagnoses, and other information. It is not clear if patients who visited either the Salem Oregon State Hospital or the Portland Oregon State Hospital were affected by the breach.

Information Source: PHIPrivacy.net

- **April 24, 2012** University of Houston College of Optometry Clinic, La Nueva Casa de Amigos Eye Clinic
  - **MED** **HACK**
  - 7,000 (No SSNs or financial information reported)

Those with questions may call (855) 834-1606.

The University of Houston College of Optometry became aware that one of their computers was infected with a virus on February 23, 2012. The person responsible for the breach may have been able to access the information for 24 hours. Patient records dating between January 2006 and February 13, 2012 could be accessed from the computer. Patient names, phone numbers, addresses, dates of birth, insurance information, future appointments, current medications, diagnoses, treatment information, vision test results, vision history information, letters from referring doctors, costs of medical services or goods, method of payment, occupation/job, gender, and languages spoken were in the patient records.

Information Source: PHIPrivacy.net

- **April 24, 2012** Sheppard Air Force Base
  - **MED** **PHYS**
  - 721

I man found medical records stacked in a bag in a closet while checking for financial records in the home of his estranged wife. The records date from 2003 to 2007 and involve the information of patients of Sheppard Air Force Base’s 82nd Medical Group. Names, Social Security numbers, addresses, phone numbers, and in some cases, patient diagnoses were on the documents.

Information Source: PHIPrivacy.net

- **April 23, 2012** Office of Dr. Gloria Traje-Quitoriano
  - **MED** **PORT**
  - Unknown

A physician’s laptop was stolen from her husband’s car. The laptop contained patient names, Social Security numbers, dates of birth, phone numbers, and addresses. The laptop was not encrypted.

Information Source: PHIPrivacy.net

- **April 23, 2012** Saint Mary’s Hospital, Naugatuck Valley Community College
  - **MED** **DISC**
  - Unknown

A Naugatuck Valley Community College instructor used patient X-rays from St. Mary’s Hospital to teach radiology technology. The instructor obtained the X-rays by using his Saint Mary’s employee login to access medical records. The X-rays were used without permission and contained patient names, dates of birth, and physician notes. The instructor told students not to disclose the practice.

Information Source: PHIPrivacy.net

- **April 23, 2012** Fl1-racers.net
  - **BSR** **HACK**
  - 72 (No SSNs or financial information reported)
Hackers launched an attack against the Formula One website in response to a decision to stage the Grand Prix in Bahrain. In addition to a denial of service attack on the official website, government websites were also attacked. The hackers managed to access a database with the names, passport numbers, email addresses, and home addresses of people who purchased tickets for the Grand Prix. The information the hackers posted was altered to protect privacy.

Information Source: Dataloss DB

April 20, 2012
University of Arkansas for Medical Sciences (UAMS)
Little Rock, Arkansas

MED DISC
7,000 (No SSNs or financial information reported)

A UAMS physician sent financial data to an individual who was not a member of UAMS’s workforce in February of 2012. Patient identifiers had not been removed from the data and UAMS learned of the error on April 6. Patients of interventional radiology seen at UAMS between 2009 and 2011 had their names, UAMS account numbers, dates of service, interventional radiology procedures, diagnosis codes, charges, and payments exposed.

Information Source: PHIPrivacy.net

April 20, 2012
Office of Dr. Rex Smith
Eugene, Oregon

MED STAT
20,915

An office burglary that occurred on or around February 19 resulted in the theft of medications and a computer. The computer contained patient names, Social Security numbers, and dates of birth. It is unclear if the computer was encrypted. The total number of patients affected and all types of information exposed are also unclear.

Information Source: PHIPrivacy.net

April 20, 2012
Under Armour Inc., PricewaterhouseCoopers
Baltimore, Maryland

BSR PORT
Unknown

The location listed is that of Under Armour’s headquarters.

A flash drive that contained Under Armour employee payroll information was lost by PricewaterhouseCoopers. The information was being transmitted via mail for auditing purposes and went missing on or around April 12. Employee names, Social Security numbers, and salary information could have been exposed. It is unclear how many people were affected in the U.S. Under Armour employs 5,400 people worldwide.

Information Source: Dataloss DB

April 20, 2012
Desert AIDS Project (D.A.P.)
Palm Springs, California

NGO PORT
4,400 (No SSNs or financial information reported)

An April 12, 2012 office burglary resulted in the theft of a laptop with sensitive information. The computer assigned to the receptionist was stolen and contained a spreadsheet with client name, client status (active, discharged, etc.), internal client identification number, date of birth, and assigned staff person. However the document was not labeled as a D.A.P. document. If someone saw the spreadsheet by itself they would not know it was linked to D.A.P.

UPDATE (05/30/2013): Approximately 4,400 patients were affected.

Information Source: California Attorney General

April 20, 2012
Indie Research LLC, BullMarket.com
Princeton, New Jersey

BSF HACK
Unknown

Those with questions may call 1-888-278-5515.

An unauthorized person or persons was able to access electronically-stored information relevant to BullMarket.com. User names, credit card information, billing addresses, email addresses, and/or login information were compromised. The breach occurred sometime between April 3 and April 7, 2012 and was discovered on April 11. Information as recent as June 2005 may have been exposed, but users with recent information appear to have not been affected.

Information Source: California Attorney General

April 20, 2012
Indie Research LLC, BullMarket.com
Princeton, New Jersey

BSF HACK
Unknown

Those with questions may call 1-888-278-5515.
April 19, 2012  South Carolina Health and Human Services, South Carolina Medicaid  
Columbia, South Carolina  
MED INSD 228,435  
(Unknown number of SSNs involved)

Those with questions may call 888-829-6561 or visit www.myscmedicaid.org.

An employee was fired and arrested after he sent the names, addresses, phone numbers, and dates of birth of Medicaid patients to his private email. It was discovered that he had compiled and emailed the information of South Carolina Medicaid patients over a period of several months. He was charged with five misdemeanor counts of violating the confidentiality of medical indigents and one count of disclosing confidential information. At least 22,600 patients had their Medicaid ID numbers emailed. It is unclear how many of those patients had their Social Security number used in place of a Medicaid ID number. Patients were warned not to give any personal information to anyone contacting them and claiming to be from the Medicaid agency.

UPDATE (02/20/2013): A dishonest employee and another individual have been charged with criminal conspiracy. The employee was also charged with willful examination of private records by a public official, public member, or public employee.

UPDATE (10/09/2013): The former employee pleaded guilty to four counts of willfull examination of private records by a public employee and one count of criminal conspiracy. The dishonest former employee faces up to 25 years in prison.

Information Source: PHIPrivacy.net  
records from this breach used in our total: 0

April 19, 2012  Cigna Dental  
Bloomfield, Connecticut  
MED INSD Unknown

On March 23, 2012, an employee sent an unencrypted document to the personal emails of herself and her son. The document contained the first names of customers and their Social security numbers. Cigna became aware of the incident on March 27 and took immediate action. The employee claimed that she had sent the document to obtain help with work from her son. She confirmed that both she and her son had deleted the email and was fired.

Information Source: California Attorney General  
records from this breach used in our total: 0

April 19, 2012  The Commercial Bank  
Meridian, Mississippi  
BSF INSD Unknown

A former bank vice president and branch manager was sentenced for falsifying loans. She used the names, Social Security numbers, and other personal information of family members and bank customers to falsify financial documents between June of 2008 and May of 2009. The woman’s fraudulent activities were discovered in 2009 and she eventually pled guilty on February 3, 2012. Her charges included mail fraud, wire fraud, bank fraud, and aggravated identity theft. The dishonest employee was sentenced to 51 months in federal prison, three years of supervised release, and ordered to pay $237,657.88 in restitution.

Information Source: Dataloss DB  
records from this breach used in our total: 0

April 18, 2012  Emory Healthcare, Emory University Hospital  
Atlanta, Georgia  
MED PORT 315,000  
(228,000 SSNs reported)

Patients with questions may call the Emory Healthcare Support Center hotline at 1-855-205-6950.

Emory Healthcare revealed that 10 backup discs that contained patient information are missing from a storage location at Emory University Hospital. The discs were determined to have been removed sometime between February 7, 2012, and February 20, 2012. The patient information was related to surgery and included names, Social Security numbers, diagnoses, dates of surgery, procedure codes or the name of the surgical procedures, surgeon names, anesthesiologist names, device implant information, and other protected health information. Patients treated at Emory University Hospital, Emory University Hospital Midtown (formerly known as Emory Crawford Long Hospital) and Emory Clinic Ambulatory Surgery Center between September of 1990 and April of 2007 were affected.

UPDATE (6/09/2012): A suit seeking class action status was filed on June 4. The suit seeks unspecified damages over the loss of 10 computer disks containing the personal and health information of between 250,000 and 315,000 patients treated between 1999 and 2007.

Information Source: PHIPrivacy.net  
records from this breach used in our total: 228,000

April 18, 2012  California State University San Marcos  
San Marcos, California  
EDU HACK 700 (No SSNs or financial information reported)
A candidate for student body president was accused of tampering with University computers in order to access student ID numbers and passwords. The information could have been used to alter election results. The University isolated and monitored the compromised accounts and rescheduled the election. The student was arrested in March on suspicion of election fraud, identity theft, and unlawful access to a computer. The student was released and no charges were filed.

**UPDATE** (04/20/2012): The student was first arrested after allegedly being caught with a password stealing device at a campus computer.

**UPDATE** (03/22/2013): The student pleaded guilty to wire fraud, access device fraud, and unauthorized use of a computer. He faces between 27 and 33 months in federal custody.

**UPDATE** (08/06/2013): The former student received a one-year sentence and is scheduled for a restitution hearing on August 12.

Information Source: Dataloss DB

---

**April 18, 2012**

**Knoxville Medical Clinic, DRD Management**  
**Knoxville, Tennessee**

MED PHYS 1,000 (No SSNs or financial information reported)

A former employee took paper documents with patient information without permission. It is unclear if the former employee meant to use the information for fraud purposes. Patient names, dates of clinic visits, dates for scheduled opiate addiction dosages, and the dosage amounts were in the paper documents. The documents were recovered.

Information Source: Dataloss DB

---

**April 17, 2012**

**Phoenix Cardiac Surgery, P.C.**  
**Phoenix, Arizona**

MED DISC Unknown

Patients in Prescott, Arizona may have also been affected.

Phoenix Cardiac Surgery inadvertently posted the clinical and surgical appointments of patients on an Internet-based calendar that was publicly accessible. The error went unnoticed for an unspecified amount of time. The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) investigated the error and determined that Phoenix Cardiac Surgery had a number of Health Insurance Portability and Accountability Act (HIPAA) violations. Phoenix Cardiac Surgery agreed to pay HHS a settlement totalling $100,000 and to comply with HIPAA. The resolution agreement can be found here.

Information Source: PHIPrivacy.net

---

**April 17, 2012**

**Virginia Military Institute**  
**Lexington, Virginia**

EDU DISC 258 (No SSNs or financial information reported)

A Virginia Military Institute (VMI) administrator emailed a spreadsheet with the grade point average of every member of VMI's senior class to the VMI student president. The email should have only contained an attachment with the names and hometowns of potential 2012 graduates. The second attachment was not only emailed to the student president, but was then forwarded to 258 senior students before the student president and VMI administration realized the mistake.

Information Source: Dataloss DB

---

**April 17, 2012**

**Ruby's Diner**  
**Glen Mills, Pennsylvania**

BSR HACK Unknown

Someone managed to install malware on a Ruby's computer system. Customer credit and debit card information was obtained and used to make fraudulent purchases across the United States and internationally. The breach may have occurred as early as December 2011.

Information Source: Dataloss DB

---

**April 17, 2012**

**Office of Dr. William F. DeLuca Jr.**  
**Latham, New York**

MED PORT 577 (No SSNs or financial information reported)

The theft of a laptop on or around January 16, 2012 resulted in the exposure of patient protected health information. The incident was reported in the HHS website.
April 17, 2012  
Catalyst Health Solutions, Alliant Health Plans, Inc.  
Calhoun, Georgia  
MED  UNKN  
632 (No SSNs or financial information reported)

An unauthorized disclosure resulted in the exposure of protected health information. The breach occurred on or around January 1, 2012 and was reported on April 17. This incident was reported on the HHS website.

April 17, 2012  
Anchorage Community Mental Health Services, Inc.  
Anchorage, Alaska  
MED  UNKN  
2,743 (No SSNs or financial information reported)

An unauthorized disclosure involving a computer or computers resulted in the exposure of protected health information. The breach occurred sometime between December 20, 2011 and January 4, 2012. This breach was reported on the HHS website.

April 16, 2012  
Kindred Transitional Care and Rehabilitation-Highgate  
Dedham, Massachusetts  
MED  PHYS  Unknown

Patients may call 800-545-0749.

An office burglary resulted in the theft of a safe on January 26. The safe contained unencrypted backup tapes that require specialized software and equipment to read. The tapes contained patient names, dates of birth, genders, diagnoses, and progress notes.

April 15, 2012  
Berrien County Sheriff’s Department  
Niles, Michigan  
GOV  HACK  Unknown

A hacker or hackers accessed information from the Berrien County Sheriff’s Department. An unspecified number of people had unspecified types of information posted online.

April 14, 2012  
Texas A&M University  
College Station, Texas  
EDU  DISC  4,000

Alumni who graduated before 1985 and requested copies of their transcripts may have been affected by a breach involving accidental disclosure. Certain alumni had their names, Social Security numbers, addresses, and telephone numbers in an electronic file that was emailed to an individual who would not normally have access to such information. The person who received the email notified the University.

UPDATE (5/03/2012): This breach was erroneously listed as occurring in Corpus Christi, Texas on this site. The breach affected those who were associated with Texas A&M University in College Station, Texas.

April 14, 2012  
Head Injury Association  
Long Island, New York  
MED  INSD  56

A former manager was indicted for stealing the identities of patients. He faces a 48-count indictment alleging grand larceny in the third degree, identity theft in the second degree, offering a false instrument for filing in the first degree, and possession of a forged instrument in the second degree. He allegedly used the names and Social Security numbers of patients to e-file fraudulent tax returns and obtain over $200,000 in federal, New York, and New Jersey tax refunds. The scam occurred in 2006 and 2007. It was not discovered until recently since those who were affected were unable to work with investigators.

The manager was convicted for similar crimes in the past. He used the information of a deceased and developmentally disabled individual from a Nassau County group home to obtain a fraudulent debit card and was also arrested for credit card fraud near Atlanta, Georgia.
UPDATE (12/19/2012): The former manager pleaded guilty to 20 counts of second-degree identity theft and offering a false instrument for filing, as well as six counts of criminal possession of a forged instrument and additional charges. He will pay $20,000 in restitution. His sentencing is expected to be on January 25, 2013 and he faces up to four years in prison.

**Information**
Source: Dataloss DB

**April 13, 2012**
**American Stock Transfer & Trust Company, LLC**
Brooklyn, New York

Mail packages containing the beneficiary statements of certain shareholders for the year of 2011 were mailed to incorrect addresses on April 2, 2012. The statements contained names, tax identification numbers of the intended shareholders, and addresses. Shareholders of a single, unnamed issuer that used American Stock Transfer as a sub-transfer agent most likely had their information mailed to a different shareholder than the shareholder listed on the beneficiary statement.

**Information**
Source: Dataloss DB

**April 13, 2012**
**The Home Depot**
Suwanee, Georgia

A dishonest employee accessed HR information with the intention of misusing the information to obtain fraudulent credit. At least 36 Home Depot employees had their names, Social Security numbers, contact information, driver’s license numbers, and possibly their financial account information accessed. The incident was discovered on March 15.

**Information**
Source: Dataloss DB

**April 13, 2012**
**State University of New York - Brockport College**
Brockport, New York

Hackers accessed Brockport College’s payment system by inserting malware into Brockport College’s computer system. Anyone who made a purchase on the campus may have had their credit or debit account information exposed. Brockport College responded by switching to cash payment for all purchases for the rest of the school term.

**Information**
Source: Dataloss DB

**April 12, 2012**
**Memorial Healthcare System (MHS)**
Hollywood, Florida

Patients with questions may call (877) 643-2062.

On January 27, 2012, MHS learned that at least one employee may have accessed patient information in order to receive fraudulent tax returns. A second employee was later identified and both employees were terminated. Patient names, Social Security numbers, and dates of birth may have been accessed between 2011 and early 2012. Medical information was not involved. Law enforcement requested that MHS delay notifying patients. On April 12, 2012, letters were mailed to patients who may have been affected.

**Information**
Source: PHIPrivacy.net

**April 12, 2012**
**Indiana University Medical Group**
Indianapolis, Indiana

A concerned citizen found a box of sensitive medical documents in a dumpster and contacted a local news team. The box contained hundreds of documents that included copies of driver’s licenses, prescriptions, signatures, and other patient information. The box was removed by Indiana University Medical Group before investigators arrived. Indiana University Medical Group claimed that the information was accidentally discarded rather than shredded. The documents were properly disposed after being collected.

**Information**
Source: PHIPrivacy.net

**April 12, 2012**
**Perry Dental**
Riverside, California

Computer equipment that contained patient insurance information was taken during an office burglary.

**Information**
Source: California Attorney General

**April 12, 2012**
**Housatonic Community College**

Two campus computers were determined to have been infected by malware. The breach occurred when a faculty or staff member opened an email that contained a virus. The virus was immediately detected. Faculty, staff, and students affiliated with the school between the early 1990’s and the day of the breach may have had their names, Social Security numbers, dates of birth, and addresses exposed. Housatonic’s president acknowledged that the cost of handling the breach could be as much as $500,000.

**Information Source:**
Dataloss DB

April 12, 2012  **Desmond Hotel**
**Albany, New York**

A foreign hacker accessed the information of guests who stayed at the hotel between May 21, 2011 and March 10, 2012. An unspecified number of credit and debit card numbers with corresponding names were accessed, but their associated PINs were not compromised.

**Information Source:**
Dataloss DB

April 12, 2012  **Associated Surveyors**
**Oklahoma**

The city in which this breach occurred was not reported.

Owners of a mini-storage business discovered that Associated Surveyors had abandoned sensitive information. The rent on the storage space had not been paid for over a year and Associated Surveyors and the items in the space were set to be auctioned off. The mini-storage owners decided to properly dispose of the documents in the unit when they found Social Security numbers, Social Security card applications, checks, bank account numbers, tax return forms, and copies of other documents with sensitive personal information.

**Information Source:**
Dataloss DB

April 12, 2012  **Triangle Tax Services**
**Miami, Florida**

A tax preparer for Triangle Tax Services was found to have information in her possession for the purpose of identity theft. A county deputy pulled the dishonest employee over for a traffic stop and found that she had checks, tax return credit cards, and handwritten names, dates of birth, and Social Security numbers. She faces at least eight counts of identity theft; though it is unclear how many of her 300 potential victims are connected to Triangle Tax Services.

**Information Source:**
Dataloss DB

April 12, 2012  **Rhinebeck Health Center, Center for Progressive Medicine**
**Rhinebeck, New York**

Rhinebeck created a page with information about the breach [here](http://www.rhinebeckhealth.com/breach.html).

On February 15, 2012, Rhinebeck learned that their unnamed computer vendor experienced a computer security breach. An unauthorized party or parties may have accessed any patient information between November 15, 2011 and December 14, 2011 that was on the Rhinebeck and Center for Progressive Medicine computer network. Patient full names, Social Security numbers, dates of birth, home addresses, phone numbers, account information, health insurance information, credit card information, laboratory tests, and diagnoses information may have been exposed. Anyone who visited either center between January 1, 2002 and December 22, 2011 may have been affected.

**Information Source:**
Dataloss DB

April 11, 2012  **North Shore University Hospital, North Shore - Long Island Jewish Health System**
**Manhasset, New York**

100 current and or former patients of North Shore University Hospital in Manhasset, New York were affected. Many more people who were not associated with the hospital were also affected.

A licensed nurse who may or may not have been affiliated with North Shore University Hospital was indicted for identity theft and possessing computer data from North Shore containing information on over 900 people. It is unclear when the breach that allowed the nurse and an accomplice to access the information first occurred. Social Security numbers, dates of birth, addresses, phone numbers, medical record numbers, insurance information, and medical histories could have been accessed. North Shore University Hospital notified 50 patients of a potential breach in 2011 and may have experienced a separate system breach in early January of 2012.

**UPDATE** (04/12/2012): The nurse also had the information of an unspecified number of U.S. Nippon Express employees.

**UPDATE** (02/05/2013): A lawsuit has been filed by a group of people who claim that the breach allowed identity thieves to access and misuse their information. Many, but not all, of twelve people who filed the lawsuit claim to have been victims.
Many, but not all, of twelve people who filed the lawsuit claim to have been victims of identity thieves. 

UPDATE (03/04/2013): North Shore Long Island Jewish Health System faces a $50 million class action lawsuit. It was also revealed that thefts of patient face sheet information for identity theft purposes have occurred at least three times in a matter of just a few years. 

UPDATE (5/24/2014): Another North Shore Hospital employee was charged for her involvement in the identity theft ring. "Latoya Talbert, 24, has been accused of stealing the identities so she could go shopping. Talbert was arraigned in Nassau County for her alleged involvement in an identity theft ring that began in 2011".

Information Source: PHIprivacy.net

April 11, 2012 X-Rite Incorporated, Pantone.com Grand Rapids, Michigan BSR HACK Unknown

On March 23, 2012, X-Rite learned that a database server had been attacked by a malicious third party. The names, contact information, and credit card information of customers who made purchases on X-Rite’s website pantone.com may have been exposed.

Information Source: California Attorney General

April 11, 2012 ACEware Systems Inc., Lewis-Clark State College, Lewiston, Idaho EDU HACK Unknown

An unauthorized party was able to access student records from ACEware Systems’ server. It contained student registration records from the Lewis-Clark workforce training center. The records included the last four digits of students’ Social Security numbers and partial credit card numbers.

Information Source: Dataloss DB

April 10, 2012 Seton Healthcare Family, HealthLOGIX Austin, Texas MED DISC 555 (No SSNs or financial information reported)

A computer mailing error caused Seton member Medicaid health plan cards to be sent to incorrect addresses. The cards were mailed by Seton’s vendor HealthLOGIX on March 9. Seton became aware of the breach when members began calling about receiving the incorrect cards a week after the mistake. Seton Health Plan members enrolled in the STAR/Medicaid plan were affected and may have had their names and dates of birth exposed.

Information Source: PHIprivacy.net

April 10, 2012 Thomas Jefferson University Hospitals (TJUH) Philadelphia, Pennsylvania MED PHYS 600

Affected patients may call (877)-309-0186.

Law enforcement informed TJUH management that sensitive documents had been recovered during an investigation. Radiology registration documents with patient names, Social Security numbers, addresses, home phone numbers, work phone numbers, dates of birth, TJUH account numbers, TJUH medical record numbers, insurance information, emergency contact information, and special radiology studies performed had been stolen from TJUH. It is unclear when the theft occurred. Patients who received services between February 4 and March 22, 2005 were affected.

Information Source: PHIPrivacy.net

April 10, 2012 Case Western Reserve University Cleveland, Ohio EDU PORT 600

The campus theft of two university-issued laptops resulted in the exposure of alumni information. Though University policy required data security measures, the laptops were not encrypted and did not have a program installed that would allow sensitive information to be deleted remotely. Master’s of arts and bachelor’s of arts alumni from 1987 through the date of the theft were affected.

Information Source: Databreaches.net

April 9, 2012 Pono Products, Inc. (Reuseit.com) Chicago, Illinois BSR HACK 1,000

Those with questions may email security@reuseit.com
A hacker or hackers were able to intercept customer information online between August 22 and September 28 of 2011. Customers who were affected may have had their login, password, and credit card information obtained. Anyone who used the same login and password combination for reuseit.com and other websites should change their password.

**Information**

**Source:** California Attorney General

**April 9, 2012**  
**Ernst & Young LLP, Cisco Systems, Inc.**  
**New York, New York**

BSF PORT Unknown

Cisco’s service provider Ernst & Young experienced a breach involving the information of current and former Cisco employees on March 26. On March 28, Cisco learned that a laptop with employee names, Social Security numbers, addresses, and the stock administration information of a select few had been stolen from an Ernst & Young employee’s home.

**Information**

**Source:** Dataloss DB

**April 9, 2012**  
**Intel, Advanced Micro Devices (AMD)**  
**Hudson, Massachusetts**

BSR INSD Unknown

A former Intel employee pleaded guilty to stealing documents for competitive advantage. The employee worked for AMD at the time of the theft and was able to retain access to some of Intel’s processor designs and chip fabrication process documents. He used his vacation time from Intel to begin working at AMD. The dishonest employee was charged with one count of stealing trade secrets for stealing a stack of documents in 2008 and four counts of wire fraud. Intel valued the documents at between $200 million and $400 million.

**Information**

**Source:** Media

**April 8, 2012**  
**Wilson County School District**  
**Wilson, Tennessee**

EDU DISC Unknown

The names and schools of students who met with graduation coaches, as well as their reasons for meeting were not completely removed from distributed meeting materials.

**Information**

**Source:** Dataloss DB

**April 8, 2012**  
**Contempo Enterprises, LLC**  
**West Des Moines, Iowa**

BSO HACK 330 (No SSNs or financial information reported)

A hacker or hackers accessed and posted sensitive Contempo Enterprises information online. Login credentials, names, email addresses, and customer data were exposed.

**Information**

**Source:** Dataloss DB

**April 6, 2012**  
**Utah Department of Health**  
**Salt Lake City, Utah**

GOV HACK 780,000 (280,000 SSNs)

Utah Medicaid clients have had their information exposed by a hack of an improperly protected Utah Department of Health computer server. The breach was discovered when an unusual amount of data was found to be streaming out of the server on April 2. Medicaid clients who had not had their Social Security numbers transitioned into the system had their Social Security numbers exposed. A majority of the affected individuals had medical claims, dates of birth, addresses, physicians’ names, and other forms of medical information exposed, but not Social Security numbers. Two out of three of those who were affected were children. The cost of working with the credit-reporting company Experian to contain the breach is estimated to be $460,000.

**UPDATE** (04/10/2012): Though the number of affected individuals was originally reported as 181,604 with 25,096 Social Security numbers exposed, Utah Department of Health reported that nearly 280,000 people had their Social Security numbers exposed by the breach. An additional 500,000 victims did not have their Social Security numbers exposed, but had some form of personal information such as date of birth, name, and address exposed. People who visited a health care provider in the past four months is likely to have been affected by the breach.

**UPDATE** (05/15/2012): The governor of Utah fired the Director of the Department of Technology Services and appointed a new employee, an ombudsman, to shepherd victims through the process of protecting their identities and credit. Two other members of the technology services department are under review. The vulnerability that caused the breach was partly, if not fully, due to failure to change a default password. Additionally, data will now be encrypted while it is on Utah servers as well as when it is in transit.

**UPDATE** (07/22/2012): Those who wish to learn more about the Utah Department of Health breach will be able to attend a
series of statewide workshops running from July 26 until August 22. Information on Utah’s Data Breach Security Tour can be found [here](#).

**UPDATE** (03/25/2013): The state of legislature of Utah added a second year of free credit monitoring to those who were affected by the breach. Additionally, a Utah health department official revealed that only 59,500 people had taken advantage of the first year of free credit monitoring service. Those who did not enroll in 2012 may call 801-538-6923 or email ombudsman@utah.gov to sign up for the 2013-2014 term.

**Massachusetts Registry of Motor Vehicles**

Two masked men stole several bags of documents and records from a state courier truck outside the Lawrence Registry of Motor Vehicle (RMV) branch on Wednesday April 4. However, the trash included records from the Wilmington branch of the RMV. Registration transactions, duplicate titles, crash reports, citation payments, rebate requests, and municipal parking records from transactions that occurred between Friday March, 30 and Monday, April 2 were stolen.

**University of California Riverside**

A hacker or hackers accessed information from the University of California Riverside. A total of 40 email addresses and corresponding passwords were posted online.

**Vote Sex!, Illinois**

No city was listed for this breach. A hacker or hackers posted 35,959 usernames, email addresses, and passwords online.

**Union Bank**

On February 15, 2012, Union Bank discovered that a former contractor kept proprietary bank data in his possession after leaving the company on January 31, 2012. The bank data included some customer information such as names, account numbers, home addresses, phone numbers, and email addresses.

**Experian, Crown Financial Group**

An unauthorized user or users was able to access credit reporting information after managing to pass Experian's authentication process. The unauthorized access incidents took place sometime between August 2, 2011 and August 9, 2011. Consumers may have had their names, addresses, Social Security numbers, years of birth, and account numbers exposed.

**Baylor Law School**

An administrative error resulted in recently admitted students receiving an email with the information of all recently admitted students. Student names, addresses, grades, LSAT scores, race, scholarship amount, and other types of
personal information were available in the email attachment. No Social Security numbers or dates of birth were in the
emailed spreadsheet. Students were encouraged to treat the data with the confidentiality of a lawyer and immediately
delete the email.

Information
Source: Databreaches.net

April 4, 2012  Glenwood IGA
Orofino, Idaho  BSR  UNKN  300

Investigators determined that a breach must have occurred at the grocery store Glenwood IGA after nearly 300 people
reported fraudulent charges on their credit cards. The credit card fraud began in early February and unauthorized
purchase attempts were made across the globe. The method of the breach is not clear.

Information
Source: Databreaches.net

April 4, 2012  World of Warcraft Latino America
Lower Merion, Pennsylvania  GOV  HACK  256 (No SSNs or financial information reported)

A hacker or hackers accessed the database information of World of Warcraft Latino America and posted the information
online. The leaked data included 256 usernames, email addresses, and passwords.

Information
Source: Databreaches.net

April 4, 2012  Mosler Automotive
Riviera Beach, Florida  BSR  HACK  218 (No SSNs or financial information)

A hacker or hackers accessed Mosler Automotive data and posted it online. A total of 218 usernames and hashed and
salted passwords were exposed.

Information
Source: Databreaches.net

April 4, 2012  State Farm Insurance
Bloomington, Illinois  BSF  INSD  Unknown

On March 6, 2012, an investigation confirmed that an employee of an unnamed State Farm office may have used customer
information in an inappropriate manner. An unknown number of customers may have had their names, addresses, credit
卡 numbers, and Social Security numbers misused by the dishonest employee.

Information
Source: California Attorney General

April 3, 2012  StandardAero
Tempe, Arizona  BSO  PORT  Unknown

The March 20 theft of a laptop and registration forms resulted in the exposure of customer information. Customer credit
card numbers were included in the registration information.

Information
Source: Databreaches.net

April 2, 2012  Applegate Valley Family Medicine
Grants Pass, Oregon  MED  PORT  2,300 (No SSNs or financial information reported)

A stolen laptop contained patient information. The theft occurred sometime between December 1, 2011 and December
17, 2011.

Information
Source: Databreaches.net

April 2, 2012  BJ's Wholesale Club
Westborough, Massachusetts  BSR  UNKN  Unknown

ON or around March 1, 2012, BJ's Wholesale learned that an unauthorized party had used the names, addresses, and
membership numbers of an unknown number of members to create new online profiles on BJs.com. Goods were then fraudulently purchased on the website between November 2011 and March 2012. The membership profile information that may have been accessed included Social Security numbers.

Information Source: Dataloss DB

April 1, 2012  Bethesda Softworks, Bethesda Blog
Rockville, Maryland  
BSO  HACK  3,657 (No SSNs or financial information reported)

A hacker or hackers posted the login information of two website administrators. The information of 8 job users was posted, as well as an additional 3,647 usernames, passwords, and emails. Anyone who used the same username, password, and/or email combination for other sites is encouraged to change them immediately.

Information Source: Dataloss DB

April 1, 2012  Onehitplay.com
Brea, California  
BSO  HACK  687 (No SSNs or financial information reported)

A hacker or hackers posted the information of users online. It is unclear if this is related to an identical incident that occurred on October 23, 2011.

Information Source: Dataloss DB

March 31, 2012  Opening Ceremony Online, LLC.
New York, New York  
BSR  UNKN  Unknown

Opening Ceremony discovered that an inadvertent breach of security resulted in the exposure of customer names, addresses, credit card numbers, credit card expiration dates, and credit card security codes. The breach was discovered sometime in March and first occurred on or around February 16, 2012.

UPDATE (5/11/2012): The breach lasted between February 16 and March 21 of 2012. Malware was discovered on the website on March 21. Affected customers were mailed notification letters on May 4. Either the credit card information was stored in an unencrypted format on the site in violation of Payment Card Industry Data Security Standard (PCI-DSS) practices, or a hacker was able to place something on the site to get credit card information after it was transmitted. It is more likely that Open Ceremony, an online clothing retailer, was not in compliance with PCI.

Information Source: California Attorney General

March 31, 2012  Sacramento Area Fire Fighters Local 522
Sacramento, California  
BSO  DISC  Unknown

On or around March 6, a spreadsheet containing the names and contact information of active and retired Local 522 members was sent by a Local 522 employee to the Sacramento Central Labor Council (CLC). The spreadsheet contained member Social Security numbers, but was only supposed to provide member mailing addresses. The email did not stop at CLC and was forwarded to Capitol Mailing, Inc. The mistake was discovered on March 23 after Local 522 members received mailing labels that displayed their Social Security numbers.

Information Source: California Attorney General

March 31, 2012  San Francisco Head Start, San Francisco State University
San Francisco, California  
GOV  UNKN  Unknown

The San Francisco Head Start/Early Head Start database was accessed by one or more unauthorized parties between August 2011 and November 2011. Names, Social Security numbers, addresses, contact information, health data, dates of birth, and other personal information may have been exposed. Head Start claimed that the delay in notification of the breach was due to an ongoing law enforcement investigation. It is unclear how San Francisco State University was involved.

Information Source: California Attorney General

March 31, 2012  St. Joseph’s Medical Center
Stockton, California  
MED  PHYS  Unknown
A storeroom window at Saint Joseph's HealthCare Clinical Laboratory (HCCL) was discovered broken on February 2, 2012. Two storage boxes containing HCCL lab requisition forms were missing from the center. People who received laboratory services between October 24, 2011 and November 18, 2011, between December 13, 2012 and January 5, 2012, and also between January 17, 2012 and January 31, 2012, may have had their names, Social Security numbers, phone numbers, addresses, and insurance information exposed.

**UPDATE (4/26/2012):** At least 700 patients were affected. Two boxes were discovered missing immediately after the robbery and a third was discovered missing on March 16.

**Global Payments Inc.**

Global Payments discovered a massive breach of their systems in early March 2012. Global Payments processes credit and debit cards for banks and merchants and a number of credit and debit cards issued to businesses were determined to be compromised. The breach was discovered when Global Payments' security systems detected unusual activity.

**UPDATE (04/02/2012):** Global Payments created a breach information website for consumers. Global Payments claimed that only a few of their North American servers were affected by the breach. They also claimed that around 1.5 million users had Track 2 data (card expiration date and credit card number) exposed. Media reports that up to 10 million consumers had their names, addresses, and Social Security numbers credit exposed were denied by Global Payments. Visa has removed Global Payments from their list of compliant service providers as a result of the breach.

**UPDATE (04/05/2012):** The breach occurred sometime between January 21 and February 25 of 2012 (REVISED TO JUNE OF 2011). Fraudulent activity has already been detected on around 800 cards.

**UPDATE (05/01/2012):** It appears that a hacker or hackers were first able to access Global Payments Inc. in June of 2011. Global Payments revised their initial estimate and believe that card holders and banks were affected at least as far back as June 2011. This could mean that at least seven million card accounts are vulnerable; though Global Payments still believe that only 1.5 million were affected.

**UPDATE (07/26/2012):** In addition to being dropped from Visa and Mastercard's lists of compliant companies, Global Payments spent nearly $85 million on security repairs and upgrades.

**UPDATE (07/30/2012):** Global Payments informed Comerica Bank in June that their ongoing investigation revealed a potential unauthorized access to its servers that contain merchant application data.

**UPDATE (01/10/2013):** Global Payments has incurred $94 million in fees associated with the breach. A total of $60 million was paid for professional fees and other costs associated with investigating the breach and remediation for its effects. The $60 million was also used to cover incentive payments to business partners and the cost of providing credit monitoring and identity protection insurance. An additional $35.9 million went towards estimated fraud losses, fines, and charges imposed on Global Payments by card networks. Global Payments received $2 million from insurance recoveries.

Global Payments also reported that it has now paid all fines related to non-compliance and has updated its systems and processes in order to be returned to the payment card network list of PCI-DSS compliant service providers.

**UPDATE (04/15/2013):** An April 2012 class action lawsuit related to the breach was dismissed on March 6. Global Payments also confirmed that the expenses associated with the breach totaled $92.7 million. A total of $20 million in breach losses was recuperated through insurance recoveries. In April 2013, Global Payments closed its investigation of the breach.

**Eclipse AeroSpace**

A hacker or hackers accessed and posted Eclipse AeroSpace database information online. The leaked information included email addresses, usernames, names, and passwords.

**Savvyinsider.com**

A hacker or hackers accessed and posted savvyinsider.com database information online. A total of 24 usernames, email addresses, and passwords were exposed.
March 30, 2012  **Public Broadcasting System**  
Arlington, Virginia  
NGO  HACK  
1,871 (No SSNs or financial information reported)

A hacker or hackers accessed and published information from a Public Broadcasting System server or database. A total of 1,598 press usernames, plain-text passwords, and email addresses were posted online. Thirty-six administrator names, usernames, email addresses and passwords were also publicly posted. Finally, 237 names, emails, passwords, and usernames from other sources were posted online.

**Information**  
**Source:**  Dataloss DB  

March 30, 2012  **Advanced Clinical Research Institute**  
Anaheim, California  
MED  PHYS  
875 (No SSNs or financial information reported)

A vehicle containing paper records was impounded overnight. Some papers with the sensitive information of research participants were discovered missing when the vehicle was reclaimed. The breach occurred on or around January 26.

**Information**  
**Source:**  Dataloss DB  

March 30, 2012  **Department of Child Support Services, International Business Machines (IBM), Iron Mountain, Inc.**  
Boulder, Colorado  
GOV  PORT  800,000

The location listed is that of IBM's headquarters.

On March 12, 2012, the Department of Child Support Services (DCSS) was notified that contractors International Business Machines (IBM) and Iron Mountain, Inc. could not locate several computer devices that had been shipped from Colorado to California. Californians who used state child support services were affected by the loss. Names, Social Security numbers, addresses, driver's licenses, names of health insurance providers, health insurance plan membership identification numbers, and employer information may have been exposed.

**Information**  
**Source:**  PHIprivacy.net  

March 29, 2012  **Greenville County School District**  
Greenville, South Carolina  
GOV  PHYS  10

A filing cabinet that was full of personnel information was accidentally locked, wrapped, and shipped to a prison in February of 2012. The prison supervisor unlocked the filing cabinet, noticed that it still contained files, and immediately sent it back. Employee driver's license and Social Security numbers were in the cabinet.

**Information**  
**Source:**  Dataloss DB  

March 29, 2012  **Go-Kart Records**  
New York, New York  
BSR  HACK  227 (No SSNs or financial information reported)

A hacker or hackers accessed and published sensitive information from a Go-Kart Records database. A total of 218 usernames, email addresses, and passwords were posted. Additionally, nine employee usernames, email addresses, and plain text passwords were posted.

**Information**  
**Source:**  Dataloss DB  

March 29, 2012  **Grant Income Tax Bookkeeping and Check Cash**  
Macon, Georgia  
BSF  INSD  10

The dishonest owner of the tax preparation business used names and Social security numbers to file fraudulent tax returns for at least 10 people between 2007 and 2009. He is accused of using nearly $8,000 in fraudulent tax refunds for his own purposes. He was indicted on 23 counts of making false claims for tax refunds, four counts of theft of government money, and four counts of aggravated identity theft on March 15, 2012. He pleaded guilty and faces a maximum sentence of 10 year sin prison and a $250,000 fine for each count of theft of government money, a minimum of two years in prison for the identity theft charges, and a maximum of five years in prison with a $250,000 fine for each count of false claims.

**Information**  
**Source:**  Dataloss DB  

St. Joseph's Medical Center, HealthCare Clinical Laboratory, Patient Service
March 29, 2012  Center
Stockton, California

A February 2 office burglary resulted in the exposure of patient records from the Health Care Clinical Laboratory Patient Service Center. Two storage boxes that contained lab requisition forms were immediately discovered missing. They contained lab information provided between December 13, 2011 and January 5, 2012. A third box containing records of services administered between October 24 and November 18 was discovered missing on March 16. Names, Social Security numbers, insurance information, addresses, and phone numbers may have been exposed. At least one patient reported an attempt to open a credit card under their name since the thefts.

Information
Source: Dataloss DB

March 28, 2012  Hawaii Community Federal Credit Union (HCFCU)
Kailua-Kona, Hawaii

An HCFCU member filed a complaint in 2011 after suspecting that their information had been improperly used for an HCFCU board nomination process. It became apparent that several employees had added names to nomination petitions, then went to credit union members to have them sign the petitions. Fewer than 500 of the 40,000 HCFCU members had their account information and the last four digits of their Social Security numbers accessed. The employees involved were disciplined and/or had their employment terminated. HCFCU employees are now required to go through a new training process to reinforce policies that prohibit accessing members’ information.

Information
Source: Dataloss DB

March 28, 2012  Douglas County Probation Office
Omaha, Nebraska

A county clerk was the victim of a car theft. She had left sensitive documents for homicide trials in the trunk of her car. The documents were recovered from the car wreckage. Personal information for police officers associated with the homicide trials and names and addresses of witnesses could have been exposed. Documents will be scanned and never physically taken from the courthouse again as a result of the breach.

Information
Source: Dataloss DB

March 28, 2012  Capital Area Community Action Agency
Tallahassee, Florida

About 100 client files were discovered missing from a file cabinet in a restricted area. The files contained Social Security numbers and other personal information. A spokesperson for Capital Area Community said that a disgruntled former or current employee may be to blame.

Information
Source: Dataloss DB

March 27, 2012  Howard University Hospital
Washington, District Of Columbia

The January 27 theft of a laptop from a former contractor's vehicle resulted in the loss of patient information. The patient files included Social Security numbers, names, addresses, identification numbers, medical record numbers, dates of birth, admission dates, diagnosis-related information, and discharge dates. The majority of those affected were patients who were treated at the Hospital between December 2010 and October 2011. Some patients who received treatment as far back as 2007 were also affected. The patient files had been downloaded onto the contractor's personal laptop in violation of the Hospital's policy. The contractor stopped working for the hospital in December of 2011.

UPDATE (09/21/2012): The number of patients who were notified was revised from 34,503 to 66,601.

Information
Source: Databreaches.net

March 27, 2012  Affordable Medical and Surgical Services
Overland Park, Kansas

A woman found over 1,000 detailed abortion records in a dumpster when she went to dump her recycling near a local elementary school. The records included names, Social Security numbers, birth dates, telephone numbers, emergency family contacts, patient health histories, number of children, term of pregnancies, number of previous abortions, reasons for failing to go through with the abortion procedures, and fees paid for the procedures. Many of the records were from 2001 and 2002. The physician who ran the practice admitted to dumping the records without attempting to properly destroy them. His clinic had closed in 2005 after he lost his medical license. The county district attorney commented that he will most likely not pursue a criminal case against the former physician.

Information
Source: PHIPrivacy.net

March 27, 2012  WorldPass

324
<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Type</th>
<th>Source</th>
<th>Records from this breach used in our total:</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 27, 2012</td>
<td>El Dorado Hills, California</td>
<td>BSR</td>
<td>HACK</td>
<td>Unknown</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A hacker or hackers accessed WorldPass' online database in early July of 2010 and was not detected until March 5, 2012. The hacker may have obtained the credit card numbers, user names, email addresses, billing addresses, and payment information of customers.</td>
</tr>
<tr>
<td>March 25, 2012</td>
<td>MilitarySingles.com New York, New York</td>
<td>BSR</td>
<td>HACK</td>
<td>171,000 (No SSNs or financial information reported)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Hackers affiliated with LulzSec (Reborn) claimed responsibility for revealing a database of militarysingles.com names, usernames, email addresses, IP addresses, and passwords on the Internet. People who used their same email and password combination for Militarysingles.com and other sites are encouraged to change their passwords. Militarysingles.com is owned by ESingles, Inc. An ESingles executive claimed that no evidence of an attack had been found as of March 28; however, a number of sources revealed that they could download and decrypt sensitive information by following a Twitter announcement.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>UPDATE (3/28/2012):</strong> ESingles released a statement claiming that a thorough investigation revealed that the database had not been hacked. A discrepancy between the number of users in the militarysingles.com database, the use of encrypted user passwords, and the fact that the website was already scheduled to be down for maintenance during the time the hackers claimed to have taken it down led ESingles to this conclusion.</td>
</tr>
<tr>
<td>March 24, 2012</td>
<td>CVS Caremark Woonsocket, Rhode Island</td>
<td>BSR</td>
<td>DISC</td>
<td>3,482 (No SSNs or financial information reported)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>People who were members of Tufts Health Plan (Tufts Associated Health Maintenance Organization, Tufts Insurance Company) received letters meant for other members. A programming error caused the addresses of members to be incorrect. Names, medical conditions, and medications were exposed.</td>
</tr>
<tr>
<td>March 23, 2012</td>
<td>Pure Austin, Texas</td>
<td>BSR</td>
<td>CARD</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A man stole 100 debit and credit cards, some bottles of alcohol, and cash from the office of a bar called Pure. The thief managed to use one of the stolen cards at a convenience store before being caught for a separate incident involving robbery by assault. Cameras showed that the man had entered through a ventilation shaft connected to the bar's office.</td>
</tr>
<tr>
<td>March 23, 2012</td>
<td>H&amp;R Block Van Nuys, California</td>
<td>BSF</td>
<td>INSD</td>
<td>Unknown</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>An H&amp;R Block office manager was caught wearing a disguise near the ATMs of three banks. The employee's vehicle was searched and contained $2,960 in cash, and client records with dates of birth, names, and Social Security numbers. A total of $6,900 cash, H&amp;R Block Emerald Cards, and the personal information of additional people were found at the home of the employee's girlfriend. The number of fraudulent tax returns, victims, and years the employee worked for H&amp;R Block were not revealed.</td>
</tr>
<tr>
<td>March 23, 2012</td>
<td>Manhattan Prep New York, New York</td>
<td>BSR</td>
<td>HACK</td>
<td>Unknown</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A hacker was able to access the names, mailing addresses, email addresses, dates of birth, usernames, passwords, phone numbers, and credit card details of customers. The breach occurred and was detected on Sunday, March 25. Manhattan Prep removed all credit card information previously associated with compromised customer accounts from their database. Customer account passwords were automatically reset. Customers were also encouraged to change any passwords that were used for both Manhattan Prep and other accounts.</td>
</tr>
</tbody>
</table>
March 23, 2012  Lake Worth Independent School District
Lake Worth, Texas

Employees of Lake Worth School District received email notification of a possible computer security breach. It appears that a former employee may have accessed the personal information of employees and could have misused it. It is unclear if a breach actually occurred. It is also unclear how the former employee may have compromised the district’s computer system.

Information
Source: Databreaches.net

March 23, 2012  Suddenlink Communications, AAT Communications
Overland Park, Kansas

On February 24, 2012, law enforcement notified Suddenlink management of an incident involving a former employee. The employee had obtained the personal information of individuals who worked at Suddenlink and AAT Communications between May 22, 2006 and July 21, 2006. Names, Social Security numbers, addresses, dates of birth, wage information, and banking information may have been exposed. The former employee was using the information for fraudulent purposes and an investigation uncovered isolated instances of information misuse between 2006 and 2012. The former employee was arrested.

Information
Source: Dataloss DB

March 23, 2012  Duke University Health System (DUHS)
Durham, North Carolina

A notice from Dukehealth.org can be found here: http://www.dukehealth.org/health_library/news/notice-to-patients-who-pre...

ON or around January 25, DUHS received notice that its billing subsidiary staff attached copies of outstanding billing statement(s) for services provided by DUHS facilities and/or DUHS-affiliated physicians to support proofs of claim filed in Chapter 13 bankruptcy actions by patients of DUHS. Patient and patient dependent names, addresses, DUHS medical record number, health insurance carriers, and clinical information were exposed. Some patients and patient dependents had their Social Security numbers and dates of birth exposed as well. Notification letters were mailed on March 23 and again on May 18.

Information
Source: Dataloss DB

March 23, 2012  BenefitsEvent, Orvis Company
Peck Slip, New York

Orvis’ hosting company notified Orvis that it may have experienced a breach. It received reports from other clients that fraudulent charges had appeared on their customers’ credit cards. The customer credit cards had been used for hosted events. The computer database was encrypted, though it appears to have been compromised.

Information
Source: Dataloss DB

March 22, 2012  Flex Physical Therapy
Bothell, Washington

Three computers were stolen on December 30, 2011. One of the computers contained the protected health information of patients.

Information
Source: HHS via PHIPrivacy.net

March 22, 2012  Delta Dental
Sacramento, California

The unauthorized disclosure of paper records sometime around December 22, 2011 may have resulted in the exposure of protected health information.

Information
Source: HHS via
The unauthorized disclosure of paper records may have resulted in the exposure of the protected health information of people associated with Department of Medical Assistance Services (DMAS). The incident related to DMAS’s relationship with Affiliated Computer Services (ACS) and occurred sometime between November 2, 2011 and November 16, 2011.

Information
Source: HHS via PHIPrivacy.net

The location of the breach is listed as Medco’s main office in New Jersey.

The unauthorized disclosure of paper records on November 30, 2011 may have resulted in the exposure of protected health information.

Information
Source: HHS via PHIPrivacy.net

The February 11, 2012 theft of a laptop resulted in the exposure of protected health information.

Information
Source: HHS via PHIPrivacy.net

The theft of a laptop on or around November 10, 2011 may have resulted in the exposure of protected health information. It is unclear if this incident is related to a December 29, 2011 incident that also resulted in the theft of a laptop that contained protected health information.

Information
Source: HHS via PHIPrivacy.net

A hacker or hackers accessed and exposed information from Zybez. Usernames, email addresses, IP addresses, and passwords were exposed.
A technician's USB thumb drive with patient information was misplaced at Georgetown University Hospital. People who were associated with the Department of Laboratory Medicine and visited the Hospital between September of 2004 and September of 2009 may have had their names, medical record numbers, dates of birth, blood types, dates of blood tests, blood test results, summary of clinical histories, and clinician names exposed. The thumb drive was last seen on September 9, 2011, and was discovered missing on the morning of September 14, 2011.

Police officers discovered a large number of credit card receipts and other items during a traffic stop in June of 2011. The driver was then arrested and admitted to using stolen credit card receipts from Comfort Inn & Suites to make fraudulent credit cards. He had stolen around 500 receipts and successfully used two counterfeit credit cards. He was sentenced to five years and 10 months in federal prison and ordered to pay $3,606 in restitution.

UPDATE (03/22/2012): Additional credit card receipts were found and connected to Brownsville, Texas.

An employee of Wayne County's personnel department accidentally sent an email with a sensitive attachment. People who were members of AFSCME Locals 25, 409, 1659, and 3309 received an email about health insurance with employee names, ID numbers, Social Security numbers, dates of birth, addresses, and other information available in an attached file. The mistake was noticed immediately and a follow-up email was sent with instructions to destroy the previous email.

UPDATE (4/16/2012): About 1,300 union members received the email and it contained the information of over 1,000 employees.

The city of Providence accidentally provided the Social Security numbers of almost 3,000 former employees when releasing information for a public records request. GoLocalProv filed an Access to Public Records Act request in order to obtain information about pension recipients in Providence. The city's legal team responded by emailing a .pdf file with retiree names, dates of retirement, dates for cost-of-living-adjustments, and monthly pension received each month. Social security numbers and employee identification numbers were displayed as redacted in the document, but could easily be read when the .pdf file was expanded or when the highlight color of the document was changed to a light color.

Unusual activity was noticed on Sailboat Owner's web servers on the morning of February 23. The website was immediately shut down, but sensitive information may have been accessed. Malware had been uploaded to the web server on the morning of February 22. A total of 2,258 unencrypted credit card records were on the server and dated from 2007 until the day of the incident. CVV codes and expiration dates were also exposed.

Someone purchased a hard drive in September of 2011 and immediately notified law enforcement that it contained confidential information. The external hard drive did not come from a Kaiser Permanente office. It contained employee data that was as recent as 2009. Current and former employees may have had their names, Social Security numbers,
dates of birth, and addresses exposed. There is no evidence that the information from the hard drive was used for illegal purposes as of March of 2012.

**UPDATE** (3/22/2012): The external hard drive was purchased at a thrift store. Phone numbers, pay stubs, COBRA Error, Trust Fund Paid Hours, or Fidelity Savings Plan Deduction reports may have also been on the hard drive.

**UPDATE** (4/16/2012): At least one source lists the total number of affected current and former employees as 30,000.

**UPDATE** (2/4/2014): Attorney General Kamala Harris has agreed to drop a data breach lawsuit against the Oakland based managed care provider, Kaiser, if they agreed to a $150,000 fine paid to the state and improved their information handling practices.

Originally the suite contended that the health care provider violated the three-month notification law. Kaiser learned of the violation in December 2011 but did not send letters to 20,539 affected Californians until mid-March 2012. The law requires data-holders disclose any breach "in the most expedient time possible and without unreasonable delay".

---

**Information**

**Source:**

California Attorney General

**March 19, 2012**

**IndyMac Bank, IndyMac Resources, Inc.**

Dallas, Texas

BSF DISC Unknown

A security company searching the web for sensitive data uncovered personally identifiable information from IndyMac Bank and Indy Mac Resources employees, and possibly others associated with the firms. IndyMac Bank failed sometime around July of 2008. The information is related to IndyMac employee pension benefits analysis and appears to have been placed on a public web server by an employee of a contractor for IndyMac. People who were employed by either IndyMac firm between January 1, 1999 and January 1, 2005 had their names, Social Security numbers, dates of birth, earnings, hire dates, and other employment related information exposed. It was available as early as January of 2007 and as recently as December of 2011.

**Information**

**Source:**

California Attorney General

**March 19, 2012**

**Adult Insider Network, Adultinsider.com**

Killeen, Texas

BSO HACK

10,704 (No SSNs or financial information reported)

A hacker or hackers accessed and posted information from the adultinsider.com database online. The leaked information included email addresses, passwords with associated salts, and usernames.

**Information**

**Source:**

Dataloss DB

**March 18, 2012**

**National Capital Planning Commission (NCPC)**

Washington, District Of Columbia

GOV HACK

21 (No SSNs or financial information reported)

A hacker or hackers accessed and posted the database information of NCPC online. A total of 21 names, email addresses, telephone numbers, passwords, and job titles were leaked.

**Information**

**Source:**

Dataloss DB

**March 17, 2012**

**Kennedy Space Center**

Orlando, Florida

GOV PORT 2,300

The theft of a company-issued laptop from an employee's car resulted in the exposure of sensitive information. The laptop was stolen from the employee's car while it was at home and contained the names, Social Security numbers, races, national origins, genders, dates of birth, contact information, college affiliations, grade-point averages, and other information of employees. The hard drive was not encrypted. The Kennedy Space Center had planned to have all hard drives encrypted by September 2012 prior to the breach.

**Information**

**Source:**

Databreaches.net

**March 17, 2012**

**Georgia Obstetrical and Gynecological Society**

Suwanee, Georgia

MED PORT 1,000 (Unknown number of financial records)
Two laptops with member information were stolen during an office burglary. Financial and other administrative information were also on the laptops. The laptops did not contain any patient information. It is unclear if the theft of the equipment was politically motivated.

UPDATE (3/26/2012): The breach appears to have been politically motivated. Two other OB-GYNs had laptops stolen from their offices after speaking out against a controversial Georgia bill.

Information Source: Databreaches.net

March 16, 2012 Huntsville Hospital
Huntsville, Alabama

125 (No SSNs or financial information reported)

A thief or thieves entered Huntsville Hospital and impersonated a vendor in order to collect old barrels of X-rays. Thieves commonly use this tactic to obtain X-rays. The X-rays are then stripped for silver. The X-rays contained patient names, dates of birth, and medical records. There were over 1,000 X-rays, but only 125 to 175 patients were affected.

Information Source: PHIPrivacy.net

March 16, 2012 University of Tampa
Tampa, Florida

30,000

A server management error caused files containing sensitive information to be made publicly accessible between July of 2011 and the breach's discovery on March 13, 2012. A classroom exercise revealed that the information was compromised and the University of Tampa's IT office was immediately informed of the discovery. The University of Tampa then notified Google and asked that the cached file be removed from the search engine.

One file included 6,818 records of students who attended in Fall of 2011. Two other files contained the information of an additional 29,540 people and included University ID numbers, names, Social Security numbers, and photos. Some people also had their dates of birth exposed. The IT office at the University of Tampa concluded that the files had only been accessed by the people who reported the breach.

UPDATE (3/22/2012): Additionally, 22,722 current and former faculty, staff, and students who were associated with the University between January 29, 2000 and July 11, 2011 may have had their information exposed. The IT office confirmed that these files had only been accessed by University insiders as well. The University will not cover the cost of credit monitoring services for those who were affected.

Information Source: Databreaches.net

March 16, 2012 Milk Inc.
San Francisco, California

Unknown

An employee of another company discovered a security issue in Oink. Oink is a "rate everything" application from mobile application developer Milk Inc. The security issue allowed anyone to download personal information of another Oink user by entering another person's username. Folders with associated email addresses, photos, and other user site information may have been exposed. Oink shutdown and the employees of Milk Inc. joined Google for a new project shortly after the issue was discovered.

Information Source: Databreaches.net

March 16, 2012 Arizona Sports Fans, Arizonasportsfans.com
Bernardsville, New Jersey

8,855 (No SSNs or financial information reported)

A hacker or hackers accessed and posted database information from arizonasportsfans.com online. The leaked information included email addresses, passwords, salts for passwords, and usernames.

Information Source: Dataloss DB

March 15, 2012 Georgia Health Sciences University
Augusta, Georgia

513 (No SSNs or financial information reported)

Those with questions may email privacy@georgiahealth.edu.

A laptop was stolen from the home of a nurse on January 18, 2012. It contained the names, dates of birth, partial diagnosis information, and internal codes associated with patients' laboratory tests. The information is from patients of
the Adult Sickle Cell Clinic.

Information
Source: PHIPrivacy.net
March 15, 2012 Edmund Optics Barrington, New Jersey MED HACK Unknown

Edmund Optics identified suspicious activity on their website on February 26, 2012. It was determined that a security breach had occurred and that some customer accounts had been compromised. The breach most likely occurred on February 8 and resulted in the theft of some customers’ credit card information. The website was secured and preventative measures were increased.

Information
Source: Databreaches.net
March 15, 2012 Iran Defense Forum, Irandefence.net Plano, Texas NGO HACK 3,212 (No SSNs or financial information reported)

A hacker or hackers accessed and posted the database information of Irandefence.net online. The leaked information included usernames, email addresses, passwords, and associated password salts.

Information
Source: Dataloss DB
March 15, 2012 vBCoderz.com Provo, Utah BSO HACK 1,290 (No SSNs or financial information reported)

A hacker or hackers accessed and posted the database information of vBCoderz.com online. A total of 1,290 email addresses, usernames, and passwords with associated salts were exposed.

Information
Source: Dataloss DB
March 15, 2012 Washington University St. Louis, Missouri EDU INSD 4,100

A University employee was discovered copying electronic files onto an external hard drive on February 17, 2012. The hard drive was recovered and the employee was fired. The hard drive contained the names, Social Security numbers, addresses, and dates of birth of University employees and job applicants. It is unclear if the hard drive information was used for fraudulent purposes.

Information
Source: Dataloss DB
March 14, 2012 RJL Insurance Services, LLC, RJL Wealth Management San Diego, California BSF DISC Unknown

RJL Insurance Services became aware of a vulnerability in its computer network that may have resulted in the exposure of some electronic files. The information was secured, but some RJL files were accessible for a period of two weeks in late September and early October of 2011. Client names, Social Security numbers, driver’s license numbers, and medical conditions may have been exposed.

Information
Source: California Attorney General
March 14, 2012 Humboldt State University Arcata, California EDU DISC 5,700

The personal information of students was accidentally sent in an email attachment as a response to a request for data. The mistake was noticed immediately and all copies of the file were removed from the system of the party requesting data. Student names, addresses, and Social Security numbers were exposed. Humboldt State University warned students to be vigilant about phishing, but stated that it is unlikely the data was misused.

Information
Source: Databreaches.net
March 14, 2012 Forte Interactive, Children’s Service Council of Palm Beach County, Ocean Reef Community Association West Palm Beach, Florida BSO DISC Unknown
Information Forte Interactive inadvertently copied from web applications used by Children's Service Council and Ocean Reef Community accidentally became publicly accessible after a system upgrade. Names, Social Security numbers, driver's license numbers, and dates of birth of individuals whose information was contained in the web portal or web portals was publicly accessible between December 7, 2011 and February 3, 2012. The issue was discovered on January 30, 2012.

Information Source:
Dataloss DB

March 13, 2012 Brigham Young University (BYU) Provo, Utah EDU DISC 1,300 (No SSNs or financial information reported)

A staff member of the University Advisement Center at BYU accidentally included a complete list of international student names, email addresses, phone numbers, and student ID numbers in an email notification about a career workshop. BYU immediately apologized for the error and noted that all of the student information except for student ID numbers could easily be found in the BYU directory.

Information Source:
Datalosch.edu

March 13, 2012 Citibank New York, New York BSF HACK Unknown

An unauthorized party was able to illegally access information maintained by Citi through a source other than Citi. The unauthorized party logged onto Citi's credit card online account access system by using passwords and user IDs. Customer names, addresses, email addresses, account numbers, and transaction information may have been viewed. Customers who were affected were notified, issued replacement cards, and required to create new account login credentials.

Information Source:
Dataloss DB

March 12, 2012 Impairment Resources, LLC San Diego, California MED PORT 14,000

An office burglary on New Year's Eve 2011 resulted in the loss of hardware that contained sensitive personal information. The full names, addresses, Social Security numbers, and medical information of clients were on the hardware. Impairment Resources notified patients in February and then filed for bankruptcy in March. The high cost of handling the breach led directly to the decision to file for bankruptcy.

Information Source:
California Attorney General

March 12, 2012 TransUnion LLC, Manufacturers Life Insurance Company (Manulife) Chicago, Illinois BSF HACK 461

The location listed is that of Trans Union's Chicago Office.

An unauthorized access occurred sometime between January 22 and February 15, 2012. Trans Union learned of the breach through its subscriber The Manufacturers Life Insurance Company (Manulife). Consumers may have had their credit reports accessed by someone using a client's login credentials. Names, Social Security numbers, and addresses would have been exposed.

Information Source:
Dataloss DB

March 9, 2012 Office of Dr. David Turner Portland, Oregon MED PORT 480 (No SSNs or financial information reported)

An office burglary in October of 2011 resulted in the theft of a laptop and other items. The laptop contained the information of current and former patients. It is unclear what type of information the laptop contained. A widespread notification of the breach was released in March after many patients could not be reached by mail.

Information Source:
PHIPrivacy.net

March 9, 2012 McDonald's Tulsa, Oklahoma BSR INSD 282
A dishonest McDonald’s employee confessed to using a handheld skimming device for three weeks to capture drive-thru customer credit and debit card numbers. He then passed the information along to others who used the numbers to produce fraudulent cards and make purchases. A total of 282 card numbers were discovered on a suspect's laptop.

**UPDATE (07/02/2012):** The former employee pleaded guilty to an aggravated identity-theft charge. He agreed to playing a part in causing a total loss of more than $51,000. Four other defendants were first caught in October of 2011. They were arrested on suspicion of trying to buy merchandise with counterfeit cards and were caught with a laptop that contained stolen credit and debit card numbers.

**Information Source:** Dataloss DB

**March 9, 2012**

*Texas-DSM.com*

**Source:** Texas-DSM.com, Texas

BSO HACK

647 (No SSNs or financial information reported)

No city was reported for this breach.

A hacker or hackers posted email addresses, passwords, and usernames online. Members of similar online forums recommended that users change their passwords for other sites since members often use the same email address, password, and username combination for multiple sites.

**Information Source:** Dataloss DB

**March 9, 2012**

*Gaming Perfection*

**Source:** Gaming Perfection Bronx, New York

BSO HACK

1,784 (No SSNs or financial information reported)

A hacker or hackers accessed and posted the database information of Gaming Perfection online. A total of 1,784 email addresses, passwords with associated salts, and usernames were exposed.

**Information Source:** Dataloss DB

**March 9, 2012**

*LifeSize Communications*

**Source:** LifeSize Communications Austin, Texas

BSR STAT

Unknown

A computer that contained unencrypted personal information was stolen from LifeSize Communications on January 26, 2012. Names, Social Security numbers and other information were on the stolen computer. Those who were affected were sent notifications on March 9.

**Information Source:** Dataloss DB

**March 9, 2012**

*Bad Boy Tires*

**Source:** Bad Boy Tires, Massachusetts

BSR HACK

111 (No SSNs or financial information reported)

No city was listed for this breach.

A hacker or hackers accessed and posted database information from Bad Boy Tires online. A total of 111 names, emails, postal addresses, phone numbers, and plain-text passwords were exposed.

**Information Source:** Dataloss DB

**March 9, 2012**

*Kelly Services*

**Source:** Kelly Services Troy, Michigan

BSO INSD

Unknown

People who signed up for employment through the Kelly Services staffing agency may have had their personal information retained by a former Kelly Services employee. Kelly Services retrieved all of the sensitive information from the former employee upon learning of the breach. Names and Social Security numbers may have been exposed.

**Information Source:** Dataloss DB

**March 9, 2012**

*New York Ironworks*

**Source:** New York Ironworks New York, New York

BSR HACK

434 (No SSNs or financial information reported)
A hacker or hackers posted 434 usernames and corresponding passwords, as well as email addresses online.

Information Source: Dataloss DB
March 7, 2012 Gila County Health and Emergency Services (Payson WIC Office) Payson, Arizona GOV PHYS 1,000

A woman found thousands of applications for Women, infants, and Children (WIC) support in a dumpster. Around 1,000 documents were originally reported in the dumpster. Additional documents were discovered when a local news team joined the woman at the dumpster a few days later. The applications included copies of drivers licenses, Social Security numbers, medical information, and many other types of sensitive information. An employee of the state agency said that the forms would normally be properly shredded, but were thrown out in a hurry without being checked.

Information Source: Databreaches.net
March 7, 2012 Lindenwood University Belleville, Illinois EDU HACK 184 (No SSNs or financial information reported)

Someone accessed student information and posted it on Twitter @LindenLeaks. The information was from the Fall 2011 semester and included grades, majors, phone numbers, and email addresses. The account was eventually deleted from Twitter. The person who originally posted the information online commented that the document had been downloaded nearly 140 times since being posted.

Information Source: Databreaches.net
March 7, 2012 Pacific Gas and Electric (PG&E) Lodi, California BSO PHYS 100

A payment drop box was broken into sometime during the weekend of March 5. Customers who used the box around that time may have had their banking institution information, check account numbers, addresses, names, phone numbers, and driver’s license numbers stolen. PG&E will change the account numbers and passwords of customers who had their information stolen.

Information Source: Dataloss DB
March 7, 2012 University of California Los Angeles (UCLA) Los Angeles, California EDU HACK 168 (No SSNs or financial information reported)

Hackers accessed and posted the usernames and passwords of individuals who had access to the UCLA.edu MySQL database. A total of 128 regular users had their names, titles, email addresses, logins, and password hashes posted online. Additionally, the IDs, usernames, salts, and password hashes from 37 staffers were posted online. Three database users also had their usernames and password hashes posted online.

Information Source: Dataloss DB
March 7, 2012 Minuteman Civil Defense Corps, Declaration Alliance, Pennsylvania NGO HACK 30 (No SSNs or financial information reported)

The city of the breach was not reported.

A hacker or hackers posted 30 names, telephone numbers, email addresses, and corresponding passwords online.

Information Source: Dataloss DB
March 6, 2012 Digital Playground Van Nuys, California BSR HACK 72,794 (44,663 credit card numbers obtained)
A group of hackers accessed customer details, credit card numbers, and administrator information. At least a) 28 administrator names, usernames, email addresses, and encrypted passwords, b) 85 affiliate usernames, plain-text passwords, c) 100 user email addresses, usernames, and plain-text passwords, and d) 82 .gov and .mil email addresses and plain-text passwords were posted. The hackers criticized the ease of obtaining the credit card numbers, expiration dates, cvvs, and customer billing addresses which were all in plain text. The hackers chose not to post customer credit card numbers.

Information
Source: Databreaches.net

March 5, 2012  Kern Medical Center  Bakersfield, California  MED PHYS 1,500 (No SSNs or financial information reported)

Concerned patients may call 1-877-800-5530 or contact KMC by email at breachinfo@kernmedctr.com.

A resident physician printed out the records of 1,500 patients for research purposes. The paper records were stored in a computer bag and the bag was stolen from the physician's car on February 25. The records contained names, health information, and test results. They may have also contained the insurance information of some patients.

UPDATE (4/20/2012): Medical record numbers, dates of treatments, diagnoses sites, cocci clinical numbers, and test results for HIV, AIDS, Hepatitis, and pregnancy may have also been exposed.

Information
Source: PHIPrivacy.net

March 5, 2012  Town of Plainfield Indiana  Plainfield, Indiana  GOV HACK 250 (No SSNs or financial information reported)

A hacker or hackers posted administrator usernames and corresponding passwords, as well as the email addresses of 250 state and Plainfield employees online. Some of the information included addresses, phone numbers, and email passwords, and some information was from employee contacts.

Information
Source: Dataloss DB

March 4, 2012  Cambridge Eastern Education and Development Society (CEEDS)  Seattle, Washington  EDU HACK 13 (No SSNs or financial information reported)

A hacker or hackers accessed and posted the database information of Cambridge Eastern Education and Development Society (CEEDS) online. The leaked data included 12 email addresses and one administrator login and (salted) password combination.

Information
Source: Dataloss DB

March 4, 2012  Epson America  Long Beach, California  BSR HACK 66 (No SSNs or financial information reported)

A hacker or hackers accessed and posted the database information of Epson online. The leaked data included 66 administrator user logins and password combinations. Many of the passwords were weak and stored in an easily readable plain-text format.

Information
Source: Dataloss DB

March 3, 2012  University of Washington  Seattle, Washington  EDU HACK 56 (No SSNs or financial aid reported)

A team of hackers revealed that they had attacked the University of Washington's system with multiple SQL injections. The first one was detected and fixed by the University of Washington, but a second one went unnoticed. The team of hackers released 31 login and password combinations from a user database and 25 WordPress user login, password, and email address combinations. The attack comes a few weeks after a hacker identified nearly 20 university systems that were vulnerable to SQLi attacks.
This breach was covered by the media and notifications of this breach were sent in 2009.

A former worker for the Miami-Dade school board misused student information. The dishonest employee worked as a clerk and accessed the student information for the purpose of obtaining fraudulent credit cards with her boyfriend. An unknown number of student Social Security numbers were accessed and used. She was caught in the act of stealing the Social Security numbers in 2009.

The media covered this breach sometime in 2011.

Divine Sports marketed itself as a non-profit that tutored at-risk youth. It appears that the owner of the company billed the Miami-Dade School District for hours of tutoring that never occurred. The company even created reports for students that did not exist by using the information of real students. Hundreds of thousands of dollars may have been fraudulently obtained over multiple years. The fraud was discovered in 2010. Divine is located in multiple states and the corporate office denied any control over the day-to-day operations of Divine Sports in Miami.

Those with questions may visit [http://www.jjtwomeymd.com/index.htm](http://www.jjtwomeymd.com/index.htm)

On September 26, 2011, Hackensack University Medical Center became aware that a dishonest employee had accessed patient information prior to September 1, 2011. A former employee working as a clerk took confidential patient files from an outpatient clinic. The files contained names, Social Security numbers, addresses, dates of birth, driver's license numbers, health insurance cards, and other insurance information. No medical records were taken.

Concerned patients may call 1-855-755-8482 and dial 42250 22112 when asked to enter a reference code.

An employee of BCBS North Carolina accidentally sent an email that revealed the email addresses of all customers who received the email. Customers received the email as notification of changes to their billing cycle on Wednesday, February 29. The employee error meant that anyone who received the email could then send unwanted messages referencing BCBS or unrelated content to other customers who received the email.

A user ID assigned to Independent Capital Management used to access consumer reports was compromised by an unknown individual. New user IDs were assigned and security was increased. The unauthorized access took place sometime between February 13 and February 15.
People who were members of the Transformers Club run by Fun Publications became aware that their credit card information had been compromised. Fun Publications conducted an investigation and determined that their e-commerce database had been compromised sometime around January 31. Members were encouraged to monitor their credit cards closely and to consider replacing any cards that were used with Fun Publications for event registration, club store purchases, or other purchases. One member who used similar login information for both the Transformers Club and PayPal realized that his PayPal account had been compromised.

Two hackers claimed responsibility for hacking the website of the city of Springfield, Missouri. The breach occurred on February 17, and the databases on the server contained over 300,000 entries. It appears that not all databases were accessed as the total number of citizens affected was reported as 2,100. Hackers claimed to have acquired 6,071 entries related to the date of birth, weight, height, race, sex, address, phone number, age, and Social Security number of people listed in online police reports. A total of 15,887 entries related to warrants that included age, date of birth, address, employer, eye color, hair color, race, sex, weight, height, and other details were obtained. Databases with 1,041 vehicle descriptions from online police reports and details related to 284,618 summons were also obtained. The hackers posted a significant amount of information, but voluntarily removed any sensitive information that could cause problems for consumers.

The FBI is investigating an incident that resulted in the information of over 100 law enforcement officers being posted online. Hackers obtained the names, addresses, and phone numbers of officers who are part of the Los Angeles County Police Canine Association (LACPCA). Private emails from officers may have also been obtained.

Documents with names, Social Security numbers, and discharge dates of veterans were discovered unattended in the lobby entrance of Robley Rex VA. An extensive review was conducted by VA officials and they concluded there was no reason to believe any information was misused or that any malicious activity was involved. Neither the reason for the breach nor the details of the breach discovery were revealed.

A miscommunication caused AC LME to lose access to servers containing sensitive health information. An Alamance County employee mistakenly changed a lock on the facility that housed data servers for AC LME. It appears that AC LME forgot to inform the county that AC LME was extending a contract for server maintenance. Former consumers of AC LME, including those who became PBH consumers on October 1, 2011, may have had their personal health information stored on these servers. The servers are now in the possession of the county and could contain the names, Social Security numbers, medical record identification numbers, addresses, and diagnoses of AC LME consumers. LME officials have not had access to the server room without being monitored by a county employee or with the forensics team assigned to examine the servers.
### February 25, 2012

**Wallace Community College**  
**Dothan, Alabama**  
**EDU**  
**HACK**  
284 (No SSNs or financial information reported)

Information from Wallace Community College was posted online by a hacker. The College became aware of the breach after being notified by [Databreaches.net](http://www.databreaches.net). Eight username, email address, and password combinations were posted in addition to 276 username, password, and full name combinations. People who used their same email and password combination for Wallace Community and other sites are encouraged to change their passwords.

**Information Source:** Databreaches.net

### February 25, 2012

**Burger King**  
**Gresham, Oregon**  
**BSR**  
**INSD**  
30

A former Burger King employee used a skimming device to capture customer information. Customers who used their credit cards at the drive-through during the late-night shift had their information copied, sold, and used to make fraudulent purchases. The dishonest employee, the person who misused the data to create forged credit cards, and two others who made fraudulent purchases were all arrested. A total of $14,000 in goods were purchased.

**Information Source:** Databreaches.net

### February 25, 2012

**Weather Shield**  
**Ladysmith, Wisconsin**  
**BSF**  
**UNKN**  
Unknown

A steady flow of employees of Weather Shield have been reporting identity theft in the form of fraudulent tax returns. The company, or one of the company's affiliates that had access to employee financial information, must have experienced some type of breach or breaches. Over 60 employees have discovered that someone had already filed and collected their tax returns. Employees experienced the problem for 2010 and 2011 tax returns, but no one has been charged for the crimes.

**Information Source:** Databreaches.net

### February 24, 2012

**Grimmer Middle School**  
**Schererville, Indiana**  
**EDU**  
**HACK**  
54 (No SSNs or financial information reported)

A hacker or hackers accessed faculty and staff usernames, email addresses, and passwords. The information was then posted online.

**Information Source:** Dataloss DB

### February 24, 2012

**Lake Central Clark Middle School**  
**Saint John, Indiana**  
**EDU**  
**HACK**  
31 (No SSNs or financial information exposed)

A hacker or hackers accessed faculty and staff usernames, email addresses, and passwords. The information was posted online.

**Information Source:** Dataloss DB

### February 22, 2012

**University of Florida**  
**Gainesville, Florida**  
**EDU**  
**DISC**  
719

People who had an unclaimed check or refund from the University of Florida had their Social Security numbers posted on Florida’s Unclaimed Property website. The information had been posted in July of 2005 and is from debts prior to that time, but had been posted through January 12, 2012. The University submitted its Annual Unclaimed Property Report to the Florida State Department of Financial Services. The state accidentally posted the Social Security numbers in addition to the usual information. The University of Florida was the only entity affected by the mistake. Students, employees, and vendors may have been affected.

**Information Source:** Databreaches.net

### February 22, 2012

**DHI Mortgage Company, Ltd.**  
**Austin, Texas**  
**BSF**  
**HACK**  
Unknown
On February 10, 2012, DHI Mortgage became aware that a software security breach by external sources had occurred in its Internet Loan Prequalification System. DHI Mortgage immediately isolated the affected server, purged certain affected files, and modified the electronic security measures. People who provided their information online for pre-qualification may have had their names, Social Security numbers, dates of birth, contact information, marital status, employment information, income, asset information, and liability information exposed.

Information
Source: California Attorney General
February 22, 2012, Coca-Cola Company Family Federal Credit Union, Atlanta, Georgia

The theft of two laptops resulted in the exposure of credit union member information. The laptops were stolen on December 21, 2011 and contained names and Social Security numbers, as well as credit card numbers in some cases.

Information
Source: Dataloss DB
February 22, 2012, Accucom Corporation, Boston, Massachusetts

An unauthorized party misused Accucom credentials to make fraudulent $1.00 charges on customer payment cards that were used on affiliated websites. Credit card numbers, names, and billing addresses may have been accessed. At least 12 New Hampshire residents were affected, but the total number nationwide was not revealed.

Information
Source: Dataloss DB
February 21, 2012, Ochsner Medical Center, New Orleans, Louisiana

Affected patients may call 1 (855) 808-4104.

A hard drive was discovered missing on February 19. It contained patient personal and medical information related to a bone density machine. Medical information, names, dates of birth, addresses, medical record numbers, and medications from patients who had bone density scans between November 2005 and January 2012 were exposed. The hard drive was designed to work with the bone density machine and specialized software would be needed to extract information.

Information
Source: PHIPrivacy.net
February 21, 2012, Ochsner Medical Center, New Orleans, Louisiana

Affected patients may call 1 (855) 808-4104.

A hard drive was discovered missing on February 19. It contained patient personal and medical information related to a bone density machine. Medical information, names, dates of birth, addresses, medical record numbers, and medications from patients who had bone density scans between November 2005 and January 2012 were exposed. The hard drive was designed to work with the bone density machine and specialized software would be needed to extract information.

Information
Source: PHIPrivacy.net
February 21, 2012, Mo’ Money Taxes, Memphis, Tennessee

Thousands of documents with sensitive information were found in a publicly accessible dumpster. An investigation began on February 20 when officers were alerted to three dumpsters filled with documents dating back to 2005. The information included Social Security numbers, driver’s licenses, phone numbers, and addresses. The landlord of the space leased by Mo’ Money appears to have mistakenly cleaned out the office space before Mo’ Money’s shredding service could access the documents. The IRS is now conducting a federal investigation related to identity theft.

Information
Source: Databreaches.net
February 21, 2012, Trident University International, Cypress, California

An unsuccessful attempt to access a database was detected by Trident University on November 29, 2011. It contained usernames and passwords of current and former students. The attempt appeared to be unsuccessful and no other information was contained in the database. Trident University offered credit monitoring services despite the belief that the attempt to access non-financial information had been unsuccessful.
February 21, 2012  
Hagerty Insurance Agency, LLC  
Traverse City, Michigan  
BSF  DISC  Unknown

Those with questions may call 800-922-4050.

An administrative change on www.hagerty.com exposed the personal information of consumers. Names, addresses, driver's license numbers, policy numbers, email addresses, phone numbers, and dates of birth were temporarily available online. The error occurred late in the afternoon of February 14 and was corrected during the afternoon of the following day.

February 21, 2012  
China East  
Wauwatosa, Wisconsin  
BSR  INSD  Unknown

A dishonest employee was caught with a backpack full of customer financial information. A resident reported the employee when he saw someone checking his mail for packages. Police investigated and were able to uncover fraudulent activity. At least 10 purchases were made with customer debit and credit cards between January and February.

February 20, 2012  
Yamaha Commercial Audio Systems  
Colombus, Ohio  
BSR  HACK  1,755 (No SSNs or financial information reported)

A hacker or hackers accessed and posted sensitive information from an official Yamaha music website. A total of eight administrator accounts, as well as 1,755 email addresses and plain-text passwords were exposed.

February 19, 2012  
LABusinessConnect.com, AdultStaffing.com  
Phoenix, Arizona  
BSO  HACK  686 (No SSNs or financial information reported)

A hacker or hackers hacked LABusinessconnect.com with the intention of exposing the company's wrong doings. A database for adultstaffing.com was contained within LABusinessconnect.com. Administrator information from LABusinessConnect.com was posted. A total of 686 usernames, email addresses, and passwords were exposed.

February 18, 2012  
BDO USA, Rubio's Restaurants, Inc.  
San Diego, California  
BSR  PORT  Unknown

BDO was contracted by Rubio's to perform financial auditing services. A BDO employee accidentally removed one or more CD-ROMs from the office. The CD-ROM or CD-ROMs contained a list of Rubio's workers' compensation claimants and a list of people who owned equity shares in Rubio's Restaurants, Inc. The CD-ROM or CD-ROMS appear to have been stolen from the BDO employee's vehicle. The workers' compensation information contained names, claim numbers, medical status, and date of loss. The medical status information included the employees' claim for injuries or illnesses. No Social Security numbers were involved. The partial equity roll list contained names and Social Security numbers.

February 17, 2012  
Islamic Finder  
Anaheim, California  
BSO  HACK  279 (No SSNs or financial information reported)

A hacker or hackers accessed and posted information from islamificfinder.org online. Usernames, names, passwords, and email addresses were exposed.
An unauthorized party or parties used Speedy Recovery Services’ Experian login to view consumer information. The unauthorized access took place between December 12, 2010 and January 21, 2012. Social Security numbers, dates of birth, and account numbers may have been exposed.

Information Source: Dataloss DB

February 16, 2012

Central Connecticut State University (CCSU)
New Britain, Connecticut

A computer breach in a CCSU Business Office exposed the information of current and former faculty, staff, and student workers. A Z-Bot virus designed to relay information was discovered on the computer on December 6, 2011. The computer had been exposed for eight days and only exposed the Social Security numbers of those who were affected. People associated with CCSU as far back as 1998 were affected.

Information Source: Databreaches.net

February 16, 2012

Drago’s Seafood Restaurant
Metairie, Louisiana

A waiter was arrested for using a skimming device to steal customer credit card information. The dishonest employee was linked to two men who were arrested for using the information. The men would purchase electronic equipment with the stolen credit card information and then attempt to resell it for cash.

Information Source: Dataloss DB

February 16, 2012

Horry Telephone Cooperative, Inc. (HTC)
Conway, South Carolina

Those with questions may call 1-855-260-2537.

Unauthorized attempts were made to illegally transfer funds from an HTC bank account between February 1 and February 3 of 2012. The unauthorized party or parties were able to view a limited amount of automated payment records being processed by a third party vendor. Names on customer bank accounts used for automated payments to HTC, customer bank account numbers used for automated payments to HTC, bank routing numbers used for automated payments to HTC, and customer HTC account numbers were exposed. HTC internal databases were not accessed.

Information Source: Dataloss DB

February 16, 2012

D.R. Horton Inc. (DHI Mortgage)
Fort Worth, Texas

A software security incident caused the personal information of mortgage applicants to be exposed. Unknown external sources caused a breach that compromised customer Social Security numbers, dates of birth, income data, and assets and liabilities information. The breach was discovered on February 10 at DHI’s Internet Loan Prequalification System.

Information Source: Dataloss DB

February 15, 2012

Doshi Diagnostic Center
New York, New York

Sensitive documents were placed in public trash bags. The bags were opened and the documents were found scattered across a sidewalk. Confidential patient records which included names, Social Security numbers, unemployment compensation records, copies of benefits cards, and other patient personal information were exposed. Patients dating back to 2006 were affected.

Information Source: PHIPrivacy.net

February 15, 2012

St. Joseph Health System
, California

Patients from the California hospitals St. Jude Medical Center, Mission Hospital, Santa Rosa Memorial Hospital, Petaluma Valley Hospital, and Queen of the Valley were affected. No single California city is listed as the breach location.
Protected patient information may have been available on the internet for one year. A patient's attorney contacted St. Jude officials to inform them that the information was available online. The patient health records included names, body mass index, blood pressure, lab results, smoking status, diagnoses lists, medication allergies, and demographic information such as gender, date of birth, language spoken, ethnicity, and race. The information was removed from online and can no longer be accessed by unauthorized parties. A total of 6,235 patients from Santa Rosa Memorial Hospital, two from Petaluma Valley Hospital, 4,263 from Queen of the Valley in Napa, and an unknown number of patients from St. Jude Medical Center in Fullerton, and Mission Hospitals in Laguna Beach and Mission Viejo were affected.

UPDATE (07/10/2012): The California Department of Public Health was still investigating Queen of the Valley Medical Center as of July 10, 2012. Additionally, two patients who were treated at Santa Rosa Memorial Hospital, filed a class action lawsuit on behalf of the 31,800 patients who were affected. They seek $31.8 million, or $1,000 per patient.

Information
Source: PHIPrivacy.net
February 15, 2012 University of North Carolina at Charlotte
Charlotte, North Carolina
EDU DISC 350,000

UNC-Charlotte will post information about the breach here. Those with questions may also call (855) 205-6937.

An online security breach occurred at the UNC-Charlotte campus and was discovered on January 31. It is unclear how much information could have been accessed. The number of people affected was not revealed. An email alert was sent to students and staff on February 15 in order to inform them that a "potentially significant data exposure of its Information Systems" had occurred. The University also stated that it had corrected the known issues related to the breach.

UPDATE (5/09/2012): Around 350,000 people had their Social Security numbers exposed. Financial information was also exposed. A system misconfiguration and incorrect access settings caused a large amount of electronic data hosted by the University to be accessible from the Internet. One exposure issue affected general University systems over a period of about three months. A second exposure issue affected the college of engineering systems for over a decade.

Information
Source: Databreaches.net
February 14, 2012 Solitude Mountain Resort
Salt Lake City, Utah
BSO HACK Unknown

Hackers stole credit card information during an attack on Solitude Mountain’s credit card system. The breach was short-lived and a small, but undisclosed number of people saw fraudulent charges on their credit cards. Anyone who used a credit card at Solitude during the week of February 7 should check their statements for unusual activity.

Information
Source: Databreaches.net
February 14, 2012 Valley National Bank, American Stock Transfer and Trust Company, LLC
New York, New York
BSF DISC Unknown

A mailing error caused 1099 forms to be sent to the wrong addresses on January 17, 2012. Names, tax identification numbers, and addresses were exposed because incorrect or multiple addresses were printed on the forms. Information on stock dividends and phone numbers was also exposed. The error was discovered when some of the forms were returned by the post office as undeliverable.

Information
Source: Dataloss DB
February 14, 2012 American Stock Transfer & Trust Company, LLC, Mesa Royalty Trust
New York, New York
BSF DISC Unknown

A mailing error caused personal information to be exposed. Beneficiary statements containing tax information for 2011 were sent by postal mail on April 2, 2012. The statements were mailed to incorrect addresses and exposed names, home addresses, and tax identification numbers of intended shareholders. The error was discovered on April 6.

Information
Source: Dataloss DB
February 14, 2012 America Stock Transfer & Trust Company, LLC
New York, New York
BSF HACK Unknown

Shareholder 1099 forms were sent to the wrong addresses due to a mailing error. Names, home addresses, and tax identification numbers could have been viewed by incorrect parties. The forms were mailed on January 17 and the error was discovered on January 18.

Information
Source: Dataloss DB
February 13, 2012 City of Rye
Rye, New York
GOV DISC Unknown
An unknown number of employee Social Security numbers were mistakenly disclosed after the City responded to a Freedom of Information law request. The Social Security numbers were included along with payroll data to the entity that requested the information. City officials verified that the information would not be passed on after the breach was discovered.

Information
Source: Databreaches.net
February 13, 2012 Combined Systems Jamestown, Pennsylvania BSR HACK Unknown

A hacker or hackers accessed the Combined Systems website and shut it down. The hackers claim to have struck in honor of the anniversary of the February 14, 2011 Bahrain uprising and to have wiped out the company's web servers. Administrator logins, customer data, and emails were posted online.

Information
Source: Dataloss DB
February 13, 2012 Gossip Girl Providence, Utah BSR HACK

The official fan website for the Gossip Girl TV show was hacked and defaced. Usernames, IDs, emails, and encrypted passwords were posted online. Another hacker followed up on the attack by decrypting many of the publicly posted password hashes.

Information
Source: Dataloss DB
February 13, 2012 Alicare, National Retirement Fund White Plains, New York BSF DISC Unknown

A mailing error caused the Social Security numbers of National Retirement Fund participants to be printed on the outside of a mailed envelope. Names and mailing addresses were also exposed.

Information
Source: Dataloss DB
February 13, 2012 #1 Chat Avenue, Kansas BSO HACK

No city is listed for this organization.

A hacker or hackers accessed and posted online information. A total of 39 administrator and moderator usernames, email addresses, and salted passwords were exposed.

Information
Source: Dataloss DB
February 11, 2012 Manwin Holding SARL (Brazzers) Waltham, Massachusetts BSR HACK

A hacker or hackers were able to access user records from the inactive forum of a website run by Brazzers. A portion of the compromised emails, usernames, and encrypted passwords were posted online.

Information
Source: Dataloss DB
February 10, 2012 Lakeview Medical Center Rice Lake, Wisconsin MED PORT

More than 500 patients of Lakeview Medical Center homecare and hospice programs had their personal information exposed by the theft of a laptop. The laptop was stolen from a car belonging to a Lakeview nurse. It contained names, Social Security numbers, dates of birth, home addresses, medicare ID numbers, and diagnostic information. It is unclear when the laptop was stolen, but the nurse who was involved no longer works for Lakeview.

Information
Source: Dataloss DB
February 10, 2012 Lakeview Medical Center Rice Lake, Wisconsin MED PORT
C.D. Peacock is suing BridgePoint Technologies for faulty IT services. BridgePoint Technologies was hired in August 2009 and in March of 2010, a breach of C.D. Peacock’s virtual private network (VPN) was discovered. The private network was designed to give remote users access to a centralized network. C.D. Peacock was allegedly advised by BridgePoint Technologies to go around the VPN since it could not be fixed. Though BridgePoint Technologies allegedly said that this move would be safe, C.D. Peacock experienced a serious security breach almost immediately. Hackers installed malicious software on its credit card processing system and other network computers in early April 2010. According to the lawsuit, this allowed hackers to “access the confidential personal data and financial information of” C.D. Peacock customers. The stolen data was transferred to the hackers’ remote system. The breach was discovered in August of 2010. BridgePoint Technologies claimed that it had not received a copy of the lawsuit as of February 10, 2012.

A hacker accessed user information on an Intel website through a vulnerability. The hacker had access to credit card data, Social Security numbers, emails, passwords, and other details.

St. Elizabeth’s Medical Center became aware of sensitive paperwork that was found exposed miles away from the medical center’s Brighton campus. St. Elizabeth’s immediately sent someone to recover the documents. It is unclear how the documents ended up in the area and a vendor may have been the source of the breach. The types of information exposed were not revealed.

UPDATE (4/9/12): The total number of patients who were notified is 6,831. The documents contained billing information such as patient names, hospital account numbers, credit card numbers and security codes. The breach was discovered when someone saw the credit card payment receipts of at least five patients flying through a field. There is no evidence that more than five patients were affected, however, it is unclear how those receipts escaped destruction.

UPDATE (7/14/15): “A Massachusetts hospital has agreed to pay $218,400 and implement a corrective action plan to correct deficiencies in its Health Insurance Portability and Accountability Act compliance program under a recently unveiled no-fault resolution agreement with federal officials.”

More Information: http://www.bna.com/hhs-hospital-settle-n17179933667/?elq=a8d4812e425e411...

Receipts, credit card numbers, addresses, phone numbers, and other information were found in an easily accessible dumpster that sat outside the closed fitness center. A local news station was contacted and followed up on the story. The dumpster was removed, but it is unclear if the documents were properly disposed. The news story received attention from the attorney general’s office and Cardinal Fitness may now face a fine of up to $305,000 for dumping the documents.

No city is listed. Board members, members, and organization officers live throughout West Virginia. People in Mobile, Alabama and Texas were also affected.

A hacker obtained and revealed 156 home addresses, phone numbers, cell phone numbers, email addresses, and usernames of police officers associated with the West Virginia Chiefs of Police Association. Retired police chiefs, and every current police chief in West Virginia had their information exposed. The hacker was associated with Anonymous.

UPDATE (08/24/2012): A hacker associated with the attack on West Virginia Chiefs of Police Association and several other law enforcement associations was caught and sentenced to 27 months in federal prison. He was also ordered to pay $14,062.17 in restitution. Alabama Department of Public Safety spreadsheets with information on sex crimes and a database listing descriptions of offenders’ cars were posted online. Over 46,000 citizens in the state of Alabama may have had their names, Social Security numbers, license plate numbers, dates of birth, phone numbers, addresses, and criminal records accessed by hackers who attacked the City of Mobile Police Department. A total of 787 police officer names, usernames, plain text passwords, addresses, and other agency information from The Texas Police Association was
posted online. The Wisconsin Chiefs of Police Association, the Texas Department of Public Safety, the Dallas Police Department, and the Texas Police Chiefs Association also experienced hack attacks.

Information
Source: Databreaches.net

February 8, 2012  Dallas Police Department
Dallas, Texas

Hackers targeted the Dallas Police Department in response to an officer being placed on leave after crashing his vehicle while intoxicated. A total of 21 full names with employee ID numbers and hire dates, as well as 23 user IDs, email addresses, and passwords were posted online by the hackers.

Information
Source: Databreaches.net

February 8, 2012  Wisconsin Chiefs of Police Association
, Wisconsin

No location is listed. Members from across Wisconsin were affected. The contact information city is listed as Shawano, Wisconsin.

Three hackers posted an administrative login and password on a public website. A fourth hacker released three logins and password combinations and 540 email addresses. The fourth hacker did not work with the other three hackers, but posted the information on the same day.

Information
Source: Databreaches.net

February 8, 2012  Eaton Vance Management
Boston, Massachusetts

A mailing error caused the Social Security numbers of some employees to be visible through the window of mailed envelopes. The employee stock and tax documents were mailed on January 25, 2011 and notification was posted on February 6.

Information
Source: Dataloss DB

February 8, 2012  Indianapolis Super Bowl (indianapolissuperbowl.com)
Indianapolis, Indiana

A hacker or hackers accessed and posted information from indianapolissuperbowl.com. In addition to 10 administrator accounts, 2,016 usernames, email addresses, and cell phone numbers were publicly posted.

Information
Source: Dataloss DB

February 8, 2012  Internet Marketing Strategies (Internet Marketing Tools), Power-blog.com
Tampa, Florida

A hacker or hackers accessed and posted information from the Internet Marketing Strategies website Power-blog.com. Emails, usernames, and encrypted passwords were exposed.

Information
Source: Dataloss DB

February 7, 2012  Department of Child Services
Avon, Indiana

The office burglary during the weekend of February 4 resulted in the theft of 10 encrypted laptops. The laptops had other safeguards as well as encryption codes. Additional items were stolen. The types of confidential and personal client information that were on the computers were not disclosed, nor was the possible number of people affected.
February 7, 2012  Valencia College
Orlando, Florida

An Excel spreadsheet with student names, addresses, dates of birth, and college ID's was listed online on a password-protected website. The password protection eventually expired and anyone could access the information online. Valencia College hired an unnamed contractor to create a custom page for prospective students to communicate with the college. The contractor then hired an unnamed sub-contractor to work on some of the website. The breach can be linked to that unnamed sub-contractor.

February 7, 2012  David Yurman (Yurman Design, Inc.)
New York, New York

Yurman mailed some 1099 forms to the wrong addresses. Names, tax information, and Social Security numbers were exposed.

February 6, 2012  Office of Robert S. Smith, M.D., Inc.
Atlanta, Georgia

Those with questions may call the Lab Management at 1-888-263-0388.

February 6, 2012  Molina Healthcare of California
Long Beach, California

An unauthorized disclosure of paper documents occurred on January 31, 2011. The breach may have affected records that date from September 23, 2009 through October 18, 2011. No further details are available.

February 6, 2012  Smile Designs
Wellington, Florida

The theft of a computer on or around December 1, 2011 resulted in the exposure of personal information.

February 6, 2012  Foundation Medical Partners
Nashua, New Hampshire

A total of 771 patient records may have been exposed as a result of a breach that occurred on November 19, 2011. No further details were disclosed.
February 6, 2012  
**Muskogee Regional Medical Center**  
Muskogee, Oklahoma  

**844** (No SSNs or financial information reported)

Patients with questions may call 1-800-722-9608 between December 2011 and March 2012.

A binder containing forms with flu test results for 2011 went missing sometime around December 5, 2011. It contained the information of patients who received a flu test between January 1, 2011, and December 5, 2011. Patient names, internal hospital department and internal account numbers, gender, medical record numbers, dates of birth, age, dates of tests, and flu test results.

February 6, 2012  
**Concentra Medical Center, Concentra Health**  
Springfield, Missouri  

**870**

Patients with questions may email privacyoffice@concentra.com or call 1-800-819-5571.

An office burglary resulted in the theft of an unencrypted laptop. It contained the names, Social Security numbers, and pre-employment work-fitness tests of Concentra patients from the Springfield area. The Concentra Springfield Medical Center will not encrypt all equipment as a result of this breach.

UPDATE (4/22/2014): Concentra agreed to pay OCR (Office of Civil Rights) $1.7 million dollars for several data breaches that occurred in both Texas and Missouri. The OCR found that "Concentra previously had recognized security risks caused by a lack of encryption on some of its technology. However, OCR said steps to encrypt the technology were "incomplete and inconsistent over time".

The OCR also found that "the company did not have sufficient security management measures in place to protect patient health information".

February 4, 2012  
**Triumph LLC**  
Raleigh, North Carolina  

**2,070** (No SSNs or financial information reported)

A laptop with Triumph client and family member information was stolen on December 13. The office burglary was committed by three men. Two of them distracted the receptionist while the third entered a hallway and stole the laptop. People in Davie, Forsyth, and Stokes counties were affected. The laptop contained spreadsheets with names, dates of birth, medical record numbers, insurance numbers, and Medicaid numbers. Notifications went out on February 2 after it was determined that the laptop would most likely not be recovered.

February 3, 2012  
**Salt Like City Police Department**  
Salt Lake City, Utah  

**1,073** (No SSNs or financial information reported)

Hackers obtained police officer and non-police related civilian information from the Salt Lake City Police Department. The attack was in response to a proposed Utah bill that would have criminalized the possession of graffiti tools with the intent to deface property. The hackers did release the names, phone numbers, usernames, titles, email addresses, and hashed passwords of over 1,000 police officers. The information of civilians was never released and the hackers eventually deleted their copies. The never released data was from people who had provided crime tips or other information to the Salt Lake City Police Department.

UPDATE (06/12/2013): A member of Anonymous was charged in 2012 for using SQL injections on multiple law enforcement and public agency websites. He agreed to a plea bargain in April and will serve 36 months in prison for violating a section of federal law addressing computer fraud. He will also pay nearly $230,000 in restitution to a number of agencies that were hacked.
A printing error caused thousands of taxpayers to receive 1099-G forms from 2011 with the Social Security number and tax refund of another taxpayer. The mistake occurred because the company was trying to conserve paper. The forms were supposed to be cut below a certain point, but the bottom half remained attached.

**Information**

**Source:** Databreaches.net

February 3, 2012 **Motorola Mobility, Inc.**

Libertyville, Illinois

BSR DISC 100 (Unknown number of financial records and SSNs involved)

Customers who purchased a refurbished Motorola XOOM Wi-Fi tablet from Woot.com between October and December 2011 are encouraged to visit motorola.com/xoomreturn or to call Motorola Mobility Customer Support at 1-800-734-5870 (Option 1) in order to determine if their tablet is affected.

Approximately 100 out of a batch of 6,200 refurbished Motorola XOOM Wi-Fi tablets were sent to new customers without being completely wiped by Motorola. The affected tablets were resold by Woot.com between October and December 2011. Previous owners may have stored user names, passwords, email addresses, videos, photographs, and documents on the tablets. There is also a possibility that any password-protected sites and applications could be accessed by people who bought the device refurbished. Any customers who purchased and returned the tablet between March and October of 2011 are eligible for two-years of paid credit monitoring services if both transactions took place at Amazon.com, Best Buy, BJ’s Wholesale, eBay, Office Max, Radio Shack, Sam's Club, Staples, or a few other independent retailers. Those users are also encouraged to change email passwords, social media passwords, and any passwords used to access sensitive applications on the tablet. Additionally, customers who purchased the refurbished tablets and discover that there is information from a previous user may mail the device back to Motorola for free, have the device reset, and receive a $100 American Express gift card.

**Information**

**Source:** Databreaches.net

February 3, 2012 **Patriot Self Storage (CubeSmart Management, LLC)**

Boston, Massachusetts

BSR PHYS Unknown

Files containing customer lease documents were discovered missing. The information was several years old and included customer names and addresses. Drivers’ license numbers and Social Security numbers may have also been exposed.

**Information**

**Source:** Dataloss DB

February 3, 2012 **American Third Position (A3P)**

Las Vegas, Nevada

NGO HACK Unknown

Activists who use hacking (hactivists) targeted several American White supremacist groups. A partial list of officers, political candidate information, financial data, and other member information was exposed.

**Information**

**Source:** Dataloss DB

February 3, 2012 **Metro Community Provider Network**

Denver, Colorado

MED HACK 2,000 (No SSNs or financial information reported)

Hackers were able to access patient names, phone numbers, dates of birth, Metro Community Provider Network internal account numbers, and medical conditions through phishing emails sent to several Metro Community Provider Network employees. Employees received an email that appeared to be from a trusted source and contained a link. Multiple employees clicked the link, which then asked for their email login information. The breach was detected on the same day that it occurred, December 5th, 2011.

**Information**

**Source:** PHIPrivacy.net

February 2, 2012 **Flores Mexican Restaurant**

Lakeway, Texas

BSR HACK 50

Over 50 people who ate at Flores’ were victims of fraudulent credit card activity. The damages total nearly $50,000. Hackers used a computer virus to infiltrate Flores’ credit card system in December. The owner noticed a drop in business of 15 percent after the breach was disclosed.

**Information**

**Source:** Databreaches.net
A Staples cashier is accused of using a skimming device to obtain the credit card information of customers. She is also accused of selling the numbers to another party. A total of $181,000 in fraudulent credit card purchases resulted from the breach. The dishonest employee faces two felonies for criminal possession of a forgery device and first-degree scheme to defraud. She also faces 50 counts of unlawful possession of personal identification and 50 counts of petite larceny.

Information
Source: Databreaches.net
records from this breach used in our total: 50

VeriSign was hacked repeatedly in 2010. The hackers stole undisclosed information. VeriSign is responsible for the integrity of web addresses ending in .com, .net, and .gov. If hackers were able to obtain certain information, it is possible that .com, .net, and .gov websites could be imitated more easily. Hackers may be able to direct people to faked websites and intercept email from federal employees or corporate executives using the .gov addresses. VeriSign officials do not believe that the attacks breaches the servers that support the Domain Name System network, but did not reveal many details about the breach. VeriSign offers a number of services that defend customer websites from attacks and manage website traffic. VeriSign also researchers international cybercrime groups. The security staff responded to the attack quickly, but the breach was not disclosed throughout the company until September 2011.

Information
Source: Databreaches.net
records from this breach used in our total: 0

A hacker or hackers accessed and posted the information from a public Syracuse Police Department website. The usernames and plain text passwords of 39 police officers were exposed.

Information
Source: Dataloss DB
records from this breach used in our total: 0

A hacker or hackers accessed information from Greene County's web server. Names, email addresses, user names, and passwords may have been compromised. Users who registered the same username, email address, and password combination for other accounts are encouraged to change those passwords as well.

Information
Source: Dataloss DB
records from this breach used in our total: 0

A former employee was able to access the Segmark Solutions computer system. It is unclear if the former employee guessed passwords, used passwords that had not been changed, or used some other method to access the computer system. He then used credit card information in the system to make fraudulent purchases. Damages caused a total of $7,000. The former employee was caught after a six-month investigation and charged with second degree computer crime and illegal use of credit cards.

Information
Source: Databreaches.net
records from this breach used in our total: 0

Police stopped a high school student and discovered several sheets of papers with student names, dates of birth, and Social Security numbers in a vehicle. It is unclear how the student obtained the printout and she is accused of using the information to file fraudulent federal income tax returns.

Information
Source: Databreaches.net
records from this breach used in our total: 159
The personal information of current and former Regions employees was lost in November after an auditor from Ernst & Young mailed a flash drive and decryption code. The envelope arrived with the decryption code, but no flash drive. The data included information related to 401k retirement plans. Names, Social Security numbers, and possibly dates of birth were on the flash drive. Regions employs about 27,000 people in 16 states.

Information Source: Databreaches.net

January 30, 2012 University of Miami Miller School of Medicine Miami, Florida

Patients with questions may call (855) 540-4773.

A briefcase containing an unencrypted flash drive was stolen from the vehicle of a University of Miami Miller School of Medicine pathologist on November 24, 2011. It contained the names, medical record numbers, ages, sexes, diagnosis information, and treatment information of patients who had specimens reviewed by the department of pathology between 2005 and 2011.

Information Source: PHIprivacy.net

January 30, 2012 Lexington Clinic Lexington, Kentucky

Concerned patients may call 1-877-851-2562 or (859)-258-5888 locally.

A December 7 overnight office burglary resulted in the theft of a laptop with patient data. It contained names, contact information, and diagnoses of patients receiving services within the neurology department. The locks to the neurology department were changed after the theft was discovered.

Information Source: PHIprivacy.net

January 30, 2012 TryMedia (TM Acquisition) Seattle, Washington

Try Media's ActiveStore application was attacked by intruders who were able to intercept and obtain the credit card information of customers. Credit card numbers, expiration dates, security codes, addresses, email addresses, and passwords to user accounts for transactions that occurred between November 4, 2011 and December 2, 2011 were accessed.

Information Source: Databreaches.net

January 29, 2012 Palos Verdes High School Palos Verdes, California

Three students were caught selling quiz answers to students. It was discovered that they had stolen and copied a master key from the janitor’s office. They then used the copy of the master key to install keylogging hardware onto the computers of four teachers. The keylogging hardware revealed passwords, which were then used to access the central files of the school network. It is unclear what types of information the students had access to. They used their access to electronically change their grades slightly. The master key copy was also used to access 20 paper tests before they were given. A student who became aware of the black market for quiz materiala reported the students.

Information Source: Databreaches.net

January 28, 2012 Oldendorf Medical Services Albany, New York

An office burglary on or around January 18 resulted in the theft of two laptops. The laptops contained the records of about 640 patients and had been used for cardiac tests. Though the laptops contained minimal clinical data, they did contain some Social Security numbers and demographic information.

Information Source: PHIprivacy.net
January 28, 2012  Naperville Unit District 203  Naperville, Illinois  

The report cards of 101 high school students were accidentally sent to the person listed as their emergency contact. A vendor made an unauthorized change to the computer program that generates report cards. If a parent had a high school student attending the district and was listed as an emergency contact for another high school student, then they received two report cards. Parent names were listed on the report cards of each student, but parents listed as emergency contacts mistakenly received the report cards anyway. No Social Security numbers were exposed. Student ID numbers, schedules, and grades were exposed.

Information  
Source:  Databreaches.net  

January 27, 2012  Preferred Skin Solutions  Tulsa, Oklahoma  

An office burglary that occurred on or around January 24 resulted in the loss of a laptop. The laptop held client records. The company sent a breach notification through Facebook and email. No financial information was on the laptop, but Preferred Skin Solutions still warned their clients about the risk of identity theft.

Information  
Source:  PHIPrivacy.net  

January 27, 2012  President’s Challenge, Indiana University  , Indiana  

A security breach caused the personal information of 650,000 President’s Challenge participants nationwide to be exposed. Hackers may have accessed participant names, email addresses, dates of birth, and nutritional data. People throughout Indiana University were participating in a Health IU fitness inter-campus competition. No financial information was available to the hacker or hackers. A small percentage and unknown number of Social Security numbers may have been available through other organizations that participate in President’s Challenge programs. It is unclear how many other organizations were affected by the President’s Challenge hack.

Information  
Source:  Databreaches.net  

January 27, 2012  Sequoia Hospital, Towers Watson  San Mateo, California  

An employee of Towers Watson posted unspecified personal information of current and former Sequoia Hospital employees online in October of 2007. Towers Watson is a Sequoia Hospital contractor. The types of information that were posted were not disclosed, but full names and Social Security numbers were included. The information remained online until December 2 of 2011.

Information  
Source:  Databreaches.net  

January 27, 2012  Craigslist  Hempstead, New York  

More than 250 people in 30 states were victims of scams perpetrated on Craigslist.com by two New York residents. The women posted phony Craigslist ads for nonexistent jobs and apartments to gather the personal information of victims between February of 2010 and October of 2011. That information was then used to obtain fraudulent state income tax returns, bank loans, and credit cards. More than $75,000 was fraudulently obtained. Early in 2011, workers in the Buffalo office of the state Department of Taxation and Finance discovered that hundreds of state tax refunds were being claimed from only about 10 addresses in the county. The two women were indicted by a grand jury on grand larceny and scheme to defraud charges. The women face up to 15 years in prison if convicted.

Information  
Source:  Databreaches.net  

January 27, 2012  Windstream  Kannapolis, North Carolina  

A concerned neighbor noticed that packages were being delivered to an abandoned house. Law enforcement confronted a man who was collecting the packages and found that he had stolen old Windstream customer files and used the information to open fraudulent accounts with online retailers. The man was an employee of Windstream and had taken paper documents from the mid to late 1990s. A second vacant home that served as a delivery location was also found. The former employee was charged with felony identity theft.

Information  

351
Bamastuff.com notified its customers that a breach in its database had been discovered. Customer names, email addresses, billing and shipping addresses, telephone numbers, credit card information, and/or cryptographically scrambled passwords may have been exposed. Customers who bought items between August 1, 2009 and January 16, 2012 may have been affected. Some customers have already experienced fraudulent charges.

City of Point Pleasant notified its customers that a breach in its database had been discovered. Little is known about the breach, though it is believed to have originated from an outside source.

Metropolitan Life Insurance Company (MetLife) of Connecticut notified its customers that a breach in its database had been discovered. MetLife paid an additional $10,000 for a special fund that will reimburse the state of Connecticut’s investigative and enforcement costs, or reimburse losses for consumers in the future. Additionally, customers who paid for a security freeze to be lifted or placed will be eligible for reimbursement and Metlife agreed to improve employee personal information protection training policies and procedures.

New York State Electric & Gas (NYSEG), Rochester Gas and Electric (RG&E), Iberdrola USA notified its customers that a breach in its database had been discovered. An employee at a software development consulting firm that was contracted by Iberdrola USA, the parent company of both NYSEG and RG&E, allowed the information systems of clients to be accessed by an unauthorized party. Customer Social Security numbers, birth dates, and in some cases, financial institution account numbers were exposed. A total of 878,000 NYSEG customers and 367,000 RG&E electricity customers were affected. An unknown number of additional customers from both companies who signed up for gas services, but not electricity services were also affected.

UPDATE (07/12/2012): The Department of Public Service reviewed the NYSEG/FG&E incident and concluded that there was no evidence that any confidential customer information was misused. In addition, the Department of Public Service recommended that both companies further refine their policies, processes, and procedures regarding confidentiality safeguards. The companies were ordered to send plans for handling the costs incurred in responding to the breach and progress reports about the implementation of recommendations.
Between 400 and 450 medical records were stolen from a chiropractic clinic during a January 2 burglary. Files for patients with last names ending in DOD through DRI; ending in ELL through GAT; and ending in GIF through HAL and who had been to the clinic since January 1, 2008 were taken.

**Information**
**Source:** PHIPrivacy.net

**January 20, 2012 Ayuda Medical Case Management Castrovile, Texas**

Thousands of patient records were found in an unsecured trash can. They contained names, Social Security numbers, addresses, phone numbers, medical conditions, and treatment information. The boxes of medical records were traced to Ayuda, whose owner claimed to have been doing little or no business after losing a state contract in September. The boxes were auctioned off after the owner failed to pay the rental fee on a storage unit.

**Information**
**Source:** PHIPrivacy.net

**January 20, 2012 Kansas Department of Aging Wichita, Kansas**

Paper files, a laptop, and a flash drive were stolen from an employee's vehicle in Wichita. A total of 100 seniors who participated in the Senior Care Act program had their Social Security numbers exposed. An additional 7,000 seniors who participated in the Older American Act program including Meals on Wheels had personal information other than Social Security numbers stolen. This personal information may have included full names, addresses, birth dates, gender, Medicaid identification numbers, case manager name and case manager telephone number.

**Information**
**Source:** Databreaches.net

**January 20, 2012 Arizona State University (ASU) Tempe, Arizona**

ASU online system users with questions about logging into their accounts may call (855) 278-5080.

ASU shutdown its online computer system after discovering a breach. An encrypted file containing user names and passwords was downloaded on Wednesday, January 18 by an unauthorized party. All online services were suspended until the night of Thursday, January 19. Students and staff will be required to enter new passwords to access their accounts since there is a chance that some information could have been compromised.

**Information**
**Source:** Databreaches.net

**January 20, 2012 Ward's Nursery & Garden Center Great Barrington, Massachusetts**

Customers who used debit or credit cards at Ward’s Nursery and Garden Center may have had their information taken. Dozens of people from various banks reported fraudulent activity on their cards and Ward’s Nursery and Garden Center appears to be a common link. Reports of fraudulent activity date back to December and people who visited Ward’s Nursery and Garden Center are urged to check their cards for fraud until the breach is determined.

**Information**
**Source:** Databreaches.net

**January 20, 2012 Department of Veterans Affairs, Ancestry.com Washington, District Of Columbia**

VA officials gave veteran Social Security numbers, names, and possibly other information to Ancestry.com in March of 2011 in response to a Freedom of Information Act request from the genealogy site. The records should have only contained the information of deceased veterans, but instead contained the information of over 2,200 living veterans. The information was then posted in 2011 and taken down in January of 2012.

**Information**
**Source:** Databreaches.net

**January 20, 2012 DreamHost Brea, California**

353
Customers were told to login and change all passwords after unauthorized activity was detected on a database. There was no evidence initially that customer passwords were taken, but customer passwords were immediately reset after the discovery.

**UPDATE (2/07/2012):** Hundreds of PHPs (Personal Home Page) have been created in order to redirect users to work-at-home scams. The Russian scam page tricks users into buying a starter kit for a phony internet-based job. Though Dreamhost took steps to ensure that user web pages could not be stolen by resetting the FTP and shell access passwords of all customers, a number of websites hosted by the company have been hijacked to redirect users to the scam page. An analysis of some of the compromised web pages revealed that the January 20 DreamHost breach may not have been what allowed hackers to access the pages. Hackers had installed backdoor PHP scripts in order to access the pages on December 26.

**Information Source:** Databreaches.net

**January 16, 2012**  
**T-Mobile**  
**Bellevue, Washington**  
BSR HACK  
44 (No SSNs or financial information reported)

A hacker or hackers accessed and posted online information. A total of 44 employee names, email addresses, phone numbers, and passwords were exposed.

**Information Source:** Dataloss DB

**January 15, 2012**  
**Zappos.com**  
**Las Vegas, Nevada**  
BSR HACK  
24 million (No financial information or SSNs reported)

Customers with questions about their Zappos passwords may email passwordchange@zappos.com

Customers were informed that their customer account information on Zappos.com may have been illegally accessed by unauthorized parties. Customer names, email addresses, billing and shipping addresses, phone numbers, final four digits of credit card numbers, and/or cryptographically scrambled passwords were linked to customer accounts and could have been obtained. The secure database that stores detailed credit card and payment information was not affected by the breach or accessed. Since passwords may have been affected, customers should change their passwords and make sure that their old Zappos.com password is not used for any other sites.

**UPDATE (1/21/2012):** A resident of Texas is suing Zappos.com and Zappos' parent company Amazon.com on behalf of millions of customers who were affected by the release of personal account information. The lawsuit is being filed in Kentucky.

**UPDATE (9/22/2014):** A federal judge has denied a motion by Zappos to dismiss a class action lawsuit for a breach of customer data in 2012. Reportedly, the parties are nearing a settlement.


**Information Source:** Databreaches.net

**January 13, 2012**  
**City College of San Francisco**  
**San Francisco, California**  
EDU HACK Unknown

The College's electronic systems have been affected by a series of dangerous viruses since 1999. The problem was noticed in 2012 when the College's data security monitoring service detected an unusual pattern of computer traffic. Further investigation revealed that servers and desktops had been infected across administrative, instructional, and wireless networks. Officials believe that it is likely that using a flash drive to transmit information between a campus computer and a personal computer resulted in exposed personal information. It appears that the viruses searched and transmitted data to sites in Russia, China, and at least eight other countries. Banking information and any other personal information that may have been accessed by visitors, students, staff, and faculty on campus computers between 1999 and January of 2012 could have been exposed.

**Information Source:** Databreaches.net

**January 12, 2012**  
**Chesapeake Wound Care Center**  
**Gambrills, Maryland**  
MED INSD 200

A podiatrist licensed in the state of Maryland operated a podiatry practice called Chesapeake Wound Care Center from his home. Between April 1, 2002 and October 11, 2004, he submitted 80 fraudulent claims to Medicare for podiatry services that had not been performed at nursing facilities. The podiatrist signed a Settlement Agreement with the government on October 30, 2007 after being caught, but then fraudulently billed Medicare advantage plans between October 31, 2007 and July 20, 2010. The podiatrist admitted to submitting false bills for podiatry care by misusing the names and personal information of about 200 nursing home patients. He was subsequently charged with health care fraud and aggravated identity theft. He was sentenced to 54 months in prison, three years of supervised release, and ordered...
to pay $1,122,992.08 in restitution for the fraudulent billing of Medicare.

Information
Source: PHIPrivacy.net

January 12, 2012 Rite Aid Corporation
Harrisburg, Pennsylvania

The misplacement of paper documents resulted in the exposure of health and/or other personal information. The breach was discovered on October 7, 2011.

Information
Source: HHS via PHIPrivacy.net

January 12, 2012 Open MRI of Chicago, Nation Wise Machine Buyers
Chicago, Illinois

The improper disposal of paper documents resulted in the exposure of health and/or other personal information. The breach was discovered on September 6, 2011.

Information
Source: HHS via PHIPrivacy.net

January 12, 2012 FileDen
Palo Alto, California

A hacker or hackers accessed and posted online information from the popular file sharing website. A total of 4,504 usernames, passwords, and email addresses were exposed.

Information
Source: Dataloss DB

January 11, 2012 Advanced Occupation Medicine Specialists (AOMS)
Bellwood, Illinois

Patients with questions may call the AOMS security-breach hotline at 855-684-6179 to receive additional instructions and information. Letters dictated by AOMS providers were accidentally uploaded onto a non-secure server in Europe. The information then became publicly searchable via internet. AOMS learned of the breach on October 12, 2011. People who were seen at AOMS for injuries and/or work-related examinations from July, 2009 through October 12, 2011 may have been affected by the breach. No names, contact information, personal information, test results, financial information or Social Security numbers were exposed.

Information
Source: HHS via PHIPrivacy.net

January 11, 2012 Vermont Department of Taxes
Montpelier, Vermont

The Vermont Department of Taxes website accidentally displayed the Social Security numbers of 1,332 individuals and the federal ID numbers of 245 businesses for two hours. The personal data was contained in a weekly group of property transfer tax returns. The three parties who were able to access the information were identified and contacted.

Information
Source: Databreaches.net

January 11, 2012 KCI USA, Inc.
San Antonio, Texas

A portable electronic device was discovered to have been stolen on or around September 8, 2011. The device may have contained health and/or other personal information.
January 11, 2012  **MDwise**  
**Indianapolis, Indiana**

People with Healthy Indiana Plan, Care Select, or Hoosier Healthwise memberships may have been affected.

An upgrade of MDwise’s customer record computer system in February 2011 resulted in the leak of records from several organizations. Anyone searching by name could have accessed the information online. Members of Healthy Indiana Plan, Care Select, and Hoosier Healthwise may have had their names, addresses, Medicaid numbers, and doctors’ names and addresses exposed online. Administrators corrected the error as soon as it was detected.

January 11, 2012  **Virtual Jerusalem**  
**Los Angeles, California**

A hacker or hackers accessed and posted information online. A total of 214 usernames, email addresses, and hashed passwords were exposed.

January 10, 2012  **Isaac Miller Elementary School, Santa Maria-Benita School District**  
**Santa Maria, California**

A man noticed dozens of books and documents inside a dumpster near Miller Elementary. The documents contained personal and financial information related to applications for free and reduced-price meals. The books were new and federally-funded. School officials claimed that the documents should have been shredded and recovered the documents and books. The books were donated.

January 10, 2012  **B-K Lighting**  
**Madera, California**

A hacker or hackers accessed and posted online information. A total of 3,410 names, addresses, usernames, passwords, phone numbers, and email addresses were taken from bklighting.com and exposed.

January 9, 2012  **Employ Bridge (Staffing Solutions), Tempo Real Estate Corporation**  
**Atlanta, Georgia**

Thousands of personal documents were found in a recycling dumpster. The documents likely contained employment information such as full names, addresses, phone numbers, email addresses, and work histories. They were taken from an office in Alpharetta without the company’s knowledge or permission. A landlord with Temp Real Estate Corporation sent a cleaning crew to clean out the office after incorrectly believing Employ Bridge’s lease had expired.

January 8, 2012  **Hydrogen Software**  
**Columbia, Montana**

A hacker or hackers accessed and posted online information. A total of 201 usernames and hashed passwords were exposed.
January 7, 2012  
**Ohio State University Medical Center**  
**Columbus, Ohio**  
MED HACK 180

A hacker or hackers outside of the US attempted to gain access to an OSU Internet server. Information on the server included names, medical record numbers, and diagnoses of 30 patients who visited the pathology department between the late 1980s and 2004. A roster of students who had received training at the medical center in 2006 was also on the server. Officials do not believe that any personal information was taken during the attempt. A total of 30 patients and 150 students were notified.

Information Source: PHIPrivacy.net

January 6, 2012  
**Pure Med Spa, Brite Smile Brite Skin**  
**Las Vegas, Nevada**  
MED PHYS Unknown

A woman alerted a local news station to a stash of improperly disposed information. Credit card applications, patient names, addresses, Social Security numbers, and possibly medical records were found sitting next to a dumpster in a parking lot. The paperwork came from multiple organizations. Among the organizations were two closed branches of Pure Med Spa and Brite Smile Brite Skin.

Information Source: PHIPrivacy.net

January 6, 2012  
**Spotsylvania County**  
**Spotsylvania, Virginia**  
EDU DISC 4,289

An employee discovered that it was possible to access current and former employee W-2 forms online via a Google search. The W-2 form contained employee name, Social Security number, address, earnings, and taxes paid for 2009 and 2010. The discovery was made on December 23 of 2011.

Information Source: Media

January 5, 2012  
**Ochsner Medical Center**  
**New Orleans, Louisiana**  
MED INSD Unknown

A janitor who worked at the Ochsner Medical Center in New Orleans and his girlfriend have pleaded guilty to charges related to stealing patient information for personal gain. The janitor stole printouts containing patient names, Social Security numbers, dates of birth, and other types of personal information. The stolen information was then used by the janitor's girlfriend to open online accounts under the patients' names. The online accounts were used to make thousands of dollars in fraudulent purchases. The date of the breach is unknown, but the janitor was employed between November of 2008 and June of 2009. Federal prosecutors first brought charges in early December of 2011.

Information Source: PHIPrivacy.net

January 4, 2012  
**New York Police Department - 40th Precinct**  
**New York, New York**  
GOV PHYS Unknown

A precinct employee trashed a number of documents after they had been damaged by a flood in the basement of the building. Dumpster divers found the documents and reported that they were readable. The documents, which contained at least one domestic violence report, stolen property records, criminal complaints, and mug shots, were then recovered, secured, and presumably shredded.

Information Source: Databreaches.net

January 4, 2012  
**SF Fire Credit Union, Pacifica-Coastside Credit Union**  
**San Francisco, California**  
BSF PORT Unknown

Those with questions may call 1-888-499-FIRE (3473).

The December 29, 2011 theft of a laptop from a parked car in San Francisco resulted in the loss of personal information. The information was being used in preparation for a merger between SF Fire Credit Union and Pacifica-Coastside Credit...
Union. Current and former account holders had their names, Social Security numbers, dates of birth, addresses, and Pacifica-Coastside Credit Union account information.

**Information**  
**Source:**  
California Attorney General

**January 3, 2012**  
**Department of Social Services Supplemental Nutrition Assistance Program**  
**Hartford, Connecticut**  
GOV DISC 130

A subpoena by the Department of Social Services revealed the names and Social Security numbers of multiple people. The subpoena was in response to reports that state employees had engaged in food stamp fraud. Instead of separate subpoenas for each individual, a sheet with 40 names and a sheet with 90 names were sent. This allowed state employees who are under investigation to learn that their fellow employees were under investigation, as well as their Social Security numbers.

**Information**  
**Source:**  
Media

**December 31, 2011**  
**California Statewide Law Enforcement Association (CSLEA)**  
**Sacramento, California**  
GOV HACK Unknown

Hackers exposed the email addresses, passwords, and names of CSLEA members. The passwords were encrypted, but were posted in their decrypted form. If anyone used the same password and email combination for CSLEA and other websites, they should immediately change their password for those other websites. Anonymous/AntiSec/LulzSec posted the information online.

**UPDATE** (1/04/2012): CSLEA became aware of the issue in early November. Old credit card information and corresponding home addresses for orders from the CSLEA online store were also obtained. Though the ordering process and encryption of credit card information were eventually taken over by Wells Fargo Bank, the card info was inadvertently placed back onto the CSLEA server when the web hosting service restored the site from an earlier version. It is unclear how old the credit card information was. CSLEA attempted to prevent hackers from accessing information after the November breach, but Anonymous was able to get past new passwords, obtain information, and release it around December 31.

**Information**  
**Source:**  
Databreaches.net

**December 31, 2011**  
**New York State Association of Chiefs of Police**  
**Schenectady, New York**  
GOV HACK Unknown

Member email addresses, passwords, and names were exposed by hackers. The passwords were encrypted, but were posted in their decrypted form. If anyone used the same password and email combination for CSLEA and other websites, they should immediately change their password for those other websites. Anonymous/AntiSec/LulzSec posted the information online.

**Information**  
**Source:**  
Databreaches.net

**December 30, 2011**  
**United Airlines**  
**Chicago, Illinois**  
BSO DISC 20 (No SSNs or financial information reported)

A customer checking frequent flyer miles on United Airlines’ mobile website was able to view the names, Mileage Plus numbers, future flight itineraries with confirmation codes, and previous trips of other Unite Airlines customers. The information could have allowed anyone to change another passenger’s seating assignment or cancel a flight by using confirmation codes and last names.

**Information**  
**Source:**  
Databreaches.net

**December 30, 2011**  
**Care2.com**  
**Redwood City, California**  
BSR HACK Unknown

On December 27, Care2 discovered that their website had been breached. Hackers accessed member login information. Care2 emailed new passwords once members had logged into their accounts. Members should change the passwords of any accounts that share the password that was previously used on Care2. Though Care2 has 17,900,617 members, a “limited number” were affected by the breach.

**Information**  
**Source:**  
Databreaches.net

**December 28, 2011**  
**Automatic Data Processing (ADP), A.W. Hastings’**  
**Westlake Village, California**  
BSO PORT Unknown

On November 12, 2011, an encrypted laptop was stolen from the home of an ADP associate. The laptop was encrypted
and password-protected. It contained files with the personal information of A.W. Hastings & Co. employees which had been given to ADP for payroll processing. Names, Social Security numbers, and addresses may have been exposed.

Information Source: Databreaches.net

December 28, 2011
Aegis Science Corporation
Atlanta, Georgia

BSO PORT 2,184 (No SSNs or financial information reported)

A laptop and external hard drive containing patient information were stolen from a locked vehicle owned by an Aegis employee on November 22, 2011. The external hard drive contained names and Social Security numbers. It may have also contained driver’s license numbers, dates of birth, and phone numbers. Though Aegis provides lab tests, results and medical records were not exposed.

Information Source: Databreaches.net

December 28, 2011
Guide Publishing Group, GuideYou.com
San Francisco, California

BSO HACK 11

An unknown number of people were affected by the breach nationwide. Guide Publishing Group reported that 11 people in the state of New Hampshire were affected.

Hackers inserted code onto the server that hosts GuideYou.com and accessed customer credit card numbers. The CVV2/CVV2/CID codes, customer names, and addresses associated with the credit card numbers were also accessible through the server. The breach was discovered on October 28, but the malicious code had been present since November 19, 2010.

Information Source: Databreaches.net

December 28, 2011
N/L Entertainment, Alamo Drafthouse Cinemas
Winchester, Virginia

BSO HACK Unknown

Customers who went to Alamo Drafthouse Cinemas may have had their debit and credit card information stolen due to a theft of information from N/L Entertainment. The Bank of Charles Town is suing N/L Entertainment for failing to prevent the theft, which lead to at least 232 fraudulent purchases made using Bank of Charles Town customer debit cards. The Bank of Charles Town is seeking $29,919.74 in damages plus an unspecified amount in interest.

The breach was first noticed and reported to the public in September. Thieves had taken financial information from people who used their debit or credit cards to make transactions between the end of June 2011 to late August of 2011.

Information Source: Databreaches.net

December 28, 2011
Loma Linda Medical University
Loma Linda, California

MED INSD 1,336 (Unknown number of SSNs)

An employee was fired after taking sensitive documents home on or around December 19. Medical records and other documents with patient dates of birth, addresses, driver’s license numbers, medical record numbers, and in some cases, Social Security numbers were removed from the hospital against hospital policy. The records were recovered.

Information Source: PHIPrivacy.net

December 25, 2011
Stratfor.com, Strategic Forecasting Inc.
Austin, Texas

BSO HACK 68,063

Anonymous/#AntiSec has claimed responsibility for the hack of a global intelligence company named Stratfor. Hackers were able to obtain tens of thousands of credit card numbers and other personal information from Stratfor.com. In addition to credit card numbers with security codes, addresses, and names, the hackers obtained 200GB of emails. The hackers also claim to have used the credit card information to make over $1 million in donations to charities. Hackers later revealed that the information was even easier to use since it had not been encrypted. Stratfor took the website down within an hour after it was hacked and defaced, but sensitive information had already been leaked.

UPDATE (1/04/2012): A total of 68,063 unique credit card numbers, 859,311 unique email addresses, 860,160 hashed passwords, 50,569 phone numbers and 50,618 U.S. resident addresses were posted. Of the 68,063 credit card numbers, about 36,000 were not expired.

UPDATE (2/15/2012): Hackers posing as officials from Stratfor have started emailing infected links to government subscribers whose email addresses were stolen during the breach.

UPDATE (2/27/2012): Wikileaks published more than five million emails that were obtained by hackers during the breach. Some of these emails could contain sensitive information that would unmask sources, reveal security information that the intelligence-gathering company had collected, and reveal information about many Fortune 500 companies that subscribe to Stratfor.
UPDATE (5/03/2012): Four Irish and British men were charged for their involvement with Anonymous’s faction Antisec and the Stratfor breach. These men were also charged with involvement in hacks of Fox, Sony Pictures, and the Arizona Department of Public Safety.

UPDATE (7/02/2012): Stratfor agreed to settle a class action lawsuit filed on behalf of customers. Stratfor will offer members of the class action lawsuit one month of free access to its service, worth $29.08, and an electronic book published by Stratfor called "The Blue Book," priced at $12.99. These two offers may cost Stratfor $1.75 million. Additionally, Stratfor agreed to pay for a credit monitoring service for any members of the class action lawsuit who request the service. Stratfor will also pay a $400,000 lump sum for plaintiff attorneys and various fees.

UPDATE (08/11/2012): Emails with data about the implementation of the domestic surveillance program TrapWire were also exposed. TrapWire gathers surveillance data from major cities in the US, encrypts it, and sends it to a secretive central database center.

UPDATE (05/28/2013): A member of Anonymous pleaded guilty to playing a part in hacking Stratfor Global Intelligence Service, Arizona Department of Public Safety, the Boston Police Patrolmen’s Association, the FBI’s Virtual Academy, and the sheriff’s office of Jefferson County, Alabama. His charges are related to stealing emails and credit card data as well as hacking Stratfor and several other websites. He faces up to 10 years in prison and is scheduled to be sentenced on September 6.

UPDATE (11/15/2013): The member of Anonymous was sentenced to 10 years in prison and three years of probation.

Information
Source: Databreaches.net
December 24, 2011 Office of the New York City Public Advocate New York, New York NGO HACK Unknown

The group Anonymous claimed responsibility for hacking and publishing a data base. The database consisted of names, addresses, telephone numbers, email addresses, medical conditions, domestic violence and abuse reports, descriptions of financial hardship, complaints about residential issues, and other very personal details of people who submitted this information via the public advocate’s website. The submissions for assistance date from April 2010.


Information
Source: Databreaches.net
December 23, 2011 Virginia Department of General Services Richmond, Virginia GOV DISC 639

Social Security numbers, tax identification numbers, and other types of personal information were exposed on the Virginia Department of General Services website since 2001. The database was not accessible via search engines, but an employee discovered that the information could be found by anyone doing a focused search on the actual website. The information was removed after the discovery.

Information
Source: Databreaches.net
December 23, 2011 Provo School District Provo, Utah GOV HACK 3,200 (No SSNs or financial information reported)

The email addresses of around 3,200 parents and students were exposed by a computer security breach. The parents and students received an official looking email that linked to a survey about satisfaction with the school district. The survey had not been authorized for release.

Information
Source: Databreaches.net
December 22, 2011 Oahu District Tax Office, State Tax Department Oahu, Hawaii GOV INSD Unknown

Fourteen Department of Taxation employees were placed on administrative leave without pay following the discovery of an internal security breach of the department’s tax database. The breach was found during an audit of the department’s security systems and internal controls. The incidents date from 2008 to present. It is unclear what types of information could have been exposed.

Information
Source: Databreaches.net
December 22, 2011 Good News Garage Burlington, Vermont NGO PORT 14,000 (Unknown number of SSNs)
A November 25 home burglary resulted in the loss of an encrypted data tape. The tape was inside a backpack that was stolen from an employee’s locked car while it was parked at home. The data tape had names, addresses, and in some cases Social Security numbers of Good News Garage donors dating back 15 years.

Information Source: Databreaches.net

December 22, 2011 Pearl River Resort Neshoba, Mississippi BSO UNKN Unknown

A possible breach in the security systems used for processing credit card transactions is being investigated. There is no information on the type of breach or how many customers may have been affected. The cause of the breach is also unknown.

Information Source: Databreaches.net

December 22, 2011 Department of Human Services (DHS) Gateway Center Springfield, Oregon GOV STAT 3,000 (No SSNs or financial information reported)

People who were fingerprinted at The Willamette Street office in Eugene between August 2008 and 2010 may have also been affected.

Those with questions may call 1-855-360-4554, extension 0.

The theft of a computer resulted in the exposure of sensitive information from DHS staff, volunteers, adoptive placements, respite providers, in-home care providers, and foster parents. People who were fingerprinted at The Gateway Center in Springfield, Oregon between August 2010 and December 8, 2011 may have been affected. People fingerprinted at The Willamette Street office in Eugene, Oregon between August 2008 and August 2010 may have also been affected.

Information Source: Databreaches.net

December 21, 2011 Ridgewood Public Schools Ridgewood, New Jersey GOV HACK Unknown

Someone was able to enter a Ridgewood school building through a compromised computer password. The breach was discovered during the week of December 14. It is unclear if a data breach occurred during the incident. Six students have been identified as possible participants in the breach.

Information Source: Databreaches.net

December 21, 2011 St. Charles Bend and Redmond Bend, Oregon MED PORT 140 (No SSNs or financial information reported)

The breach occurred in the city of Bend or Redmond Oregon.

A laptop was stolen from a St. Charles employee's car in late October. It contained the personal information of 140 patients who were seen in the St. Charles Bend or St. Charles Redmond emergency room. The laptop was discovered in brush by an elementary school student in late November. After the laptop was returned on December 16, it was discovered that attempts to gain unauthorized access to its contents had failed.

Information Source: PHIPrivacy.net

December 21, 2011 United States Chamber of Commerce Washington, District Of Columbia NGO HACK 3,000,000 (No SSNs or financial information reported)

Hackers in China were able to breach the computer system of the United States Chamber of Commerce. The hackers had access to the information of roughly three million members from November 2009 to May 2010. Though the breach was discovered in May of 2010, there is evidence that some systems were still compromised in March of 2011. Email communications with no more than 50 of the Chambers’ members were compromised. Company names, key company contacts, trade-policy documents, meeting notes, trip reports, and schedules were in the email communications.
A breach of Butler Schein Animal Health’s (BSAH) systems (MyVetDirect.com) may have affected clients whose veterinarian’s websites were hosted by MyVetDirect.com. People who placed orders on veterinarian websites that were hosted by MyVetDirect.com may have had their names, credit card information and numbers, addresses, telephone numbers, email addresses, billing and delivery information, and other purchase information obtained.

Information Source: Databreaches.net

December 20, 2011

University of Mississippi Medical Center and Mississippi State Department of Health
Jackson, Mississippi

MED PORT 1475 (No SSNs or financial information reported)

Patients may call 1-855-241-2575 or email hipaaprivacy@umc.edu.

Research study participants may have had their personal information exposed by the theft of a laptop. The laptop was stolen when UMMC employees left the laptop unsecured for a short period of time against departmental guidelines. It was reported stolen on October 31, and the employees who left it unsecured were disciplined. Two databases with research related health information were on the laptop. One had the age, sex, race, medical record number, zip code, and lab results of 1,400 patients. The other database contained unspecified protected health information from 75 patients.

Information Source: PHIprivacy.net

December 17, 2011

Office of Paul C. Brown, M.D., P.S.
Renton, Washington

MED PORT Unknown

An October 14, 2011 office burglary resulted in the exposure of patient information dating from 1993 to 2004. Office equipment and CDs with patient information were discovered missing on October 17. Affected patients were mailed notification letters on December 13, 2011 and informed that their names, Social Security numbers, dates of birth, addresses, diagnoses, medical conditions, lab results, medications, surgery records, radiological tests, and other clinical treatment information could have been on the stolen CDs. The office now plans to install encryption technology and update physical security systems in order to protect patient data from more breaches.

Information Source: PHIprivacy.net

December 16, 2011

Restaurant Depot, Jetro Cash & Carry
College Point, New York

BSR HACK 300,000

The location listed is that of Restaurant Depot’s corporate location.

People who shopped at Jetro or Restaurant Depot between September 21 and November 18 may have had their credit or debit card information taken by a hacker. Customer names, card numbers, expiration dates, and verification codes were exposed. The breach investigation began on November 9 when the parent company became aware of customers experiencing card fraud.

Information Source: Databreaches.net

December 16, 2011

Peoples Gas, North Shore
Chicago, Illinois

BSO INSD 100

A contract worker or employee of a contractor may have stolen and misused the personal information of an undisclosed number of customers. The natural gas utilities serve nearly one million customers in the Chicago area, but state law bars the utilities from disclosing the number of customers affected. However, a November news report revealed that the theft of information had occurred in October and over 100 people were affected. An employee working in iQor’s human resources department was linked to the incident. The employee was fired and faces criminal investigation and prosecution.

Information Source: Databreaches.net

December 16, 2011

North Penn School District (NPSD)
Lansdale, Pennsylvania

GOV HACK Unknown

A student is being investigated by the North Penn School District (NPSD) and Towamencin Township Police Department for hacking into the NPSD computer network. Computer devices are being analyzed to determine what types of information may have been accessed. No further information is available due to the ongoing investigation.
People who donated to UJA-Federation may have had their bank account information taken by a dishonest worker. A worker who led a $2 million identity theft ring surreptitiously took pictures of checks given to UJA-Federation during her two years of employment. The dishonest worker also collected donor names, addresses, and account numbers. The information was then sold to other members of the identity theft ring and used to create fraudulent checks and open credit cards. The dishonest worker was fired when the crimes were discovered.

**Jefferson County Public Schools**
Loudon, Kentucky

Around 6,500 ACT Explore test results for 8th graders were mailed to incorrect addresses. The breach was discovered when parents began calling the district. Parents were asked to shred the tests. The exact cause of the mailing error is unknown.

**Trilegiant Corporation**
Stamford, Connecticut

A call center employee who worked for a Trilegiant vendor used his phone to take pictures of customer names and credit or debit card numbers. The dishonest employee was seen doing this at least once, but no misuse of customer information had been reported as of December 14, 2011.

**Mr. Janitor, Eagle Harbor Country Club**
St. Augustine, Florida

The owner of a cleaning company called "Mr. Janitor" was arrested for stealing personal information from Eagle Harbor Country Club members. An unknown number of members had their information stolen and used to open fraudulent credit cards and bank accounts in their names. The owner of the cleaning company was charged with identity theft of more than $50,000 and/or affecting more than twenty persons.

**Fletcher Allen Health Care**
Burlington, Vermont

A physician pleaded guilty to unlawfully obtaining the private medical information of another person. The former employee accessed the records of several women who were not his patients. In one case, he was in a sexual relationship with a woman and accessed her information to check if she carried sexually transmitted diseases. The crime occurred in 2008. The physician is scheduled to be sentenced on March 26, 2012 and faces a maximum sentence of one year in prison and a $50,000 fine.

**Metabasis Therapeutics**
La Jolla, California

A temporary employee of Metabasis Therapeutics was assigned to computer help-desk support in 2008. The dishonest employee somehow obtained unauthorized access to the names and personal-identification information of Metabasis Therapeutics employees and their relatives. The information was used to open credit cards; the credit cards were used to purchase travel packages, which were then resold. A total of $250,000 worth of Las Vegas air, hotel, and show-ticket packages were purchased on Travelocity.com. The former temporary employee was given a four year sentence in federal prison after being convicted for credit card fraud and aggravated identity theft.
Anonymous and AntiSec released FFA information which included 22 email addresses linked to IP addresses of newsletter subscribers, 13 email addresses linked to type of credit card and security code number, and administrator login information which included encrypted passwords. The attack was in response to FFA's successful efforts to pressure Home Depot and Lowe's into removing advertisement on a TLC show called "All-American Muslim." The FFA strongly opposed the idea of having a Muslim family featured in a positive way on TV.

Anonymous also hinted at an attack on Lowe's for caving into the FFA's demands.

Information
Source: Databreaches.net

December 11, 2011  Coalition of Law Enforcement and Retail (CLEAR)
Deerfield Beach, Florida  NGO  HACK
2,400 (No SSNs or financial information reported)

A hacker released member information that had been stored on the CLEAR website. Member phone numbers, residential and email addresses, and place of employment were exposed. Administrator passwords that had easily been decrypted were also released. One person claimed to have used the information to access the email of a police department. The hacker claimed that the attack was a response to the mistreatment of Occupy protesters.

Information
Source: Databreaches.net

December 10, 2011  Office of Gene S. J. Liaw, MD.
Seattle, Washington  MED  PORT  1,105

An unencrypted USB drive was determined to be missing on April 4, 2011. It contained patient names, Social Security number, addresses, phone numbers, dates of birth, diagnosis codes, and insurance information.

Information
Source: HHS via PHIPrivacy.net

Atlanta, Georgia  MED  PORT  884 (No SSNs or financial information reported)

A burglary that occurred on or around April 15, 2011 resulted in the theft of laptop with patient information.

Information
Source: HHS via PHIPrivacy.net

December 9, 2011  Health Care Service Corporation (HCSC)
Chicago, Illinois  MED  PHYS  501 (No SSNs or financial information reported)

The theft of paper records on or around June 28, 2011 resulted in the exposure of patient information.

Information
Source: HHS via PHIPrivacy.net

December 9, 2011  Capron Rescue Squad District
Capron, Illinois  MED  PORT  815 (No SSNs or financial information reported)

Unauthorized access or disclosure of patient information resulted after a breach involving a laptop. The breach was discovered on or around February 5, 2011.

Information
Source: HHS via PHIPrivacy.net

2,334 (No SSNs reported)
The exact location of this breach was not listed. It occurred somewhere in Texas.

On or around June 25, 2011, a breach involving a laptop, a computer, and a network server was discovered. Patient information was exposed as a result of the breach.

Information
Source: HHS via PHIPrivacy.net

December 9, 2011  InStep Foot Clinic
Edina, Minnesota
MED PORT 2,600 (No SSNs or financial information reported)

Electronic medical records may have been exposed as a result of the theft of a laptop on or around August 28, 2011.

Information
Source: HHS via PHIPrivacy.net

December 9, 2011  Centro de Ortodancia
Aguadilla, Puerto Rico
MED PHYS 2,000 (No SSNs or financial information reported)

Paper records were found to have been exposed to unauthorized parties on or around May 6, 2010.

Information
Source: HHS via PHIPrivacy.net

December 9, 2011  Knox Community Hospital
Mount Vernon, Ohio
MED PHYS 500 (No SSNs or financial information reported)

X-ray records were discovered to have been improperly disposed of on or around October 1, 2011. Patient information may have been exposed.

Information
Source: HHS via PHIPrivacy.net

December 9, 2011  Julie A. Kennedy, D.M.D.
West Palm Beach, Florida
MED STAT 2,900 (No SSNs or financial information reported)

A network server was discovered to have been stolen on or around September 30, 2011. It may have contained patient information.

Information
Source: HHS via PHIPrivacy.net

December 9, 2011  Logan County Emergency Ambulance Service Authority (LEASA)
Logan, West Virginia
MED PORT 12,563

Affected patients may call (304) 792-0191 (ext. 201) or email psheppard@leasa.org for more information.

A laptop was discovered missing on October 1, 2011. It was either lost or stolen. It contained names, Social Security numbers, addresses, and health information from patients. The laptop appears to have not been used to connect to the internet since October 1 and LEAS is attempting to block potential use of the device.

Information
Source: HHS via PHIPrivacy.net
CDs with personal information were discovered lost on or around August 24, 2011. Other items with personal information may have been lost as well.

Information
Source: HHS via PHIPrivacy.net

December 9, 2011  Stone Oak Urgent Care and Family Practice
San Antonio, Texas

A computer or laptop was discovered to have been lost or stolen on or around October 23, 2011.

UPDATE (12/28/2011): A total of five computers containing medical and personal information were stolen from a physician’s office during the breach. A thief had pried open an office door during the weekend of October 22-23. Patients were informed on December 5 that their names, Social Security numbers, dates of birth, account numbers, disability codes, and diagnoses were stored on the computers.

Information
Source: HHS via PHIPrivacy.net

December 9, 2011  Amerigroup Community Care of New Mexico, Inc.
Albuquerque, New Mexico

Papers were discovered stolen on or around July 15, 2011.

Information
Source: HHS via PHIPrivacy.net

December 8, 2011  Subway
Milford, Connecticut

Over 150 Subway franchises and at least 50 other small retailers had customer data hacked from their point-of-sale (POS) systems. Four Romanian hackers were indicted for hacking and misusing the credit card information between 2008 and May of 2011. Over $3 million in fraudulent charges on customer cards was obtained by scanning the internet for vulnerable POS systems and then easily breaking the passwords to these systems. Keyloggers and a backdoor were also installed to allow further access to the system. Retailers who were hit had used a certain type or types of basic POS software and many had failed to change the default password for the software.

UPDATE (01/08/2013): A Romanian national was arrested and sentenced for his role in the POS system hack of Subway. Three other Romanians face charges related to the breach.

UPDATE (03/19/2013): The scheme may have affected 150 restaurants and may have led to $10 million in fraudulent charges. Two additional hackers were sentenced on conspiracy to commit computer fraud and conspiracy to commit access device fraud charges.

Information
Source: Databreaches.net

December 8, 2011  Los Angeles Police Department (LAPD)
Los Angeles, California

The personal information of over 24 members of the LAPD’s command staff was posted on a website. Officers had their property records, campaign contributions, biographical information and, in a few cases, the names of their family members posted. This breach appears to be different from the one that affected members of Coalition of Law Enforcement and Retail (CLEAR) on or around December 11.

Information
Source: Media

December 7, 2011  Veterans Administration Medical Center
Miami, Florida

An employee was charged with selling the personal identities of disabled hospital patients. At least 22 military veterans who received services at the VA in Miami had their information sold. The employee was worked at the VA Travel Benefits
Sections and had access to the names, Social Security numbers, addresses, and dates of birth of disabled veterans who had been reimbursed for travel expenses related to their medical treatment. The employee was caught late in 2010 after several veterans complained about unauthorized credit card accounts opened in their names.

Information Source: PHIPrivacy.net

<table>
<thead>
<tr>
<th>Date</th>
<th>Organization</th>
<th>Location</th>
<th>Records from this breach used in our total:</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 7, 2011</td>
<td>Jeanne D'Arc Credit Union</td>
<td>Lowell, Massachusetts</td>
<td>327</td>
</tr>
</tbody>
</table>

A total of 327 New Hampshire residents were affected. The total number of people affected nationwide was not revealed.

An employee took a flash drive with customer information on December 27, 2010. Someone at the former employee's new company noticed that files from Jeanne D'Arc were installed on a computer at the new company. Copies of the files were sent back to Jeanne D'Arc. Jeanne customer names, Social Security numbers, and loan account numbers were exposed.

Information Source: Databreaches.net

<table>
<thead>
<tr>
<th>Date</th>
<th>Organization</th>
<th>Location</th>
<th>Records from this breach used in our total:</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 6, 2011</td>
<td>Massachusetts eHealth Collaborative Waltham, Massachusetts</td>
<td>BSF INSD</td>
<td>14,475 (222 Social Security numbers)</td>
</tr>
</tbody>
</table>

A briefcase was stolen from an employee's car during lunch sometime during the spring of 2011. The briefcase contained a company laptop that had not yet been encrypted and paper copies of appointment schedules. The laptop contained the information of patients and providers from 18 practices. A recent backup of the laptop files revealed that 5,338 subscriber numbers, 2,777 names with no other information, and 222 names with associated Social Security numbers, dates of birth, subscriber numbers, and phone numbers had been on the laptop. Seventy of the 222 who had their names, Social Security numbers, dates of birth, subscriber numbers, and phone numbers exposed also had their addresses exposed.

Information Source: PHIPrivacy.net

<table>
<thead>
<tr>
<th>Date</th>
<th>Organization</th>
<th>Location</th>
<th>Records from this breach used in our total:</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 3, 2011</td>
<td>State of Tennessee Sponsored Group Health Plan Nashville</td>
<td>GOV DISC</td>
<td>1,770</td>
</tr>
</tbody>
</table>

State employees who canceled their health or dental insurance had their information mailed to the wrong address in October. Each mailing included a certificate containing the information of the recipient and three other letters aimed at other members of the plan. Names, Social Security numbers, addresses, employee ID numbers, and healthcare insurance coverage dates were exposed. The error was discovered on October 6, 2011.

Information Source: Databreaches.net

<table>
<thead>
<tr>
<th>Date</th>
<th>Organization</th>
<th>Location</th>
<th>Records from this breach used in our total:</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 3, 2011</td>
<td>Pulaski County Special School District Little Rock, Arkansas</td>
<td>GOV PORT</td>
<td>1,100</td>
</tr>
</tbody>
</table>

A former employee's laptop was stolen during a home burglary sometime in mid November. On November 30, the District learned that the former employee's laptop contained confidential records. Current and former District employees had their names, Social Security numbers and other confidential information exposed.

UPDATE (12/22/2011): It was revealed that a finance director loaded private information onto a personal laptop and took it home to finish work. Though the finance director's last day with the School District was September 2, 2011, the laptop still contained sensitive data when it was stolen on November 11.

Information Source: Databreaches.net

<table>
<thead>
<tr>
<th>Date</th>
<th>Organization</th>
<th>Location</th>
<th>Records from this breach used in our total:</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 3, 2011</td>
<td>Contra Costa County Martinez, California</td>
<td>GOV DISC</td>
<td>Unknown</td>
</tr>
</tbody>
</table>

Patients with questions may call (925)-957-7400.

Residents who owed money to the county health department had their names inadvertently published in a public document. The names were published in a report to the Board of Supervisors dated July 27, 2010. The error was discovered at the end of November, 2011. No patient information was exposed, but the publication of the names in the report constitutes a breach of patient confidentiality laws. The information was removed from the online report.

Information Source: PHIPrivacy.net

<table>
<thead>
<tr>
<th>Date</th>
<th>Organization</th>
<th>Location</th>
<th>Records from this breach used in our total:</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 2, 2011</td>
<td>Transcend Capital Dallas, Texas</td>
<td>BSF PORT</td>
<td>Unknown</td>
</tr>
</tbody>
</table>

A laptop was stolen from an employee's office after a brief absence during working hours at a Dallas branch. The theft occurred on October 31 and those who were affected were notified on November 11. Some affected clients may have had...
their Social Security numbers exposed, but most could have had their names and account numbers exposed. Transcend Capital informed clients that their account numbers would be changed in response to the incident and that their accounts would be monitored for suspicious activity. Transcend Capital also implemented a policy of securing laptops to desks as a result of the breach.

Information
Source: Databreaches.net

December 2, 2011
University of Kansas (KU)
Lawrence, Kansas
EDU PHYS Unknown

Documents containing the personal information of current and former student housing residents was stolen during a burglary at the Department of Student Housing office on November 30. Names, dates of birth, apartment numbers, email addresses, KU ID numbers, and other information, some of it related to student dependents, were on the documents. The number of affected students was not revealed, but those who were affected were told to be cautious of identity theft.

Information
Source: Databreaches.net

December 1, 2011
Extreme Pizza
Omaha, Nebraska
BSR HACK Unknown

Someone hacked into the Extreme Pizza computer system and took information from cards that had been swiped by Extreme Pizza. The thefts date back to September of 2011. Credit card transactions were moved to a different type of card reader in response to the breach.

Information
Source: Databreaches.net

November 30, 2011
The College of New Jersey
Ewing, New Jersey
EDU DISC 12,815 (No SSNs or financial information reported)

The College's On-Campus Student Employment System had a vulnerability that allowed student applicants to see the personal information of other students. A student applicant notified the College of the problem on November 2 after seeing the information of 12 other students. The system flaw was fixed within hours, but no duration was given for the breach.

Information
Source: Databreaches.net

November 29, 2011
University of California Riverside (UCR)
Riverside, California
EDU HACK 5,000

Those with questions may call 1-855-827-2277.

Several customers of the UCR Dining Services location reported fraudulent credit and debit card activity to UCR. On or around November 16, it became clear that registers at UCR food services locations were compromised by a cyber hacker. Anyone who used a card, including visitors, between the summer of 2011 and November 16, 2011 may have had their financial information obtained. The information includes cardholder names, numbers, expiration dates, and an encrypted version of debit PINs.

Information
Source: Databreaches.net

November 28, 2011
Jewish Community Services of South Florida
Miami, Florida
NGO INSD 30

A coordinator at the Jewish Community Services office was arrested on charges of selling Holocaust survivor identity information. The dishonest employee misused access privileges to collect client names, addresses, Social Security numbers, and dates of birth of clients who regularly seek help from the Holocaust Survivors Assistance program. A police informant was offered the information of five clients after contacting the dishonest employee. The informant told the employee that he wanted the information for tax fraud purposes and was able to obtain 30 identifications for $1,000. The dishonest employee was captured after handing over 32 sheets of identity information.

Information
Source: Databreaches.net

November 27, 2011
101Domain.com
Carlsbad, California
BSO HACK 10,000

A phishing attack exposed the personal information of users with domain names. The unauthorized access was discovered by 101domain.com when a vendor contacted them to inform them of a breach that affected multiple vendors, including 101Domain.com.
UPDATE (12/20/2011): The websites 101domain.com, bluesit.com, free-domain.com, rerundomains.com, RWGUSA.com, and RWGUSA.net could have all been affected by a server breach at one of 101Domain, Inc.’s vendors. Encrypted customer names, addresses, email addresses, and in some cases, credit card or PayPal account information could have been compromised.

Information Source: Databreaches.net

November 27, 2011 \(\text{Cabarral Realty, Inc.} \quad \text{Waco, Texas}\)

A hacker named Kahuna posted three data dumps from the realty company. The names, email addresses, rental addresses, and payment information for approximately 625 renters were revealed.

Information Source: Databreaches.net

November 26, 2011 \(\text{Skagit County Health Department} \quad \text{Mount Vernon, Washington}\)

A student ran a Google search on her own name in mid-September and discovered some of her private information online. Skagit County Health Department was notified. People who used services at other county departments also had information exposed. The types of information did not include credit card numbers, Social Security numbers, dates of birth, or addresses, but did include information from receipts for department services.

Information Source: Databreaches.net

November 23, 2011 \(\text{MassBay Community College} \quad \text{Wellesley, Massachusetts}\)

A glitch allowed nearly 400 workers from 2002 to 2011 to view the personal information of any employees in MassBay's worker database system. The information included Social security numbers, home addresses, and other personnel information.

Information Source: Databreaches.net

November 23, 2011 \(\text{University of Kentucky HealthCare} \quad \text{Lexington, Kentucky}\)

Those with questions may call 1-877-528-3970 or email privacy@uky.edu.

An employee's phone was lost or stolen on September 25, 2011. Patient health conditions, medical record numbers, and possibly even names could be accessed from the phone.

Information Source: PHIPrivacy.net

November 23, 2011 \(\text{Sitka Wellness Center, EMR4Doctors.com} \quad \text{Sitka, Alaska}\)

Concerned patients may call (907) 747-2726.

A patient discovered their own personal information and that of 565 others online. Patient names, Social Security numbers, addresses, and dates of birth were exposed. A chiropractor from the Sitka Wellness Center claims that an electronic medical record software vendor known as EMR4Doctors.com stored the patient information for 9 months in 2008. The company stopped doing business in 2009. The information was removed from the Internet.

Information Source: PHIPrivacy.net

November 22, 2011 \(\text{YMCA of Metro Atlanta} \quad \text{Atlanta, Georgia}\)

A software testing vendor was robbed of several computers on November 9. One of the computers contained personal information of YMCA members active in 2008. Addresses, phone numbers, email addresses, dates of birth, bank account numbers, and credit card numbers were exposed.

Information Source: PHIPrivacy.net
Customers who used credit cards to sign up for WineLibrary.com may have had their financial information compromised. Wine Library began investigating the possibility of a breach in October when they received initial customer complaints. All credit card data was removed from the site on November 11th after an increase in customer complaints. The hacking incident(s) was traced back to China.

Information
Source: Databreaches.net

Virtual Radiological Professionals (vRad)
Eden Prairie, Minnesota

The October 14 car theft of an employee's laptop resulted in exposed physician and patient information. Though the laptop had a self-encrypting drive, it was not functioning properly. Patient and physician names, addresses, Social Security numbers, and bank account numbers or credit card numbers were exposed. Some patients also had unspecified medical information exposed as well.

Information
Source: PHIprivacy.net

Ohio Rehabilitation Services Commission
Columbus, Ohio

A state government watchdog revealed that confidential personal information was located in an outdoor trash bin. The documents contained documents related to a job agency for Ohioans with disabilities. The extent of the breach and the cause of the breach are being investigated.

Information
Source: Databreaches.net

Blairsville High School
Blairsville, Pennsylvania

Two students managed to obtain the login credentials for Blairsville High's online security system by repeatedly guessing. Their attempts began in May and were only discovered during the fall term when one of the students revealed his teacher's Social Security number in class. Teacher addresses, Social Security numbers, and salaries were exposed.

Information
Source: Databreaches.net

Morris Heights Health Center
New York, New York

A laptop was stolen from the area of MS 399/MS 459. It contained student information from the 2009-2010 school year such as names, dates of birth, genders, heights, weights, body mass indexes, ethnicity, asthma diagnoses, and influenza vaccination information.

Information
Source: PHIprivacy.net

Lebanon Internal Medicine Associates, P.C.
Lebanon, Pennsylvania

Contractors responsible for cleaning out the medical office after a storm improperly disposed of a computer that contained sensitive patient information. Lebanon Internal Medicine Associates left no specific instructions for the removal of the damaged computer. Patient information dating between November 1999 and August 25, 2011 was exposed and included full names, Social Security numbers, dates of birth, home addresses, account numbers, diagnoses, laboratory test results, and medical insurance information. It is believed that the information was inaccessible due to security measures within the server and flood damage.
An employee was arrested for using a skimming device to collect customer credit card information. At least 16 people were affected, but more are expected to come forward. The dishonest employee was underage at the time of the crimes and was held on suspicion of identity theft and forgery. Customers who used cards at the McDonald's drive through between October 10 and November 9 of 2011 may have been affected. Investigators became aware of the breach when members of the Washington State Employees Credit Union began filing claims for fraudulent use of their credit cards.

A restaurant manager was found to have sold the identities of U.S. citizens to illegal aliens employed at multiple McDonald’s restaurants. The employee was sentenced in U.S. District Court to 32 months in federal prison for her role in the identity theft scheme. Fourteen arrests were made and five suspects face federal identity theft charges. The rest were charged with immigration violations. It is unclear how many people were involved in the identity theft scheme. Other McDonald’s managers also stole and sold the identities of U.S. citizens.

Between 2009 and July 2011, the owner of Community Tax used confidential information to file false tax returns through Community Tax. Nearly 1,400 tax returns were linked to the owner over those two years. On August 31, 2011, the owner was indicted on 32 counts. She faces between two and 27 years in prison, along with three or less years of supervised release, mandatory restitution, and up to $750,000 in fines or twice the cost of her crimes. The dishonest owner illegally obtained names, Social Security numbers, and dates of birth, then used the information to file tax returns. The refunds from the tax returns went to her bank accounts and debit cards. She also used online filing websites to file false tax returns. The scheme was uncovered when a criminal complaint was filed.

Members of Honolulu’s APEC Host Committee may have had their personal information exposed after requesting security clearances to meet with President Barack Obama. Someone gained unauthorized access to eight East-West Center computers beginning on October 25 by using “unusually sophisticated methods.” Committee member names, Social Security numbers, and dates of birth could have been acquired.

Morton’s is located in Stamford, Connecticut. The Bicycle Club is located in Englewood Cliffs, New Jersey. An identity theft ring that targeted wealthy customers of steakhouses was uncovered. At least 28 current and former waiters and associates were arrested. Waiters used credit card skimmers to steal the credit card information of customers who paid with American Express Black cards and other high-limit credit cards. The crimes occurred between April 2010 and November 2011. At least 50 victims have been identified.

Thousands of patient records were stolen by a former employee. Names, ages, genders, Medicare coverage information, phone numbers, and dates of birth were exposed. The employee did not steal the records for ID theft purposes, but rather for their usefulness in contacting potential clients. The unnamed former employee owns a home health care agency.
Detailed medical information was discovered on the back of a drawing from a student of Hale Elementary. An attorney from Sawicki and Phelps donated the firm’s old paper to her child’s school. A local news team contacted the school after discovering the incident and additional pieces of paper were collected and stored in a secure location. The number of people affected was not revealed.

Information Source: PHIPrivacy.net

November 17, 2011
Medcenter One
Bismarck, North Dakota

On the weekend of October 21, 2011, a Medcenter One laptop computer and a bag containing 11 internal paper forms for processing patient charges were stolen from an employee’s car along with valuable personal items. The forms contained patient name, date of birth, address, phone number, insurance company and policy number, Medicare number, and patient hearing diagnoses. The stolen laptop contained the names and dates of birth for 650 hearing aid patients from 2003 up to the time of the theft.

Information Source: PHIPrivacy.net

November 16, 2011
Sutter Physicians Services (SPS) and Sutter Medical Foundation (SMF)
Sacramento, California

Patients with questions may call (855) 770-0003 and enter a digital reference code: 7637111511.

A company-issued password-protected unencrypted desktop computer was stolen from SMF’s administrative offices during the weekend of October 15, 2011. Approximately 3.3 million patients whose health care provider is supported by SPS had their names, addresses, dates of birth, phone numbers, email addresses, medical record numbers and health insurance plan name exposed. The information dated from 1995 to January of 2011. An additional 934,000 SMF patients had dates of services and description of medical diagnoses and/or procedures used for business operations in addition the the previously listed information exposed. This information dated from January 2005 to January 2011. Patients will receive notification letters no later than December 5.

UPDATE (11/23/2011): Two lawsuits have been filed against Sutter Health. One class-action suit alleges that Sutter Health was negligent in safeguarding its computers and data and then did not notify the millions of patients whose data went missing within the time required by state law. The suit seeks $1,000 for each member of the class and attorneys’ fees.

UPDATE (07/21/2014): "A state appellate court Monday ordered the dismissal of a lawsuit that could have cost Sutter Health more than $4 billion when it ruled that millions of the health care giant’s patients had no right to sue over the theft of a computer with their personal, medical and insurance records on its hard drive.

The court decided it has not been shown – and the patients have not alleged – that any unauthorized persons have actually viewed the contents of the hard drive, a fact that deprives the patients of grounds to seek civil damages".

Information Source: PHIPrivacy.net

November 16, 2011
McDonald’s
Oak Park, Michigan

A supervisor noticed a drive-thru cashier using a skimming device. The dishonest employee admitted to stealing the information from more than 100 customer cards, and stealing between 15 and 20 accounts during each drive-thru shift. Another person provided the skimming device and paid the employee $15 per credit account.

Information Source: Databreaches.net

November 16, 2011
Bright Directions College Savings Program, Illinois State Treasurer’s Office
Springfield, Illinois

A mailing error led to the Social Security numbers of over 36,000 people to be visible from the outside of envelopes mailed in October. Those who were enrolled in the Illinois Treasurer’s Office Bright Directions college savings program were affected.

Information Source: Databreaches.net
An employee was caught with a skimming device after hotel guests complained about fraudulent charges on their credit and debit cards. The employee managed to get the information after cleaning the rooms of hotel guests. Hotel security was able to determine which employee had taken the credit card information by checking key card information for room activity. A hidden camera in a mock room showed that the employee was checking the personal belongings of guests and using the skimmer on any cards that were found.

Information
Source: Databreaches.net

November 14, 2011

The Public School Employees' Retirement System
Harrisburg, Pennsylvania

GOV DISC 2,000

About 2,000 pension fund members had their information placed online when an employee accidentally posted an unencrypted file on a public website. At least one person saw the information. The date of this error was not reported. Member names and Social Security numbers were exposed.

Information
Source: Databreaches.net

November 15, 2011

Citizens Equity First Credit Union (CEFCU)
Peoria, Illinois

BSF PORT Unknown

The theft of a laptop resulted in the exposure of customer names, Valley Credit Union account numbers, Social Security numbers, and addresses. The laptop was stolen outside of the office sometime before November 4. No information was given about the number of customers who were affected or who the laptop was stolen from.

Information
Source: Databreaches.net

November 14, 2011

Smokers Choice
New York, New York

BSR HACK 200

A man was arrested for his role in the unauthorized collection and use of credit card numbers from over 200 Columbia County residents. Investigators began searching for a common link between the affected residents in August. Results of the investigation lead them to overseas activity in Russia and video surveillance from Wal-mart security.

Information
Source: Databreaches.net

November 14, 2011

Santa Clara University
Santa Clara, California

EDU HACK 60 (No SSNs or financial information reported)

The academic records database of Santa Clara University was hacked in order to change the grades of over 60 current and former undergraduate students. The breach was discovered when a former student pointed out that her current transcript showed a grade better than the one on a transcript that had previously been printed. Tens of thousands of student records dating back more than a decade were examined. The “sophisticated” hacking incident or incidents had altered student transcripts from all three of the University’s schools and changed some grades for courses taken as far back as 2006. The incident or incidents is believed to have occurred between June 2010 and July 2011. Some students received subtle upgrades and others had their grades changed from F’s to A’s.

Information
Source: Databreaches.net

November 13, 2011

Brownsville Independent School District
Brownsville, Texas

EDU DISC Unknown

Affected employees may call (965) 548-8061.

Brownsville ISD discovered that a number of employees had their names, Social Security numbers, disability plan information, and salary information available on a publicly accessible website. Employees who were enrolled for
disability insurance had their information posted in April 2011 on the Employee Benefits/Risk Management website.

Information
Source: Databreaches.net

November 13, 2011
**Providencenightlife.net**
**Providence, Rhode Island**

Hackers posted data from providencenightlife.net users onto Pastebin. The data included usernames, clear-text passwords, and email addresses.

Information
Source: Databreaches.net

November 12, 2011
**United States Postal Service (USPS)**
**Washington, District Of Columbia**

A customer logged onto her USPS online store account and was able to see the name, address, and the final four digits of another customer’s credit card number. The customer alerted the USPS customer service, but was told that the error had already been noted. On October 28, USPS became aware that a coding issue during an update had resulted in an error that exposed credit card information. Customers were notified of the problem on November 8. The error was subsequently fixed.

Information
Source: Databreaches.net

November 11, 2011
**University of Texas-Pan American**
**Edinburg, Texas**

Those with questions may email infosecurity@utpa.edu.

On September 1, 2011, a spreadsheet containing information on 19,276 students was accidentally made accessible from the internet due to an administrative error. The spreadsheet contained the names, addresses, phone numbers, email addresses, majors, class or classes, levels, colleges, student ID numbers, and GPAs of students enrolled as of September 1 of 2011. The problem was corrected on November 2 soon after it was discovered. The spreadsheet had been accessed 15 times by unknown parties between September 1 and November 2.

Information
Source: Databreaches.net

November 11, 2011
**Virginia Commonwealth University**
**Richmond, Virginia**

Those with questions may call (855) 886-2931 or email responseteam@vcu.edu.

Hackers were able to access a Virginia Commonwealth University (VCU) computer server. It contained files with the personal information of current and former VCU and VCU Health System faculty, staff, students and affiliates. Suspicious files were discovered on the server on October 24. It was taken offline and subsequent investigation revealed that two unauthorized accounts had been created on a second server. While the first server did not contain personal data, the second server did and had been compromised through the first server. Data included either a name or eID, Social Security number, and in some cases, date of birth, contact information, and various programmatic or departmental information.

Information
Source: Databreaches.net

November 10, 2011
**Wakulla County School Board**
**Crawfordville, Florida**

The information of 2,400 students in grades four through ten was accidentally posted online. A parent discovered the breach after searching their child’s name. The student’s FCAT scores and Social Security number appeared on a public site. The cause of the unintended disclosure was not reported.

Information
Source: Databreaches.net

November 10, 2011
**Steam (The Valve Corporation)**
**Bellevue, Washington**

records from this breach used in our total: 0

50,000 (No SSNs or financial information reported)

records from this breach used in our total: 0

5,400 (No full credit card numbers or SSNs revealed)

records from this breach used in our total: 0

19,276 (No SSNs or financial information reported)

records from this breach used in our total: 0

176,567

records from this breach used in our total: 176,567

2,400

records from this breach used in our total: 2,400

35 million
The November 6 defacement of Steam forums led to an investigation that revealed hackers had accessed a Steam database with sensitive user information. The database contained user names, hashed and salted passwords, game purchases, email addresses, billing addresses, and encrypted credit card information. Users were prompted to change their Steam forum passwords and encouraged to change their Steam account passwords. Anyone using their Steam forum password for other websites should change their password since hackers could have obtained email address and password combinations. Steam is the Valve Corporation’s social-distribution network. People who use the company’s online gaming content were affected.

UPDATE (11/16/2012): A judge dismissed a class action lawsuit related to the November 6, 2011 breach. The plaintiffs of the lawsuit used Steam to purchase and access online gaming content. They alleged present and future harm as a result of the breach. According to the judge who dismissed the lawsuit, the plaintiffs did not prove that they were harmed by the Steam breach.

Information Source: Databreaches.net

November 9, 2011  Columbia-St. Mary’s Ozaukee Hospital
               Mequon, Wisconsin
                      MED  INSD 30 (No SSNs or financial information reported)

A janitor sold patient records to gang members. The janitor was able to use a master key to access boxes of sensitive information that were due to be shredded. Some of the locks to the restricted boxes were also broken. The scheme went on for up to eight months and investigators were able to seize nearly 30 patient records.

Information Source: PHIPrivacy.net

November 9, 2011  Behavioral Health Services of Pickens County
                   Pickens, South Carolina
                      MED  PORT 200 (No SSNs or financial information reported)

A man who purchased a used computer hard drive discovered that it had detailed clinical assessments for patients referred to Behavioral Health Services of Pickens County and a monthly monitoring list of patient referrals from the Pickens County Department of Social Services. Information about patient drug and emotional problems and pending litigations was on the hard drive.

Information Source: PHIPrivacy.net

November 9, 2011  ValueOptions, National Elevator Industry
                   Newtown Square, Pennsylvania
                      BSO  PORT 7,019

On July 6, 2011, four tape cartridges with sensitive information were shipped in a container from VOI. The container was placed into a cardboard shipping box and shipped. ValueOptions Inc. (VOI) was informed that the package had not arrive as of August 1. An outside agency investigated the loss of the packages until September 22. Notification that the tapes had been lost was sent on November 4. The tapes contained names, addresses, phone numbers, dates of birth, Social Security numbers, and plan subscriber ID numbers. VOI processes the benefits information for National elevator Industry’s Health Benefit Plan, as well as other organizations. A total of 350 New Hampshire residents were affected by the breach and 6,669 New York residents were affected as well. The total number of people affected from different organizations and across the United States was not reported.

Information Source: Databreaches.net

November 9, 2011  Habitat for Humanity Delaware County ReStore
                   Delaware, Ohio
                      NGO  HACK 444

A number of identity thefts were linked to Habitat for Humanity of Delaware County ReStore. An investigation revealed that hackers had accessed the store’s computer system and took customer names and credit card numbers. Detectives believe there are other sources of identity theft that have yet to be identified. The date of the access was not reported, but as many as 444 customers could have had their information taken.

Information Source: Databreaches.net

November 8, 2011  IQCR
                   Rock Hill, South Carolina
                      BSO  INSD 100

An employee of IQCR wrote down names, Social Security numbers, and dates of birth from records. The records came from a gas company in Chicago and were processed by IQCR. That information was then used to apply for credit cards. This occurred in October of 2011. The dishonest employee and her partner were caught after people alerted authorities about being declined for credit cards they had not requested. Authorities discovered that the fraudulent credit requests all came from the same computer IP address and went to the same residential address. The couple face 10 years in prison.
A dishonest employee swiped customer credit cards after initial transactions, then processed a second transaction for cash back and pocketed the amount of the second fraudulent transaction from the cash register. A store manager noticed the employee stealing money and reported her. A customer complaint about an unauthorized transaction then revealed the extent of the breach. The fraudulent transaction complaints date from May 25 to June 10. Store records reveal that $6,197 was stolen in this way.

A woman found tax return information lying on the ground in front of an abandoned Jackson Hewitt on or around October 22. Hundreds of documents were exposed. The building owner called a shredding company to dispose of the documents, but ended up leaving them outdoors until the disposal company arrived. The person responsible claimed that all the records were over four years old and were difficult to transport from the office. The paperwork came from the Jackson Hewitt office at 1734 Divisadero St.

A dishonest employee was arrested for using customer debit and credit card numbers to make online purchases. The employee was charged with 21 counts of deceptive practice, 21 counts of identity theft, four counts of felony theft, and 17 counts of misdemeanor theft. Anyone who used debit or credit cards at the Peoria Heights McDonald’s between September 15 and October 30, 2011 may be at risk. The stolen account numbers came from CEFCU debit cards.

Someone stole thousands of X-rays from Saint Jospeh medical Center. Authorities believe the X-rays were taken for their silver content rather than for identity theft purposes. They contained patient names, dates of birth, medical record numbers, dates of service, physicians, and some diagnostic information. Patients who were X-rayed between 2004 and 2005, as well as sometime during 2007 may have been affected.

A man tried to steal X-rays. Investigators believe he wanted the X-rays for the tiny amount of silver inside rather than the protected health information of patients. The incident may have been related to other thefts in the Massachusetts and New Hampshire areas.

Two men were arrested for posing as employees of an X-ray removal company in order to steal old X-ray films. The two men hit multiple locations. It is believed that their primary focus was the silver contained in the films, however patient medical and personal information was also linked to the X-ray films. Around 1,000 X-rays were stolen from Harvard University Health Services and a barrel of X-rays was taken from Anna Jaques Hospital. The men were charged with conspiracy and larceny from a building. The thefts occurred in August, but it is unclear how many other organizations were affected. The men were also linked to a crime or crimes in New Hampshire.

UPDATE (03/05/2012): The men were tied to thefts and theft attempts at Anna Jaques Hospital in Newburyport and Saints Medical Center in Lowell.
November 4, 2011  Thomas Jefferson University Hospitals  Philadelphia, Pennsylvania

The Hospital’s notice can be read [here](#).

On September 6, X-ray films were stolen from the Hospital by thieves posing as representatives of an X-ray recycling vendor. The thieves were most likely looking to strip the silver from the old films. If any information had been taken from the X-rays it would include patient names, gender, dates of birth, dates of services, medical record numbers, and areas x-rayed.

November 4, 2011  www.podiatry.com, PRESENT e-Learning Systems  Boca Raton, Florida

The names, email addresses, and affiliations of certain people who registered with PRESENT e-Learning Systems' Podiatry program were posted online at Pastebin.com. An additional 86 people had their names and mailing addresses posted on Pastie.org after registering for a podiatry online tutoring course. A hacker called "Teku" claimed responsibility.

November 4, 2011  University of California Los Angeles (UCLA) Health System  Los Angeles, California

A September 6 home theft resulted in the loss of an external computer hard drive. It contained the first and last names, birth dates, medical record numbers, addresses, and other medical record information of patients. The information dated from July 2007 to July 2011 and belonged to an individual who maintained the information in order to fulfill job duties. Other items were taken during the theft, but none have been recovered.

**UPDATE** (12/20/2011): A class action lawsuit was filed on December 14. It alleges that the UCLA Health System violated California's Confidentiality of Medical Information Act. Since the act provides for statutory damages of $1,000 per person, the UCLA Health System could owe nearly $16.3 million to the 16,288 patients who were affected.

**UPDATE** (12/22/2011): A total of 16,288 people had some type of information on the laptop, but 2,761 had enough information on the laptop to cause "more than a minimal amount of financial, reputational, or other harm" if accessed.

**UPDATE** (10/17/2013): A state appellate court dismissed the class action lawsuit. The ruling was that health care providers are not necessarily liable when medical information is misused or stolen unless the information is accessed by unauthorized parties.

November 4, 2011  Lawrence Memorial Hospital, Mid Continent Credit Servies, Inc. (Blue Sky Credit), BrickWire LLC  Lawrence, Kansas

Those with questions may call 785-505-4945 or email lmhcompliane@lmh.org.

A breach of a website hosted by BrickWire LLC resulted in the exposure of patient names, phone numbers, email addresses, health care providers, payment amounts, dates of payment, credit card information and checking account information. Lawrence Memorial Hospital’s vendor Blue Sky Credit used BrickWire LLC for the online bill-pay service offered to Lawrence Memorial’s patients. The personal and financial information of patients who paid through the website was accidentally made available on the Internet between September 20, 2011 and October 28, 2011.

**UPDATE** (11/17/2011): It appears that BrickWire left a portal open that contained payment records from 28 LMG patients after doing a system upgrade on September 20. However, the information of every patient who used the online bill pay system between 2005 and September of 2011 was available in a database that was accessible through the portal.
November 4, 2011 Amsterdam Hospitality Group New York, New York BSO INSD 237

An auditor for the Amsterdam Hospitality Group sold credit card information to another man for identity theft purposes. As an employee for the Amsterdam Hospitality Group, the auditor had access to the credit card account information and identifying information of people who stayed at a number of Manhattan hotels. It is unclear which hotels were affected. Over $840,000 in fraudulent credit card purchases were made with the stolen information.

Information Source: Databreaches.net records from this breach used in our total: 237

November 4, 2011 Washington South Supervisory Union Northfield, Vermont GOV HACK Unknown

Supervisory Union notified all employees that a serious security breach on its financial computer system was discovered and that their financial information may have been compromised. The breach was not described in detail, but employees were informed that payroll would be temporarily using paychecks. Supervisory Union contacted all banking institutions that were involved in direct deposit and informed them that client data may have been compromised. Employees were also encouraged to contact all banking institutions to review their financial accounts, contact their banks, change their email passwords, and avoid clicking on suspicious emails.

Information Source: Databreaches.net records from this breach used in our total: 0

November 3, 2011 Kunz Opera House Pinckneyville, Illinois MED PHYS 4200 (Unknown number SSNs)

ER patients in Metropolis and Staunton who saw Dr. Tim Mathis may have been affected.

A physician kept 14 boxes of medical records from former patients in the front window of his building. A fire that struck the building, the Kunz Opera House, damaged the records and personal property. Some records were found in the street. An unspecified number of the damaged records were then buried in a secure location.

Information Source: PHIPrivacy.net records from this breach used in our total: 4,200

November 3, 2011 Top of the Line Marketing Rockville, Maryland BSO INSD 1,200

Between the summer of 2010 and February of 2011, a dishonest employee of Top of the Line Marketing passed along names, Social Security numbers, and dates of birth for the purpose of identity theft. A police raid uncovered 42 debit cards and a list of 1,200 Maryland residents that had been distributed by the dishonest employee. Some of the information had been used to collect unemployment benefits on prepaid Visa cards. The person who was found with the fraudulent debit cards and list pleaded guilty to one count of conspiracy to commit access device fraud and one count of aggravated identity theft. He faces a maximum of five years in prison for the first count and a mandatory two-year sentence for the second.

Information Source: Databreaches.net records from this breach used in our total: 1,200

November 2, 2011 Avia Dental Plan, Inc. Wheeling, West Virginia NGO UNKN 2500

Avia received notification of a breach involving an intruder or intruders using a password for the administrative software suite. The United State Secret Service became aware of the theft of a password that allowed outsider access to Avia Dental Plan member information. Names, Social Security numbers, dates of birth, addresses, phone numbers, email addresses, credit card information, and in some cases dependent information, were exposed.

Information Source: PHIPrivacy.net records from this breach used in our total: 2,500

November 2, 2011 Maloney Properties, Inc. Wellesley, Massachusetts BSO PORT 621 (Unknown number of SSNs involved)

The October 15 theft of a laptop resulted in the exposure of unencrypted personal information. Residential housing data was on the laptop. This included names, the full Social Security numbers of some people, and the last four digits of most.

UPDATE (3/26/2012): Maloney Properties, Inc. agreed to pay $15,000 in civil penalties. The property management firm must also ensure that personal information is not unnecessarily stored on portable devices, ensure that all personal information stored on portable devices is properly encrypted, ensure that all portable devices containing personal information are stored in a secure location, and effectively train employees on the policies and procedures with respect to maintaining the security of personal information. Up to 621 people were affected by the car theft of an employee’s unencrypted laptop.
Information
Source: Databreaches.net

November 2, 2011

University of Alabama
Tuscaloosa, Alabama

EDU DISC Unknown

On October 26, students who had at least one failing midterm grade during the Fall 2011 semester received an email from the office of the assistant dean of students. The email, which informed students of their grade, was not blind copied. Each email recipient could see the email addresses of other students who received the email. No other information was exposed.

Information
Source: Databreaches.net

November 2, 2011

Aaron’s
Fresno, California

BSR STAT 1,008

On September 26, Aaron’s became aware of an office burglary that resulted in the theft of computers, TVs, electronic gaming devices, and other goods. Customer names and Social Security numbers were on one of the computers. At least 1,008 New Hampshire residents were affected, but the total number of affected people nationwide was not revealed.

Information
Source: Databreaches.net

November 2, 2011

MetroLux, Metropolitan Theatres
Loveland, Colorado

BSO HACK 1,180

Metropolitan Theatres is headquartered in Los Angeles, California.

The parent company of MetroLux, Metropolitan Theatres, reported an external breach of the local theater's computer system. Someone attacked the data transmission system and stole customer financial information via computer. The issue was first noticed on October 21. The breach was analyzed and new servers were installed. Though the system was confirmed to have been compromised, not all of the 1,180 people who reported fraud had used their credit or debit cards there.

Information
Source: Databreaches.net

November 1, 2011

High Point Regional Health System, Premier Imaging LLC
High Point, North Carolina

MED INSD 47

A former employee was fired after taking patient files home sometime between September 14 and October 6. The files contained patient names, Social Security numbers, dates of birth, addresses, driver's license numbers and insurance information. A total of 47 patient records were returned, but it is unclear if the employee may still have others.

Information
Source: Databreaches.net

October 28, 2011

Mama's Boy Italian Ristorante
Durango, Colorado

BSR HACK 100

A hacker accessed the restaurant's computer system in early August and infected it with a virus. Customer debit and credit card numbers to be sent to outside parties. The virus was not discovered until mid-October. Over 60 of the credit and debit numbers that were duplicated to fraudulent cards were used in Florida.

Information
Source: Databreaches.net

October 28, 2011

Henry Ford Health System
Troy, Michigan

MED STAT 520 (No SSNs or financial information reported)

Patients with questions may call (866) 523-6770.

A computer with sensitive patient information was stolen sometime between August 5 and August 7. It held patient names, physician names, medical record numbers, and genotype test results.

Information
Source: PHIprivacy.net

October 28, 2011

Muir Orthopaedic Specialists
Oakland, California

MED PHYS 1,800 (No SSNs or financial information reported)
Patients with questions may call 1 (877) 371-7902.

The July 27 theft of a binder exposed patient information. The binder contained surgical patient labels from August 2004 to July 2011, corresponding dates of birth, and medical record numbers.

**Information**

**Source:** PHIPrivacy.net

**Date:** October 27, 2011

**Department of Education**

**Washington, District Of Columbia**

GOV DISC 5,000

As many as 5,000 users of the Department of Education's website may have had their information viewed by other users who logged in to the website. The breach lasted for six to seven minutes and exposed Social Security numbers and other student information. The site was shut down and examined for 48 hours after the incident.

**Information**

**Source:** Databreaches.net

**Date:** October 27, 2011

**Clarinda Bank Iowa**

**Clarinda, Iowa**

BSF UNKN Unknown

A breach of a data processor affected Clarinda Bank Iowa. The type of breach was not reported, and it is possible that other banks were affected by the data processor breach. Specific bank customers were notified of the breach by letter on October 23.

**Information**

**Source:** Databreaches.net

**Date:** October 27, 2011

**Eaton Group**

**Baton Rouge, Louisiana**

BSO PHYS Unknown

A local news team was alerted to a group of scattered documents near a lake and an interstate. Most of the documents were labeled with an "Eaton Group" stamp. The owner of the law group and collection service was not sure how the documents came to be exposed rather than properly disposed of. The court case documents exposed names, Social Security numbers, addresses, bank statements, bank account numbers, Mastercard account numbers, and other sensitive information. The papers were collected and properly destroyed, but the owner did not see a reason for concern since most of the information was available in the public record.

**Information**

**Source:** Databreaches.net

**Date:** October 27, 2011

**Ocala Police Department**

**Ocala, Florida**

GOV INSD 149

A police officer was linked to a tax fraud ring. The officer accessed the Drivers And Vehicle Information Database (DAVID) in order to give the personal information of around 149 drivers to co-conspirators. The information was then used to open 184 bank accounts where fraudulent tax return checks could be cashed. An investigation was opened when the insider attempted to recruit someone else. The insider was suspended without pay until the investigation is completed.

**Information**

**Source:** Databreaches.net

**Date:** October 27, 2011

**James A. Haley VA Hospital**

**Tampa, Florida**

MED PORT Unknown

A camera from the Plastic Surgery Clinic was discovered missing in November of 2010. It contained Social Security numbers and graphic photos of female patients before and after surgery for breast cancer. The same investigation that uncovered the missing camera also revealed that laptops, televisions, thumb drives, microscopes, a hospital surveillance system, and other equipment had been lost or stolen within the past two years. One missing thumb drive contained additional patient information.

**Information**

**Source:** PHIPrivacy.net

**Date:** October 26, 2011

**Indigo Joes'**

**Shelby, Alabama**

BSR PHYS Unknown

The information of hundreds of people was discovered in a trash storage location. The documents appear to be connected to employees of a defunct restaurant named Indigo Joes’. Paycheck stubs, Social Security numbers, Driver’s licenses, and other personal information were discovered.
An abandoned Indalex plant still contained personnel records. Employee names, Social Security numbers, medical records, addresses, and other sensitive information were exposed when scavengers looking for aluminum and other materials ravaged the abandoned plant. The plant was closed in 2008 and Indalex filed for bankruptcy in 2009. Indalex received clearance from a bankruptcy court to officially abandon the plant in 2010. The damage was discovered when 40 workers from the Stanislaus County jail alternative work program cleared the plant.

**Information**
**Source:** Databreaches.net

October 24, 2011 **Pan American Games**

This breach pertains to a website that was overseen by the Guadalajara (Mexico) 2011 Organizing Committee. No location is listed.

An anonymous tipster alerted reporters to a breach that allowed the personal information of journalists covering the Pan American Games to be viewed. The tipster claimed that reporter names, dates of birth, the first five digits of passports, photos, family numbers, and addresses were accessible. Reporters from across the Americas were affected. The Guadalajara 2011 Organizing Committee stated that they had deleted the personal information from their database after the discovery.

**Information**
**Source:** Databreaches.net

October 23, 2011 **Hazleton Community Ambulance Association**

Hundreds of sheets were found inside of folders in improperly discarded boxes. The sheets were easily visible and accessible through sliding doors on either side of the dumpster and a firefighter alerted a local newspaper to the incident. The records contained names, Social Security numbers, payroll information, addresses, phone numbers, insurance information, dates of birth, and medical histories from employees and former patients of the Ambulance Association. It appears that all of the records are from 2003 and 2004. An Ambulance Association officer admitted to placing the boxes in a dumpster rather than following usual procedure and shredding them.

**Information**
**Source:** PHIPrivacy.net

October 22, 2011 **Onehitplay.com**

A hacker or hackers posted the account information of Onehitplay.com users online. The cost of the breach is estimated at $214,000.

**Information**
**Source:** Dataloss DB

October 22, 2011 **International Association of Chiefs of Police (IACP), Boston Police Patrolmen’s Association, Baldwin County Sheriff’s Office in Alabama, Matrix Group**

This breach has no central location. Multiple organizations were affected by two groups of hackers.

Factions of Anonymous and Antisec posted sensitive law enforcement files on the internet on Friday October 21. Data from multiple law enforcement vendors’ and agencies’ computer systems were compromised. At least four groups were affected. An IACP membership roster, Birmingham and Jefferson County police officer names, Social Security numbers, ranks, addresses, and phone numbers, Matrix Group client and financial information, and data from an unnamed web design and marketing firm with law enforcement customers were exposed.

**Information**
**Source:** Databreaches.net

October 22, 2011 **Concordia Plan Services (CPS)**

Concordia Plan Services was also known as Worker Benefit Plans. Those with questions may call (888)-414-8021. Microfilm that contained the plan enrollment information of benefits members was lost by a delivery service sometime between February and May of 2011. It contained names, addresses, dates of birth and in some cases Social Security numbers and limited medical information from the 1960’s and 1970’s. A vendor received the microfilm from CPS on
February 3rd. The vendor attempted to transfer the microfilm to another company, but learned that the microfilm had been misplaced sometime prior to or during May. CPS's vendor informed them of the situation on August 23.

Information
Source: PHIPrivacy.net

October 20, 2011 AdvancePierre Foods Cincinnati, Ohio

BSR PORT Unknown

An unencrypted flash drive with sensitive employee information was lost during transportation. It was mailed to the company's 401k provider, Milliman, on September 8. An envelope arrived on September 12 without the flash drive. Employees were notified on October 5. Current and former employees may have had their names, Social Security numbers, dates of birth, dates of hire, and compensation amounts from 2009 and 2010 exposed.

Information
Source: Databreaches.net

October 20, 2011 PSEG Newark, New Jersey

BSO PORT Unknown

The September 25 home theft of an employee's laptop resulted in the exposure of PSEG employee information. Names, Social Security numbers and other personnel information were exposed.

Information
Source: Databreaches.net

October 20, 2011 College of the Holy Cross Worcester, Massachusetts

EDU UNKN 493

Seven Holy Cross employees fell for phishing attempts. The employees had their email accounts attacked and emails containing personal information for hundreds of people were exposed. Though Holy Cross has a policy of encrypting all emails that contain personal information, these emails were not encrypted. Those who could have been affected were notified that their Social Security numbers, driver's license numbers, dates of birth, financial information and other types of information were at risk.

Information
Source: Databreaches.net

October 20, 2011 Wells Fargo Jacksonville, Florida

BSF DISC Unknown

Customers in South Carolina were also affected.

Customers with questions may call 1-800-869-3557.

A mailing error exposed customer bank account information to other customers. Pages from other customer accounts which included bank account numbers, balances, and transactions were accidentally mailed to other customers in September paper statements. The error was caused by a printer malfunction. Wells Fargo temporarily took the printer out of service after the breach was discovered. At least 50 customers noticed the problem.

Information
Source: Databreaches.net

October 19, 2011 Well United Methodist Church, Iowa Correctional Institute for Women Mitchellville, Iowa

Gov INSD 48

A former inmate was able to obtain and misuse the information of prison church volunteers. The former inmate had held a leadership role in the congregation and was hired as an administrative assistant after being released in 2007. Her position as administrative assistant may have allowed her to misuse the personal information that volunteers were required to submit in order to obtain prison security clearance.

UPDATE (05/19/2012): The former inmate was sentenced to four years in prison for using the personal information of other church members to fraudulently obtain credit accounts. She had worked as an administrative assistant in the program between her 2007 release and a 2008 probation that sent her back to prison. She was able to misuse the information of 48 people once leaving prison.

Information
Source: Databreaches.net

October 17, 2011 Spectrum Health Systems, Inc. Worcester, Massachusetts

MED PORT Unknown

The August 24 office theft of a hard drive resulted in the exposure of patient information. No patient information was believed to have been exposed, but an investigation of the breach revealed that the hard drive had been stolen along with a laptop and a desktop computer. It contained information from people who received Spectrum program services at the Westborough, Worcester, Milford, Framingham, Southbridge, Fitchburg, and Weymouth locations between 2002 and March of 2011. Inpatient and outpatient names, Social Security numbers, diagnostic codes, medical insurance numbers,
addresses, phone numbers, and dates of birth were exposed.

Information Source: PHIPrivacy.net

October 16, 2011

**Law Office of Ashley Bell, Department of Family and Children Services, Court Appointed Special Advocates (CASA)**

Gainesville, Florida

BSO  PHYS  Unknown

Sensitive client files were found in a newspaper recycling bin at The Gainesville Times. The files were related to the physical and sexual abuse of juveniles and client Social Security and phone numbers were exposed. The breach may have been caused by a college intern who disposed of the files inappropriately. Some files were as recent as 2009, but all cases were closed.

Information Source: PHIPrivacy.net

October 15, 2011

**San Antonio Independent School District (SAISD)**

San Antonio, Texas

GOV  DISC  70

Dozens of students had their names, Social Security numbers, phone numbers, dates of birth, home addresses, and dropout likelihood posted online for several months. The dropout likelihood was included in reports along with other personal details such as academic problems, homelessness, and history of running away from home. The reports were never meant to be posted and a note that read "All student information is confidential. This report must be SHREDDED when no longer in use" was clearly visible at the bottom of each report. An administrator accidentally changed the SAISD site settings and exposed the information at an unspecified time. The total number of students affected was not reported, but it appears that several reports each contained confidential information for 60-70 students. Students appeared in multiple reports.

Information Source: Databreaches.net

October 14, 2011

**Securities and Exchange Commission (SEC), Financial Tracking Technologies (FTT)**

Washington, District Of Columbia

GOV  DISC  Unknown

FTT, a contractor working with SEC’s ethics compliance program, violated its agreement with SEC by providing names and account numbers to a subcontractor, or subcontractors without permission. An SEC September 16 security review revealed that FTT had failed to comply with contractual obligations. The system was taken offline and FTT was told to terminate all third party access to SEC systems.

Information Source: Databreaches.net

October 14, 2011

**Freda J. Bowman MD, PA**

, Texas

MED  UNKN

The city where the breach occurred was not reported.

Protected health information from a network server was breached on or around August 8, 2011. The incident may have been an unintended disclosure which allowed unauthorized users to view information, or it may have been a hacking attack.

Information Source: HHS via PHIPrivacy.net

October 14, 2011

**Scott County Memorial Hospital**

Scottsburg, Indiana

MED  PORT  2,059 (No SSNs or financial information reported)

Those with questions may call (812) 883-1708 for medical record information or (855) 251-4581 for information regarding this breach.

A surgeon, had a palm pilot device stolen from his parked vehicle on or around the morning of July 13, 2011. It held patient names, dates of birth, surgical procedures, diagnoses, and anesthesia. Patients who had seen the surgeon between December 27, 2007 and June 24, 2011 were affected.

Information Source: HHS via PHIPrivacy.net

October 14, 2011

3,116 (No SSNs reported)

383
NEA’s former public website was compromised by a hacker or hackers on July 12, 2011. People who previously registered with the website in order to use the website’s special functions may have had their email addresses and user name and password combinations exposed. Some individuals also had their names, addresses, and dates of birth compromised. Since passwords may have been obtained, individuals who may have been affected should not use their NEA website password for any other accounts.

Information
Source: HHS via PHIPrivacy.net

The theft of a laptop on or around August 11, 2011 resulted in the exposure of protected health information.

Information
Source: HHS via PHIPrivacy.net

The city where this breach took place was not reported.

The July 1, 2011 theft of a desktop computer and network server resulted in the exposure of patient information.

Information
Source: HHS via PHIPrivacy.net

The theft of a laptop from a nurse’s car may have exposed names, dates of birth, genders, Medicaid client identification numbers, procedure codes, diagnoses codes, and other health information. The theft took place on March 10, 2011, but it was not until August that the risk to patient privacy was discovered. A notice was sent on September 9.

Information
Source: PHIPrivacy.net

Patients with questions may call 1 (888) 613-3688.

The July 2 car theft of a computer hard drive may have exposed patient information. Patients who visited NIOS between January 1, 2006 and July 2, 2011 could have had their names, Social Security numbers, addresses, dates of birth, telephone numbers, and billing account data obtained.

Information
Source: PHIPrivacy.net

It appears that the Social Security Administration accidentally releases the names, Social Security numbers, and birth dates of thousands of living U.S. citizens each year in a database called the “Death Master File”. Social Security officials revealed that the number of U.S. citizens mistakenly listed each year is about 14,000, while 90 million are accurately reported. A Scripps Howard News Service review of three recent copies revealed 31,931 living U.S. citizens who'd had their Social Security numbers released to U.S. business groups.
United Healthcare may also be known as "UnitedHealthcare" and United Health Group may also be known as "UnitedHealth Group."

A hard drive containing information on United Healthcare Medicare plan members was stolen from Futurity First Insurance Group. Member names, Social Security numbers, and in some cases, birth dates and private health information were exposed. Futurity First, United Healthcare’s sales and marketing services provider, sent the hard drive to a vendor for repair. The hard drive was stolen from the vendor on or around June 28 - July 28 and reported stolen on August 12. Futurity First then told United Healthcare on September 14.

**UPDATE (10/30/2011):** Three additional organizations were affected by the breach. A total of 705 members from Mutual of Omaha Insurance Company, 1,631 United of Omaha Life Insurance Company enrollees, and 3,994 United Health Group Health Plan in Minnesota enrollees were also affected in addition to the 582 originally reported. Information from the Health and Human Services website also reveals that the hard drive was lost on July 28.

**UPDATE (11/4/2011):** A total of 690 American Continental Insurance Company members from Tennessee were also affected by the breach.

---

**Genentech Inc.**
San Francisco, California

Customers with questions may call (888) 829-6553.

An unauthorized person may have gained access to Genentech's list of personal information for patients who used Genentech assistance to pay for their drugs. The breach was discovered on August 17. Names, Social Security numbers, addresses, phone numbers, dates of birth, email addresses, driver's licence numbers, medical information, and health insurance information may have been exposed.

---

**TechCentral**
Arlington, Texas

A laptop was stolen from an employee on August 27. It contained the names, Social Security numbers, and credit card account numbers of some customers. Notifications were mailed on September 28.

---

**Community & Southern Bank**
Alabama, Georgia

Multiple branches in Atlanta were affected.

An employee who worked at three different branches for Community & Southern Bank was indicted on five counts of theft by taking and seven counts of identity fraud. The dishonest employee was fired after an internal audit uncovered discrepancies. Police allege that the employee took $60,000 from client bank accounts, and the total taken could be more than $100,000 if fraudulent loans are included. Most customers who were affected had fraudulent withdrawals and loans under $1,000.

---

**St. Joseph Medical Center, Baxter, Baker, Sidle, Conn & Jones**
Towson, Maryland

A Baltimore law firm called Baxter, Baker, Sidle, Conn and Jones lost a hard drive with patient records. It contained patient names, Social Security numbers, medical records, addresses, dates of birth, and insurance information. The law firm was using the medical records of patients who were suing a cardiologist at St. Joseph Medical Center. The hard drive was lost by an employee during travel on August 4. Patients were informed in early October.

---

**Indiana University School of Optometry**
Bloomington, Indiana

(No Social Security numbers or financial information reported)
Health information stored on a computer server was accidentally made available to the public online between August and September of 2011. Patients who were seen by a former faculty member of the school were affected because of a configuration error that occurred on August 12. The issue was discovered on September 9 and had been corrected by September 10. Patients seen by a certain doctor between January of 2007 and June of 2011 at clinics in Carmel and Indianapolis, Indiana were affected. Some hospital inpatients seen between August 2007 and August 2008 were also affected.

Information Source: Media
October 10, 2011 University of Georgia (UGA) Athens, Georgia
EDU DISC 18,931

A data file that contained employment information such as names, Social Security numbers, dates of birth, dates of employment, gender, race, home phone numbers, and addresses was accidentally placed on a publicly available web server. The information was available from 2008 until 2011. Faculty and staff who worked at UGA in 2002 were affected.

Information Source: Media
October 7, 2011 The Nemours Foundation Wilmington, Delaware MED PORT 1.6 million

Three unencrypted computer backup tapes were reported missing on September 8. The tapes were stored in a locked cabinet, which had been temporarily relocated on or around August 10 for a facility remodeling project. The cabinet was not found. The tapes had been stored in the cabinet since 2004 and contained patient information stored between 1994 and 2004. Names, Social Security numbers, addresses, dates of birth, insurance information, medical treatment information, and direct deposit bank account information were exposed.

UPDATE (10/12/2011): Patients and their guarantors, vendors, and employees at Nemours facilities in Delaware, Pennsylvania, New Jersey, and Florida were affected. In addition to medical treatment information, the payroll information of current and former employees was exposed. Nemours took steps to encrypt all computer backup tapes and move non-essential computer backup tapes to a secure, off-site storage facility after the breach.

Information Source: PHIPrivacy.net
October 7, 2011 James A. Haley Veterans Hospital Tampa Bay, Florida MED PHYS Unknown

Hundreds of paper patient forms were compromised in May. An off-duty Tampa police officer discovered the records in a Motel 6 in May. The occupants of the motel room were detained on identity theft charges. The forms contained patient names, Social Security numbers, and dates of birth. The papers included Turbo Tax cards, receipts, and medical records from the Veterans Affairs hospital. At least one veteran had a fraudulent debit card charge.

Information Source: PHIPrivacy.net
October 3, 2011 Dentistry at the Crest Aurora, Colorado MED PHYS Unknown

Hundreds of sensitive dental patient records were found by a street Sweeper. They were scattered near a dumpster behind a shopping center. The records appear to be from a dental practice in Lone Tree, a 20 mile journey. The party responsible for the breach is unknown. Billing records with patient names, Social Security numbers, dates of birth, and addresses were exposed.

Information Source: PHIPrivacy.net
September 30, 2011 First Priority Life Insurance Company, Blue Cross of Northeastern Pennsylvania, Penn Foster Scranton, Pennsylvania MED PHYS 500

Around 500 employees were affected by the home theft of a laptop and sensitive papers. A Blue Cross business associate took home reports that contained names, Social Security numbers, and addresses of First Priority policyholders. The reports and laptop were stolen while the home was vacated due to flooding. The laptop was recovered a few days later.

Information Source: PHIPrivacy.net
September 30, 2011 Florida Hospital Orlando, Florida MED INSD 12,000

Patients with questions may call (855) 366-0141. Patients in Orange, Osceola, and Seminole counties were affected.

Patients who visited emergency departments of three Central Florida county Florida Hospitals between January 1, 2010 and August 15, 2011 may have had their information improperly accessed by one or more employees. Patient names, Social Security numbers, dates of birth and insurance information were exposed. Several employees were fired for
misconduct, but one employee was fired for viewing patient information without authorization for the purpose of identifying motor vehicle accident victims. The hospital launched an investigation after a car-accident victim felt that a soliciting attorney had somehow obtained his medical information.

**UPDATE (10/19/2011):** The FBI is now investigating the disclosure of patient information. It appears that three employees sold accident victim data to an attorney referral service. Former patients have also been contacted by funeral homes and at least one patient became an identity theft victim.

**UPDATE (08/18/2012):** One dishonest employee who worked at Florida Hospital Celebration allegedly viewed the emergency room records of 763,000 patients. A total of 12,000 patients from the group of 763,000 were contacted by the Hospital and notified of the risk of identity theft.

**UPDATE (10/22/2012):** The former employee worked at Florida Hospital from July 2006 until July 2011 and was responsible for registering emergency patients. The scam involved patient phone referrals to a lawyer or chiropractor who knew details about car accidents and hospital treatments. The dishonest employee had illegally gathered the patient information during emergency visits. He pleaded guilty to conspiracy to obtain health information and wrongful disclosure of health information.

**UPDATE (01/07/2013):** A man associated with Metro Chiropractic and Wellness Center and City Lights Medical Center pleaded guilty to charges related to illegally obtaining patient information from two spouses who worked at Florida Hospital Celebration. He was charged with one count of conspiracy to defraud the United States and four counts of making a payment to a non-licensed physician.

**UPDATE (04/12/2013):** One former patient affected by the breach has brought a lawsuit against Adventist Health System/Sunbelt, Inc. Florida Hospital Celebration and 36 other hospitals compose the Adventist network. The former patient is alleging that their privacy rights as a patient were violated when Adventist Health System/Sunbelt Inc. failed to prevent emergency room works from selling access to their medical records.

**UPDATE (07/12/2013):** The lawsuit that was filed in April was dismissed by a judge on July 3. Another lawsuit was then filed in Orange County Circuit Court in Orlando.

Information
**Source:** PHIPrivacy.net

September 30, 2011

TRICARE Management Activity (formerly Civilian Health and Medical Program of the Uniformed Services, CHAMPUS), Science Applications International Corporation (SAIC)

SAIC may be contacted at (855) 366-0140 for domestic calls and (952) 556-8312 for international calls. SAIC’s website is [http://www.saic.com/](http://www.saic.com/)

The car theft of backup tapes resulted in the exposure of protected health information from patients of military hospitals and clinics. Uniformed Service members, retirees and their families were affected. Patient data from the military health system that dates from 1992 to September 7, 2011 could have been exposed. The personally identifiable and protected health information of those who received care in the San Antonio area military treatment facilities and others whose laboratory workups were processed in these facilities was exposed. It includes Social Security numbers, addresses, phone numbers, clinical notes, laboratory tests, prescriptions, and other medical information. The information was stolen from the car of an SAIC employee, along with a stereo system and a GPS device on September 13.

**UPDATE (10/16/2011):** Four people have filed a $4.9 billion lawsuit over the improper disclosure of active and retired military personnel and family data. The lawsuit would give $1000 to each of the 4.9 million affected individuals.

**UPDATE (11/4/2011):** SAIC reported that 5,117,799 people were affected by the breach.

**UPDATE (01/06/2012):** A second class action lawsuit filed in the Superior Court of California in San Diego seeks unspecified monetary damages related to the theft of the computer tapes targets SAIC. The suit was filed in December and seeks certification as a class action for all TRICARE beneficiaries in California whose personal identity and health care information were compromised by the September 2011 theft of the tapes.

**UPDATE (03/14/2012):** Some of the people affected by the breach have become victims of identity theft. The class action lawsuit against the Department of Defense and SAIC was amended to reflect the new information about fraudulent charges appearing on credit cards.

**UPDATE (04/08/2012):** SAIC’s insurance will most likely be enough to cover any judgments or settlements that result from the data breach. SAIC also revealed that the Office for Civil Rights in the Health and Human Services Department opened an investigation into the tape theft on November 17, 2011.

**UPDATE (07/10/2012):** Eight class action lawsuits have been consolidated into one case alleging that personal information was mishandled. The case will be handled by the U.S. District Court in Washington, D.C.

**UPDATE (5.13.2014):** On Friday, "a federal district judge dismissed the majority of a consolidated class-action lawsuit filed against the Department of Defense, its TRICARE health insurance program and a contractor following a 2011 data breach that affected over 4.7 million individuals.

In his ruling, U.S. District Judge James Boasberg wrote that the case raises "thorny standing issues regarding ... when is a consumer actually harmed by a data breach -- the moment data [are] lost or stolen or only after the data [have] been accessed or used by a third party?"

He noted that most courts "have agreed that the mere loss of data -- without evidence that [the information] has been either viewed or misused -- does not constitute an injury sufficient to confer standing," adding, "This court agrees" (Kolbasuk McGee, GovInfoSecurity, 5/13)."
Summit Medical Group, Emory Family Practice, Fountain City Family Physicians, Office of Dr. Kenneth Reese, Knoxville, Tennessee

Patients at the Summit Medical Group medical centers at Deane Hill and Northshore Drive were affected. Affected patients may call 865-212-0116.

The September 4 theft of documents from an employee's car resulted in the exposure of patient names and diagnoses. The car was parked at the employee's home. Summit Medical Group account numbers, dates of birth, primary physician's names, names of hospitals, and dates of discharges were exposed.

Fairview and North Memorial Hospitals, Accretive, Minneapolis,

The July 25 theft of a laptop resulted in the exposure of patient information. It was stolen from a rental car parked in the parking lot of a Minneapolis restaurant. The laptop was in the possession of an employee of the contractor Accretive. It contained the names, addresses, dates of birth, medical information, and Social Security numbers of patients. A total of 14,000 Fairview patients were affected. Approximately 2,800 North Memorial patients were affected, but did not have their Social Security numbers exposed.

UPDATE (1/20/2012): A lawsuit was filed against Accretive Health, Inc. as a result of the breach. Approximately 23,500 patients in Minnesota were affected by the breach. The Minnesota Attorney General claims that Accretive failed to protect patient health care records and failed to disclose its extensive involvement in patient health care. According to the Minnesota Attorney General, Accretive gained access to sensitive patient data through contracts with the two hospitals and numerically scored patients' risk of hospitalization and medical complexity, graded their "frailty," compiled per-patient profit and loss reports, and identified patients deemed to be "outliers." The physical and mental health information included a checklist of 22 different chronic medical conditions that patients did or did not have. This was without the knowledge or consent of patients and the Attorney General argues that patients had the right to know how their information was being used and to have it kept confidential.

Accretive tells investors that its contracts with hospitals include risk scoring patients, reducing avoidable hospital admissions, identifying the sickest and most impact-able patients for proactive management, and identifying real-time interventions with significant revenue or cost impact. The lawsuit alleges that Accretive violated state and federal health privacy laws, state debt collection laws, and state consumer protection laws. It seeks an order requiring Accretive to fully disclose to patients: 1) what information it has about Minnesota patients; 2) what information it has lost about Minnesota patients; 3) where and to whom it has sent information about Minnesota patients; and 4) the purposes for which it amasses and uses information about Minnesota patients. In addition, the lawsuit asks Accretive to disclose whether it has sent health data about Minnesota patients to an offshore site in new Delhi, India and requests that restrictions be applied to how Accretive treats and uses patient data.

The press release from the Office of Minnesota Attorney General Lori Swanson can be found here.

UPDATE (08/24/2012): A settlement agreement with Accretive Health was announced at the end of July. The settlement requires Accretive to stop doing business in Minnesota for two years and to pay approximately $2.5 million to the State of Minnesota, a portion of which will be used to compensate patients.

Atlanta Perinatal Associates, Atlanta,

A former employee hacked into APA's database, copied patient information, and deleted APA's list. It is not clear exactly how the former employee was able to access the database, but the purpose was to benefit the former employee's new employer. Names, telephone numbers, and addresses of APA patients were taken. APA's competitor, SeeBaby, used the information to create a direct-mail marketing list.

UPDATE (1/10/2012): The former employee was sentenced to serve 13 months in prison for hacking into the competitor's computer in order to lure away patients.

Two Georges' Restaurant, Corpus Christi, Texas

At least 16 people reported fraudulent credit card charges after using their cards at the restaurant. The fraudulent charges total $20,000. The owners of the restaurant were evicted for not paying rent and have not been located. Former
employees of the restaurant are still waiting for their final paychecks.

Information
Source: Databreaches.net

September 24, 2011  Electronic Data Systems, Hewlett-Packard Enterprise Services, Alabama Department of Corrections
Montgomery, Alabama

A dishonest employee accessed the Electronic Data System's database of names and Social Security numbers of student loan borrowers. The former employee then used the information to file false tax returns in 2009. Sentencing is scheduled for December 19, 2011 and involves a minimum of two years in prison, a maximum of 354 years in prison, and a maximum fine of $6,250,000.

UPDATE (12/22/2011): The dishonest employee was sentenced to 94 months in federal prison for stealing the identities of student loan borrowers, and for giving them to a co-conspirator who used them to file false tax returns. Tens of thousands of names and Social Security numbers were stored at the employee's home.

UPDATE (12/17/2012): A second person was sentenced to federal prison for participating in the identity theft scheme. She worked in the central records office for the Alabama Department of Corrections and was able to provide other conspirators with sensitive information from state databases. She was sentenced to 50 months in prison for conspiracy, wire fraud, and aggravated identity theft. Restitution in the amount of $113,000 was also required.

Information
Source: Databreaches.net

September 23, 2011  University of Texas San Antonio (UTSA)
San Antonio, Texas

Students and prospective students who enrolled in or applied to courses in UTSA's Honors College may have had their information exposed. On August 2, a UTSA employee discovered that a system misconfiguration allowed unauthorized users to access names, dates of birth, addresses, phone numbers, email addresses, GPAs and other personal information of students and prospective students. Between June 20 and August 2, Honors College users as well as all other UTSA employees with access to the online system could view student information.

Information
Source: Databreaches.net

September 23, 2011  United States Steel and Carnegie Pension Fund, Benefits Administration Services
New York, New York

A CD with the names, Social Security numbers and dates of birth of U.S. Steel Mining retirees and dependents was lost in the mail. Benefits Administration Services (BAS) mailed the CD in August, but it was not received. BAS is still working with the U.S. Postal service to recover the CD.

Information
Source: Databreaches.net

September 23, 2011  Veterans Affairs Illiana Health Care System
Illiana, Illinois

Veterans with questions may call the VA Illiana's privacy officer at (217) 554-4943.

An appointment book was discovered missing on July 14. It contained the last names and last four digits of veterans' Social Security numbers. It is unclear where the book was taken from, but it is clear that it was not properly safeguarded.

Information
Source: PHIPrivacy.net

September 20, 2011  ProMedica
Toledo, Ohio

A mail sorting machine mistake caused sensitive information to be mailed to unintended patients. The breach was discovered when a patient opened a letter that contained her name and address, but the financial assistance application of a different patient. Names, addresses, dates of birth, phone numbers, and Social Security numbers were exposed.

Information
Source: PHIPrivacy.net

September 20, 2011  Good Samaritan Hospital
Baltimore, Maryland

A man posing as a vendor took two barrels of old X-ray film. The film contained medical data from over five years ago. It had been put aside for destruction or recycling. Authorities believe the thief wanted to extract the silver contained in the films.
A hacker or hackers were able to access Ashley Industrial Molding benefit plan information through AssureCare Risk Management (ARM) on August 9. It is unclear if this incident is related to the ARM incident reported here on August 12, 2011.

Patients with questions may call 1-877-698-2333.

Paper tracking records of tissue issued in orthopaedic surgeries performed at HJD in 2009 and 2010 were mistakenly discarded on or around June 23. It appears that the papers were then compacted and buried in a landfill rather than properly disposed. Patients who were affected had their name, date of birth, gender, hospital, date of surgery, and clinical surgery information exposed.

A May 22 office burglary resulted in the loss of three computers with patient information. Patient names, Social Security numbers, dates of birth, addresses, telephone numbers, and other personal information were exposed. A notification dated June 15 was posted on Yanez's website.

An external computer hard drive was stolen from a MedAsset employee's car on June 24. MedAsset provides administrative and business services to medical centers. The hard drive contained the personal information of patients who were being considered for governmental benefits at six Saint Barnabas acute care hospitals and patient information from Cook County Health and Hospitals System in Chicago. Patient names, medical center account numbers, medical record numbers, dates of birth, medical center charges, amount paid, health insurance information and discharge dates were exposed. Approximately seven percent of the Saint Barnabas System patients who were affected had their Social Security numbers exposed as well. The six Saint Barnabas Health Care System clinics are:

Clara Maass Medical Center - 8,795
Community Medical Center - 6,950
Kimball Medical Center - 6,785
Monmouth Medical Center - 6,443
Newark Beth Israel Medical Center - 15,015
Saint Barnabas Medical Center - 6,179
Also, 32,008 CCHHS patients were affected.
Hackers posted the names and email addresses of hundreds of U.S. Intelligence officials. At least 95 individuals with email addresses from the high security National Security Agency were affected, as well as many others in key positions at the White House, Pentagon, CIA, FBI, the Office of Director of National Intelligence and the State Department. Hundreds of executives at major government contracting firms that specialize in national security projects also had their names, emails, and possibly telephone numbers exposed and work addresses exposed. These organizations include Northrop Grumman, Boeing, General Dynamics, SAIC and CACI.

Information Source: Databreaches.net

September 17, 2011
Legislative Data Center
Sacramento, California
GOV HACK
50 (No SSNs or financial information reported)

Over 50 employees of the California State Assembly were warned that their personal information may have been obtained by a hacker. Some lawmakers were affected by the breach. On Friday, officials learned that one of the servers had been breached. It appears that the goal of the hacker or hackers was to overload the Capitol’s Internet service. People who participated in a flexible-benefits program were affected by the breach. The type of data exposed was not reported.

Information Source: Databreaches.net

September 16, 2011
Guilford County Tax Department
Greensboro, North Carolina
GOV DISC
1,000

On September 9, Guilford County became aware of the accidental placement of Tax Department files online. The names, bank account numbers, Social Security numbers, and addresses of citizens who had garnishments from the Tax Department were available online. The mistake affected people who submitted checks to the Tax Department between July 2010 and December 2010. The information was available as early as December of 2010 and taken down on September 9 of 2011.

UPDATE (9/16/2011): At least 1,000 people were affected by the breach.

Information Source: Databreaches.net

September 16, 2011
Xavier University
Cincinnati, Ohio
EDU PHYS Unknown

Sensitive student athlete medical records were misplaced by a coach who was transplanting them to an athletic event. A recently released prisoner found the documents and attempted to sell them back to the University for $20,000. The man was caught, pled guilty to extortion, and was sentenced to two years in prison.

Information Source: PHIPrivacy.net

September 16, 2011
Veterans Administration Medical Center (Biloxi)
Biloxi, Mississippi
GOV PHYS
1,814

The VA believes an employee’s office at the Veterans Administration Medical Center in Biloxi was inappropriately accessed without proper authorization on July 21. A number of medical files with veteran names, Social Security numbers, dates of birth and other personal information like medical diagnoses were found spread on the office floor. The breach could affect veterans, deceased veterans and VA employees in seven counties in southern Mississippi, four counties in southern Alabama, and seven counties in the Florida Panhandle.

Information Source: PHIPrivacy.net

September 15, 2011
United States Army
Alexandria, Virginia
GOV PORT
25,000

A CD with sensitive Non-Appropriated Fund retiree information was lost in the mail between Alexandria, Virginia and San Antonio, Texas. The CD never officially arrived after being sent during the last week of August. It contained retiree records with names, Social Security numbers, retirement date, type of retirement, amount of life insurance carried, term data, dates of service, and other retirement data.

Information Source: Databreaches.net

September 15, 2011
Montgomery County Department of Job and Family Services
GOV PORT
1,200
A flash drive with sensitive information was discovered missing on August 24. It contained the names and Social Security numbers of people who sought assistance from the Transition Center.

**Information**

**Source:** Databreaches.net

**September 15, 2011**

**Dayton, Ohio**

**GOV**

**PORT**

**1,200**

A flash drive with sensitive information was discovered missing on August 24. It contained the names and Social Security numbers of people who sought assistance from the Transition Center.

**Information**

**Source:** Databreaches.net

**September 15, 2011**

**Brandywine Healthcare Center**

**Winter Haven, Florida**

**MED**

**INSD**

**83**

A nurse was arrested and charged with grand larceny, ID theft, and scheming to defraud several elderly patients. The nurse collected patient information and texted it to a co-conspirator. The co-conspirator then used the information to obtain fraudulent tax returns in the names of the victims. Over 30 of the 83 victim records found at the co-conspirator’s home were from the Brandywine Health Center.

**Information**

**Source:** PHIPrivacy.net

**September 14, 2011**

**Bright House Network**

**St. Petersburg, Florida**

**BSR**

**HACK**

**Unknown**

Bright House servers which process Video on Demand (VOD) orders were breached. Historical customer data from as far back as June 22, 2011 was exposed. Customer names, addresses, phone numbers, and Bright House Network account numbers could have been exposed. Customers were notified in September.

**Information**

**Source:** Databreaches.net

**September 13, 2011**

**Bonney Lake Medical Center**

**Bonney Lake, Washington**

**MED**

**STAT**

**2,370**

An August 12 office burglary resulted in the loss of several computers and a main computer server with patient information. Patient names, Social Security numbers, addresses, insurance information, and medical records may have been exposed.

**Information**

**Source:** PHIPrivacy.net

**September 12, 2011**

**Vacationland Vendors, Inc.**

**Wisconsin Dells, Wisconsin**

**BSR**

**HACK**

**40,000**

Vacationland Vendors, Inc. arcade equipment used in Sevierville, Tennessee was also affected.

A hacker gained unauthorized access to Vacationland Vendors’ card processing systems at Wilderness Waterpark Resort in the Dells and Wilderness at the Smokies in Sevierville. The breach occurred on March 22. Customers who used a credit or debit card at one of the resorts between December 12, 2008 and May 25, 2011 were affected.

**Information**

**Source:** Databreaches.net

**September 12, 2011**

**McDonald’s**

**Monticello, Minnesota**

**BSR**

**INSD**

**Unknown**

A minor working at a McDonald’s drive-thru repeatedly used a skimming device to obtain the credit card numbers of customers. The dishonest employee swiped credit cards in the skimmer as customers paid for their meals throughout July and August. The credit card information was then used by identity thieves to create duplicate cards with false names. Investigators are actively looking for more victims. Those who may have been affected should call the Sheriff’s Office (763) 682-7733.

**Information**

**Source:** Media

**September 10, 2011**

**Tampa Signal**

**Tampa, Florida**

**BSR**

**INSD**

**Unknown**

The actions of at least one dishonest employee put the personal information of thousands of homeowners into the hands of identity thieves. People who purchased an ADT home security system through Tampa Signal in February may have had their information sold by one or more employees. The personal information exposed included Social Security numbers and dates of birth. Fraudulent tax returns were filed in the names of an unknown number of victims.

**Information**

**Source:** Databreaches.net

**September 9, 2011**

**Methodist Hospital**

**Houston, Texas**

**MED**

**PHYS**

**Unknown**

392
Three people are accused of using cancer and transplant patient files from Methodist Hospital to make fraudulent purchases. A dishonest employee took the birth dates and Social Security numbers of patients and passed them along to two co-conspirators. The trio then opened accounts and took out loans in the names of at least five patients. They face life in prison if convicted.

Information
Source: PHIPrivacy.net

September 9, 2011

Indiana University School of Medicine
Indianapolis, Indiana

EDU PORT

3,192 (178 cases of Social Security numbers)

A laptop with sensitive information was stolen from a physician's car on Tuesday, August 16 of 2011. It contained patient information such as name, age, sex, diagnosis, medical record number, and in 178 cases, Social Security numbers. Individuals were notified on September 2.

Information
Source: PHIPrivacy.net

September 8, 2011

Austin Center for Therapy and Assessment
Austin, Texas

MED PORT

1,870

Patients who have questions may call 282-2282.

The July 8 theft of a laptop resulted in the exposure of private patient information. Patient names, addresses, Social Security numbers and treatment information may have been obtained from the stolen laptop.

Information
Source: HHS via PHIPrivacy.net

September 8, 2011

Treatment Services Northwest
Portland, Oregon

MED STAT

1,200 (No SSNs or financial information reported)

A computer was stolen on or around July 29, 2011. It contained the protected health information of 1,200 patients who visited for outpatient alcohol and drug treatment services.

Information
Source: HHS via PHIPrivacy.net

September 8, 2011

Stanford University Hospital and Clinics
Palo Alto, California

MED DISC

20,000 (No SSNs or financial information reported)

The medical records of about 20,000 emergency room patients were posted on a commercial website for nearly a year. It is unclear how the spreadsheet with names, account numbers, admission and discharge dates, billing charges and diagnosis codes came to be on the website. The information was not financially sensitive. The website was called "Student of Fortune" and allowed students to pay for assistance with their school work. The spreadsheet was posted in relation to a question about how to convert the data into a bar graph. A former patient reported the availability of the spreadsheet on August 22.

UPDATE (10/3/2011): A class-action lawsuit for $20 million has been filed against Stanford University Hospitals and Clinics (SHC) and Multi-Speciality Collection Services, LLC (MSCS). It was filed on September 28 and about $1,000 for each of the 20,000 affected is sought. MSCS is a former billing vendor of SHC and was operating under a contract that specifically required it to protect the privacy of patient information.

UPDATE (10/5/2011): The source of the breach was confirmed by the Hospital and contractors. MSCS’s marketing agent sent the electronic spreadsheet to a job prospect as part of a skills test. The applicant asked for help through the Student of Fortune website.

Information
Source: PHIPrivacy.net

September 7, 2011

North Bay Regional Health Centre
Napa, California

MED INS

5,800 (No SSNs or financial information reported)
A privacy audit uncovered a breach caused by an employee. The employee accessed health information for persons other than those with whom they provided care. These inappropriate accesses date back to 2004. Only affected patients received a letter notifying them of the breach and offering suggestions for personal security.

**UPDATE** (03/02/2013): The employee was a registered nurse and will receive a hearing in June of 2013. No prosecution has occurred.

**Information**

**Source:** PHIPrivacy.net

**Recorded Date:** September 3, 2011

**Recorded Location:** New Horizons General Partnership

**City:** Granbury, Texas

**Medical:** MED

**Insurance:** INSD

**Recorded Cases:** 12

A couple who worked with New Horizons pleaded guilty to one count of conspiracy to commit false statements relating to health care matters. They each face up to five years in prison, a $250,000 fine, and the possibility of restitution. From at least January 1999 through April 2010, they defrauded the Texas Medicaid program by using the names and Social Security numbers of at least 12 inmates and other persons to create "ghost" employees for New Horizons. The false time sheets and inaccurate payroll reports allowed the couple to collect pay checks from the "ghost" employees. One member of the couple also submitted false claims for ICF/MR services to Medicaid. A total of $1,820,359 was fraudulently obtained from the Texas Medicaid program.

**Information**

**Source:** Databreaches.net

**Recorded Date:** September 3, 2011

**Recorded Location:** Texas Police Chief Association

**City:** Elgin, Texas

**Government:** GOV

**Hack:** HACK

**Unknown:** Unknown

Private emails from police officers and other information may have been exposed after the Texas Police Chief Association website was hacked. The hacking group Anonymous claimed responsibility for the attack as retaliation for the arrest of dozens of people suspected of being involved with Anonymous. Specifically, Anonymous claimed that "For every defendant in the Anonymous ‘conspiracy’ we are attacking two top Texas police chiefs, leaking 3GB of their private emails and attachments."

**Information**

**Source:** Databreaches.net

**Recorded Date:** September 2, 2011

**Recorded Location:** Pacific Retina Specialists

**City:** Seattle, Washington

**Medical:** MED

**Insurance:** INSD

**Recorded Cases:** 60

At least 60 patients had their records stolen by a billing technician during late 2010. The information included names, Social Security numbers, dates of birth, addresses and health insurance policy numbers. Many patients who used Medicare Advantage plans at the clinic were affected. The former employee and an accomplice also forged the names of three doctors on prescription forms. The patient prescription information was then used to obtain narcotic prescription drugs worth thousands of dollars. The former employee was sentenced to five years in prison.

**Information**

**Source:** PHIPrivacy.net

**Recorded Date:** September 1, 2011

**Recorded Location:** El Paso Independent School District (EPISD)

**City:** El Paso, Texas

**Education:** EDU

**Hack:** HACK

**Recorded Cases:** 72,000 (26 confirmed cases)

Hackers accessed the EPISD server and were able to collect the personal information of students, teachers and other employees. There were names, Social Security numbers, and addresses from approximately 63,000 students and 9,000 teachers on the district’s internal network (myepisd.org). EPISD was not aware of the breach until a computer security company noticed hackers bragging about breaking into EPISD’s system. Names, ethnicity codes, and student ID numbers for 26 students were posted by hackers named Sy5t3mF41lur3 & t3hblackhatter of H05t_Bu5t0rz.

**UPDATE** (09/07/2012): A hacker accused of carrying out the attack is scheduled to plead guilty to two counts of computer fraud and one count of fraud linked to identification documents.

**Information**

**Source:** Databreaches.net

**Recorded Date:** September 1, 2011

**Recorded Location:** Harvard University

**City:** Cambridge, Massachusetts

**Education:** EDU

**Disciplinary:** DISC

**Unknown:** Unknown

Harvard’s switch to Google "@college" email accounts resulted in the potential compromise of some student emails. Fewer than ten students reported that emails from other students with similar names were forwarded to them. The problem occurred because the email system did not distinguish between the older "@fas" accounts and the newer "@college" accounts. For example, the system would forward emails from ctucker@fas.harvard.edu to the new address of ctucker@college.harvard.com even if the "@harvard" email had been taken by a different student. Students with "@harvard" emails also had their emails forwarded to other students’ accounts.

**Information**

**Source:** Databreaches.net

**Recorded Date:** September 1, 2011

**Recorded Location:** Harvard University

**City:** Cambridge, Massachusetts

**Education:** EDU

**Disciplinary:** DISC

**Unknown:** Unknown

**Recorded Cases:** 0
Almost 14,000 documents related to drivers license and state identification applications were stolen from two separate offices over a total of two years. The applications included names, dates of birth, addresses, and in some cases Social Security numbers. The documents were stolen in May or June from secured areas at the North Macomb PLUS Office in Chesterfield Township and from the Southwest Macomb PLUS Office in Warren. The information dates back to 2009.

**Information**

Source: Databreaches.net

### September 1, 2011

**North Macomb PLUS Office, Southwest Macomb PLUS Office**

14,000 (Unknown number of Social Security numbers)

### September 1, 2011

**Birdville**

Haltom City, Texas

Two students may face criminal charges for hacking into the Birdville School District's network server and accessing a file with 14,500 student names and Social Security numbers. The students are a high school junior and a senior. Students who attended during the 2008-2009 school year may have been affected.

**Information**

Source: Databreaches.net

### August 27, 2011

**Avalon Centers**

Depew, New York

A former judge was arrested for making false statements to a federal agent. The former judge was attempting to reopen an eating-disorder clinic and tossed old records into a nearby dumpster in June of 2010. Authorities found 15 to 20 boxes of papers with patient names, Social Security numbers, addresses, dates of birth, medical complaints, medical diagnosis, treatment information and other health information. When a federal agent asked the former judge about the boxes, he responded that they contained business information without any sensitive medical information.

**Information**

Source: Media

### August 27, 2011

**The Lexington VA Medical Center**

Lexington, Kentucky

An employee took a laptop home without authorization. It contained patient names, dates of birth, the last four digits of patient Social Security numbers, and medical diagnoses. The employee's actions were not believed to be intentionally malicious.

**Information**

Source: PHIPrivacy.net

### August 27, 2011

**Living Healthy Clinic, University of Wisconsin - Oshkosh College of Nursing**

Oshkosh, Wisconsin

A computer security breach that occurred in July may have exposed the information of uninsured Winnebago County residents who sought health services. The information included names, Social Security numbers, addresses, and the health records of a limited number of people. The breach was discovered when University technology staff identified evidence of a computer virus on a desktop computer. There was no indication that unauthorized parties attempted to download information.

**Information**

Source: PHIPrivacy.net

### August 26, 2011

**Fidelity National Information Services, Inc. (FIS)**

Jacksonville, Florida

After breaking into FIS's network and gaining access to FIS's database, a group of criminals obtained 22 legitimate ATM cards. Copies of the cards were made and shipped to Greece, Russia, Spain, Sweden, Ukraine and the United Kingdom. The criminals altered the cards so that they could be used to withdraw an unlimited amount of cash. A total of $13 million was taken from accounts between the evening of Saturday March 5 and Sunday evening.

**UPDATE** (06/04/2013): An additional 7,170 pre-paid accounts may have been at risk. It appears that approximately 100 client financial institutions also had sensitive data exposed during the breach.

**Information**

Source: Media

### August 24, 2011

**Allianceforbiz.com, ShoWorks, Inc.**

Spokane, Washington

20,000 (No SSNs or financial information reported)
A hacker accessed a database of sensitive customer information. An Excel spreadsheet with usernames, passwords, email addresses, company names, and other types of personal or business information of 20,000 people was posted online on August 22. No credit cards were accessed and the website was closed until all passwords were changed.

**Information**
Source: Databreaches.net

August 23, 2011 **Berkshire Bank**
**Pittsfield, Massachusetts**

Customers with questions may call 1-800-773-5601.

Loan account numbers were printed on the outside of envelopes sent to customers. The account numbers were on the line just above customer name and address.

**Information**
Source: Databreaches.net

August 23, 2011 **Allstate Financial**
**Norwalk, Connecticut**

A personal financial representative lost his laptop on May 23, 2011, and then reported the loss to Allstate Financial on June 13, 2011. Customer policy information may have been stored on the laptop’s hard drive. On July 25, customers were notified that their policy information may have been exposed.

**Information**
Source: Databreaches.net

**New York, New York**

A programming error caused the names and Social Security numbers of current and former retirement plan enrollees to be accessible to unauthorized plan administrators. The error had existed in the database’s search function since October 2009. A plan administrator notified Lincoln Financial Group of the issue on July 18.

**Information**
Source: Databreaches.net

August 23, 2011 **Northwestern Counseling and Support Services**
**St. Albans, Vermont**

A thief stole a petty cash lockbox from Northwestern Counseling’s office sometime between June 18 and June 27. The lockbox contained cash, as well as itemized receipts with client Social Security numbers. Affected clients were notified of the breach in early July.

**Information**
Source: PHIPrivacy.net

August 23, 2011 **meridianEMR**
**Livingston, New Jersey**

On June 16, 2011, meridianEMR announced that it had filed a lawsuit against Intuitive Medical Software (UroChart). meridianEMR’s Advanced Monitoring System detected copying activities on meridianEMR’s server. meridianEMR immediately contacted Intuitive in response to the discovery. A second group called The Shappley Clinic was also accused of accessing meridianEMR’s data and placing patients in meridianEMR’s system at risk. The lawsuit contends that UroChart and another party have and have had unlawful access to patient information in violation of patient privacy rights. UroChart is accused of violating New Jersey’s Computer Related Offenses Act and behaving willfully and intentionally with malice.

**Information**
Source: PHIPrivacy.net

August 22, 2011 **Texas Health Presbyterian Hospital Flower Mound, Texas Health Partners Flower Mound, Texas**

Those with questions may call 1-855-419-1525.

An employee’s company-issued laptop was stolen on June 21, 2011. The theft was reported immediately, but the laptop was not recovered. It contained 1) physical descriptions such as age, gender, weight, and height, 2) medical information such as date and time of admission, date and time of laboratory order, lab results, dates of service, diagnosis, discharge instruction and summary, name of physician, insurance, procedure, room number, medical history, and medical record number, and 3) personal information that included employer, marital status, phone number, name of account guarantor, and Social Security number for a small number of patients.
A laptop was discovered missing while another breach was being investigated. The two breaches appear to be unrelated. Consultants may have had their names, addresses and bank account information exposed. At least 27 New Hampshire residents were notified of the breach, but the total number of affected people nationwide was not reported.

Information Source:
Databreaches.net

An unidentified suspected may have accessed the names, Social Security numbers, addresses, and bank account information of 28 consultants. The breach was discovered when commission funds were fraudulently transferred into an unfamiliar bank account; this occurred over two commission cycles in late 2010. The cause of the breach is not known.

Information Source:
Databreaches.net

Two laptop computers were discovered missing from Mount Sinai's office in Long Island City, Queens. A public notice was made on July 11 of 2011. The laptops contained the names, Social Security numbers and diagnosis information of patients. Mount Sinai encrypted all hard drives that contained confidential information in order to protect patients in the future.

Information Source:
PHIPrivacy.net

Member notifications of approval of medical procedures were sent to the incorrect addresses. Each approval letter contained the member’s name, address, service requested, and HPSM member ID number. The mistake was discovered on June 9, 2011 and the programming error that caused it was immediately fixed.

Information Source:
HHS via PHIPrivacy.net

Patients with questions may call a customer service representative at (573) 882-2013 or (573) 884-1983. Customer service representatives can also be reached at (800) 877 2372. More information is available at http://www.muhealth.org/ProtectedInformation.

On June 14, University of Missouri Health Care officials failed to receive an expected delivery of copies of patient billing information and immediately notified the University of Missouri Police Department. The package had been sent via private courier to University of Missouri Health Care from a Kansas City bank that serves as the clearinghouse for the University of Missouri Health Care’s billing. The package included copies of payments received by the bank between June 6 and June 13 and would have exposed bank account numbers, partial credit card numbers, names and addresses. Notification letters were sent on June 21. University of Missouri Health Care has terminated its contract with the courier responsible for delivering the missing package. Affected parties are advised to contact their banks or credit card companies and change their account or card numbers.

UPDATE (1/26/2012): Privacy Rights Clearinghouse received documentation that revealed people in Columbia were affected by the breach.

Information Source:
PHIPrivacy.net

Citigroup and Bank of America are both headquartered in New York, New York.

A breach of an unnamed merchant or merchants may have resulted in the exposure of customer credit and debit card information. Citigroup deactivated the credit cards of affected customers and notified them that Citigroup had been informed of a security breach at a retailer. Within a week, Bank of America also sent new debit cards to some customers after learning that some accounts may have been compromised at a merchant.
Hundreds of inmates could have viewed the names and Social Security numbers of guards at Fort Dodge. The information was located inside a desk in an area used as an inmate barber shop. The area was once used as an office, but the furniture was not checked, cleaned or removed before the conversion. The information had been sitting in the desk for three or four months before an officer found it.

A computer file containing the names and Social Security numbers of former faculty, staff and students was accidentally made accessible online. The file contained information from 1999 and could be located through a Google search for 10 months. A change in Google’s search engine made the file accessible from September 2010 to July 1, 2011. A person who performed a Google search on his name discovered the breach on June 30.

A BART Police Officers Association database was hacked. The names, postal addresses and email addresses of officers were posted online. A French national claimed responsibility for the hack and described the BART site as having zero security in place.

An unauthorized person broke into Purdue’s computer system on April 5, 2010, and tried to use the server to attack other servers. Purdue staff learned of the breach three days latter and began an assessment. The server was taken offline and staff later determined that Social Security numbers belonging to current and former students who took mathematics courses and a limited number of faculty, faculty family members and contractors were exposed. The Social Security numbers were then matched to their owners and notification was sent to the Attorney General’s office in June of 2011.

A server that contained data from school children in Wilson and Richmond counties was mistakenly put online. The information was gathered between 2003 and 2006 as part of a research study on classroom practices. It included names, Social Security numbers and dates of birth. A concerned parent notified the state Department of Public Instruction after finding the information online. The error was fixed in July, though it is unclear how long the information was available online.

Bethesda's website was hacked for the second time in three months. No groups have claimed responsibility for the hack. The breach affected Bethesda’s forum user database and occurred on the morning of August 12. Information in the database was encrypted, but all user forum passwords were reset as a precaution. Bethesda is recommending that users alter their passwords for other sites if they were similar to the ones used in the forum.
Anonymous has claimed responsibility for a hack of BART’s user database. A list with the first and last names, email addresses, passwords, phone numbers, full addresses and other personal information of MyBart.gov users was posted publicly. MyBart.gov users should change their login information for other sites if they used the same login information for MyBart.gov.

Anonymous exposed the security holes in BART’s database in order to protest BART’s temporary suspension of wireless service throughout BART stations. BART had already been criticized for disabling wireless service in an attempt to counter protests over a fatal officer-involved shooting. The MyBart.gov homepage was also defaced.

Information Source: Databreaches.net

August 13, 2011 University of Hawaii - Kapiolani Community College
Honolulu, Hawaii

EDU PHYS 2,000

A worker noticed that boxes of sensitive financial records were out of place. Some boxes were discovered to be missing and officials began searching for them on July 1. The breach was reported to students during the first week of August. It is unclear when the boxes were taken and there was no sign of forced entry into the area where they were stored. The files contained names, addresses, Social Security numbers and credit cards. People who made transactions with credit cards between February and November of 2010 for non-credit classes, transcript requests, or payment of non-resident fees were effected.

Information Source: Databreaches.net

August 13, 2011 St. Francis Hospital
Wilmington, Delaware

MED PORT 474 (No SSNs or financial information reported)

Those with questions may call (855) 831-4185 or (302) 421-4185.

A doctor lost a thumb drive that contained the personal health care information of 474 maternity patients. It did not contain names, financial information or SSNs. The thumb drive was returned to the doctor on June 11 by an anonymous sender. The doctor had not realized it was missing and reported the incident to St. Francis on June 13. The doctor was authorized to remove the thumb drive from the Hospital, but it should have been encrypted and password protected.

Information Source: PHIprivacy.net

Plymouth, Minnesota

BSF HACK 25,330

The location listed is that of Assurecare Risk Management Inc. Though 25,330 Gypsum employees were affected, the total number of individuals affected across companies was not reported.

Reznick’s former service provider AssureCare reported a breach of a server that contained Reznick information. The information from employee benefits plans from 2001 to 2006 could have been accessed by outside parties. Current and former employees and their spouses may have had their names, Social Security numbers, addresses, dates of birth and medical information exposed. The server was accessed by external intruders on May 9 and May 10 of 2011.

UPDATE (10/13/2011): Employees enrolled in Gypsum’s health and dental care plans were also affected.

Information Source: PHIprivacy.net

August 11, 2011 Country Corner Market
Amherst, Virginia

BSR HACK 125

A hacker or hackers were able to access Country Corner’s website and obtain customer information. Customers may have been tricked into giving their financial information through emails that appeared to be from Country Corner, a fake Country Corner website set up by hackers, or some other method of phishing. It is also possible that customer data was taken directly from Country Corner’s computer system. Customers began reporting fraudulent charges and Country Corner’s computer system was discovered to contain malware.

Information Source: Databreaches.net

August 11, 2011 TGI Fridays
Laurel, Maryland

BSR INSD 73

A former waiter was indicted on charges of copying and selling the numbers from 73 customer credit cards. The 16 charges include theft, identity theft, and conspiracy to commit theft. The former employee is believed to have used a
skimmer to copy the credit card numbers of restaurant patrons between December of 2009 and April 2010. The employee was caught when two Secret Service employees who had eaten at the restaurant noticed unauthorized charges on their credit cards.

Information Source: Databreaches.net
August 11, 2011 Energy Federation, Inc. Westborough, Massachusetts BSO HACK 20

Two malware pieces were discovered on Energy Federation’s server on July 12. They appear to have been inserted on July 7 and July 10. The purpose of the malware was to collect information on the server. Customer names, credit card numbers and expiration dates, but contact information could have been exposed. At least 20 New Hampshire residents were affected by the breach, but the total number of affected customers nationwide was not revealed.

Information Source: Databreaches.net
August 11, 2011 Eye Safety Systems Sun Valley, Idaho BSR HACK Unknown

A May 2011 website breach of a third party vendor may have compromised the credit card transaction data of Eye Safety Systems’ customers. Customer names, phone numbers, email addresses, addresses, and credit card information may have been accessed. Customers were notified on May 28 and Eye Safety Systems took measures to improve online security.

Information Source: Databreaches.net
August 10, 2011 Department of Social and Health Services - Washington Seattle, Washington GOV DISC 3,950 (No SSNs or financial information reported)

A coding error caused mailing mistakes to be made in July. Medical enrollment forms with the addresses of custodial parents were sent to non-custodial parents. However, no addresses were disclosed in cases involving foster care of domestic violence.

Information Source: Databreaches.net
August 10, 2011 Cal Poly Pomona Pomona, California EDU DISC 38

On August 2, a lecturer working in a student lab discovered that two files on a server could be accessed by faculty members, staffers and students from the College of Business Administration. The files were confidential and included personal information such as names and Social Security numbers. A total of 38 current and former faculty members were affected by the breach. The University determined that the information had not been digitally copied by anyone.

Information Source: Databreaches.net
August 10, 2011 University of Wisconsin - Milwaukee Milwaukee, Wisconsin EDU HACK 79,000

On May 25, University technology staff learned that unauthorized individuals had installed computer viruses on a University server. It housed a software system for managing confidential information. The names and Social Security numbers or people associated with the University could have been exposed. There was no evidence that unauthorized parties had attempted to download the confidential information.

Information Source: Databreaches.net
August 9, 2011 McDonald’s Norfolk, Virginia BSR INSD 185

A cashier pleaded guilty to conspiracy to commit access device fraud and aggravated identity theft. The cashier was part of a group of friends who used stolen credit card numbers to make $50,000 in purchases. The cashier’s job was to swipe customer debit and credit cards while working at McDonald’s.

UPDATE (2/03/2012): The man who was the ring leader of the credit card scam and recruited the McDonald’s employee was sentenced to seven years in federal prison on February 3. He reportedly paid a female employee $10 for each credit card she swiped at the restaurant. About 185 customers were affected and $163,000 in fraudulent charges were made. The dishonest employee pleaded guilty and was sentenced to two years in prison. Three other people were sentenced for their involvement, but the extent of their involvement was not revealed. A fourth remains a fugitive.
August 8, 2011  **Department of Veterans Affairs**  
**Fayetteville, North Carolina**  

A dishonest VA worker used his tax return preparation business to submit fraudulent tax returns. VA patient personal information such as names, Social Security numbers and birth dates were used to create fake dependents on people's tax returns. The VA worker then collected fees from customers in exchange for fraudulently increasing the dollar amount of their tax returns. He was convicted in February and sentenced to 11 years in federal prison. The employee handled information from VA patients in North Carolina and Virginia.

Information Source:  
**PHIPrivacy.net**  

August 5, 2011  **The Brigham, Women's/Faulkner Hospital**  
**Boston, Massachusetts**  

Patients who have questions may call 877-694-3367.

A physician who worked for both hospitals left an external hard drive in a piece of luggage. The luggage was lost in a cab on or around June 21. Information related to inpatient hospital stays from July 10, 2009, to January 28, 2011, may have been on the hard drive. The types of information that could have been on the device include patient names, medical record numbers, dates of admission, medications, and information about diagnosis and treatment.

Information Source:  
**PHIPrivacy.net**  

August 4, 2011  **University of Arizona**  
**Tucson, Arizona**  

A hacker accessed the employee listserv on or around August 4. This allowed an unauthorized party to send an offensive photo and additional lewd messages through the University's mailing list. The listserv is normally only used by administrators to transmit official University business. It is unclear if any information was exposed.

Information Source:  
**Databreaches.net**  

August 3, 2011  **Franklin County Children Services, Parenthesis Family Advocates**  
**Columbus, Ohio**  

A boxes of files were found by a recycling bin. The files contained sensitive information from children with Franklin County Children Services. Medical information, criminal records and other personal documents were left out in the open. The papers have been linked to someone with access to Parenthesis' documents; however the cause of the breach is unknown.

Information Source:  
**Databreaches.net**  

August 3, 2011  **Department of Veterans Affairs**  
**Washington, District Of Columbia**  

The inspector general at the VA found that IT contractors had accessed the VA's electronic health record system without appropriate security clearances. An tipster had left a message about the situation on a departmental hotline in the summer of 2010. Contractor personnel were found to be improperly sharing user accounts when accessing VA networks and the Veterans Health Information System and Technology Architecture systems. Employees of the contracting company were unaware of proper IT security protocol.

Information Source:  
**PHIPrivacy.net**  

August 2, 2011  **Pocatello Family Medicine, Idaho State University**  
**Pocatello, Idaho**  

The firewall protecting computerized records was accidentally left inactive for nine months. It was disabled during maintenance in August of 2010, but was never restored. The problem was discovered when IT staff assisted an employee on May 18, 2011. It appears that an electronic medical record for the clinic that was stored on the server was never accessed during that time. Other information on the server included scanned images of drivers licenses and insurance cards. There is also no evidence that these records were accessed, downloaded or printed. It does appear that someone downloaded movies and a television program onto the site in order to use the storage space and illegally sell access to the material.

**UPDATE** (05/22/2013): The information of 17,500 patients was exposed. The Department of Health and Human Services released a resolution agreement on May 21 for HIPAA violations related to the breach. The release can be found here: [http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/isu-agreement.pdf](http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/isu-agreement.pdf)
UPDATE (05/30/2013): The University of Idaho agreed to pay $400,000 and upgrade security procedures in the settlement agreement.

Information Source: PHIprivacy.net

August 2, 2011 SilverPop
Atlanta, Georgia

A laptop that contained information related to SilverPop's Health and Welfare Plan was stolen on April 15. Affected individuals may have had their protected health information exposed.

Information Source: HHS via PHIprivacy.net

August 2, 2011 New River Health Association
West Virginia

The disclosure of sensitive paper records resulted in unauthorized access to personal information. The breach either occurred or was discovered around April 1, 2011.

Information Source: HHS via PHIprivacy.net

August 1, 2011 City of Pittsburgh
Pittsburgh, Pennsylvania

Someone obtained employee names, addresses and possibly Social Security numbers. Fraudulent accounts could be set up with this information. Multiple city employees from different departments received bills from PayPal for purchases they did not make. The fraudulent charges range from $40 to $3,000. It is not clear how the thieves accessed Pittsburgh city employee information. Police officers and other Department of Public Safety employees are among those who were affected.

Information Source: Databreaches.net

August 1, 2011 University of North Carolina - Chapel Hill
Chapel Hill, North Carolina

Someone broke into the UNC-Chapel Hill judicial office and took the files of 30 students. The break-in was discovered at the beginning of the day on Monday. University student affairs officials contacted each of the students who had their records stolen.

UPDATE (8/9/2011): A suspect was caught. He was arrested on charges of breaking-and entering, larceny and possession of stolen goods.

Information Source: Databreaches.net

August 1, 2011 Mills-Peninsula Medical Center
Burlingame, California

A relative of a mail room employee discovered sensitive documents at the employee's residence and returned them in June of 2011. The employee had taken home medical documents between November of 2009 and September of 2010. The records consisted of patient names and diagnostic test results. Fifteen of the documents included patient addresses and insurance identification or Social Security numbers. The employee was fired.

UPDATE (10/22/2011): A total of 1,438 people were affected by the breach. The former employee was charged with embezzlement and forgery. She claims that she was overwhelmed with sorting the documents at work and that she planned to dispose of them properly.

Information Source: PHIprivacy.net

July 31, 2011 Ascensus
On April 15, 2011, law enforcement notified Ascensus of a cyber attack that had affected Ascensus' network and those of other companies. The virus was determined to be a new type of malware and was immediately blocked from Ascensus' network. However, the virus created and may have been able to export files with client names and Social Security numbers.

**Information Source:** Databreaches.net

**July 31, 2011**

**Tufts University, Massachusetts General Hospital (MGH)**

**Boston, Massachusetts**

EDU PORT Unknown

A research associate's laptop was stolen during the course of research with a Tufts professor. The research was being conducted at MGH. The laptop was mostly used for research, but a sensitive file had been uploaded in early 2010. It contained a spreadsheet with the information of applicants who applied to the Graduate School of Arts and Sciences at Tufts. Applicant Social Security numbers were included in the spreadsheet. The theft occurred in April of 2011 and was reported to MGH. Tufts learned of the breach on June 16, 2011.

**Information Source:** Databreaches.net

**July 30, 2011**

**Chase Bank**

**Rancho Peñasquitos, California**

BSF CARD 950

A man was charged with using a skimming device to take over $200,000 from customer accounts. He was arraigned on 45 counts of identity theft, grant theft, burglary, making fake ID cards and causing losses that exceeded $200,000. He was caught when bank investigators discovered that someone was installing an ATM skimming device on the door of the bank’s ATM lobby every Saturday after closing. The device was then removed by the thief early on Mondays. This happened for at least six consecutive weeks. Hidden cameras were also used to record customer pins at the ATMs. Agents were able to arrest the man as he returned to retrieve the skimming device.

**Information Source:** Media

**July 30, 2011**

**Belmont Savings Bank (BSB)**

**Boston, Massachusetts**

BSF PORT 13,000

Belmont Savings Bank has agreed to pay a fine of $7,500 related to a consumer data breach case with the Massachusetts attorney general’s office. In May, a bank employee left a backup tape on a desk rather than storing it. A cleaning crew disposed of the tape later that night. Names, Social Security numbers and account numbers were exposed. The tape contained the personal information of over 13,000 customers, but is believed to have been incinerated after disposal along with other sensitive materials from BSB.

**Information Source:** Databreaches.net

**July 30, 2011**

**Nyack Hospital**

**Nyack, New York**

MED PORT 1,400

The hospital theft of a hard drive resulted in the exposure of current and former employee information. The names, Social Security numbers, addresses, dates of birth and other information related to employees and their families were on a human resources department computer. A flood on June 23 caused the HR department to temporarily relocate. Workers returned on July 6 and discovered that the hard drive had been stolen. The information dates back at least 12 years.

**Information Source:** Databreaches.net

**July 30, 2011**

**Wellness Centers of Atlanta**

**Alpharetta, Georgia**

MED PHYS Unknown

Patient records were left in an abandoned pain clinic. The new owner reported the discovery to police. Hundreds of files with medical information of former patients were discovered. It is unclear if anyone else accessed the information.

**Information Source:** PHIPrivacy.net

**July 26, 2011**

**Lincoln National Life Insurance Company, Lincoln Life & Annuity Company of New York**

**New York**

BSF DISC 705

On April 29, an employee accidentally attached a sensitive file to an encrypted email that was sent to a third-party payroll provider. It contained the names and Social Security numbers of pension plan participants of multiple payroll vendors. The error was discovered on May 17, and notifications were sent in July.

**Information Source:** Databreaches.net

**July 31, 2011**

**Dresher, Pennsylvania**

On April 15, 2011, law enforcement notified Ascensus of a cyber attack that had affected Ascensus' network and those of other companies. The virus was determined to be a new type of malware and was immediately blocked from Ascensus' network. However, the virus created and may have been able to export files with client names and Social Security numbers.
<table>
<thead>
<tr>
<th>Date</th>
<th>Company</th>
<th>Location</th>
<th>Sector</th>
<th>Type</th>
<th>Source</th>
<th>Records Used in Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 26, 2011</td>
<td>Esteé Lauder</td>
<td>New York, New York</td>
<td>BSR</td>
<td>PORT</td>
<td>Unknown</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>A company-issued laptop was determined to be missing. A notification letter was sent to current and former employees on July 13. Names and Social Security numbers were exposed. The number of employees affected is unclear.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Information Source:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Databreaches.net</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>July 26, 2011</td>
<td>University of Nevada - Las Vegas (UNLV)</td>
<td>Las Vegas, Nevada</td>
<td>EDU</td>
<td>HACK</td>
<td>2,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Current and former UNLV employees may have been affected by a breach. It is possible that an unauthorized user gained access to a former employee's computer in December of 2008. Employee information that included Social Security numbers would have been exposed. The potential breach was discovered in 2011 during maintenance on a computer in UNLV's Controller's Office.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Information Source:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Databreaches.net</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>July 23, 2011</td>
<td>Margarita's Mexican Restaurant</td>
<td>Huntsville, Texas</td>
<td>BSR</td>
<td>HACK</td>
<td>Unknown</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>A number of people reported fraudulent debit and credit card purchases. The problems were traced back to a Margarita's computer that had been infected by a virus. Investigators discovered that criminals had sold a number of the customer credit and debit card numbers that were stolen from the system. Margarita's had no obvious security flaws at the time of the breach and has since upgraded its firewall protection.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Information Source:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Databreaches.net</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>July 21, 2011</td>
<td>StudentCity.com</td>
<td>Peabody, Massachusetts</td>
<td>BSR</td>
<td>HACK</td>
<td>266</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Several customers reported problems with their credit and ATM cards after purchasing vacation trips on the website. Customer names, passport numbers and dates of birth were also exposed. The breach appears to be the result of a hacking attack. StudentCity.com first became aware of the problem on June 9. Though 266 New Hampshire residents were affected by the breach, the total number of affected US customers was not reported.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Information Source:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Databreaches.net</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>July 21, 2011</td>
<td>Zpizza</td>
<td>Irvine, California</td>
<td>BSR</td>
<td>HACK</td>
<td>Unknown</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Zpizza was affected by malware on the point of sales system used to process credit and debit card transactions. The breach affected customers who used their credit or ATM cards between September of 2010 and January of 2011 at 12 locations. Customers in California, Montana and Virginia were affected.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Information Source:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Databreaches.net</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>July 21, 2011</td>
<td>Extreme Pizza</td>
<td>San Francisco, California</td>
<td>BSR</td>
<td>HACK</td>
<td>Unknown</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>The stores that were affected by the breach include those in Berkeley, CA on College Ave. and Shattuck Ave., Dublin/Pleasanton, CA, Hercules, CA, Granite Bay, CA, Modesto, CA, Newark, CA, Pacifica, CA, Point Richmond, CA, Sacramento, CA, San Bruno, CA, San, Diego, CA in Point Loma, San Francisco, CA on Fillmore St., Folsom St., Union St., San Ramon, CA, Colorado Springs, CO in Co-North Academy, and Hillsboro, OR. On February 28, 2011 Extreme Pizza discovered that hackers had accessed the point of sales systems of several west coast franchises. The attacks occurred in August and the customer information was misused between that time and January of 2011.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Information Source:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Databreaches.net</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>July 21, 2011</td>
<td>Mountain Mike's Pizza</td>
<td>Martell, California</td>
<td>BSR</td>
<td>HACK</td>
<td>Unknown</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Widespread credit and ATM card fraud has been linked to a hack of Mountain Mike's Pizza. The website was infected by malicious software in October; it was detected and removed in April of 2011. Customers who paid by debit or credit card between October of 2010 and April of 2011 are advised to call their financial institution and have their debit or credit card number changed as a precautionary step.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Information Source:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
July 20, 2011  
**Swedish Medical Center**  
**Seattle, Washington**  
MED DISC 19,799

The full names and Social Security numbers of current and former employees were accessible online for nearly nine weeks. Employees who worked for Swedish, but not Swedish Physician Division, in 1994, 1995, 2002, 2003, 2004 and 2006 had their information posted sometime between the middle of April and June 17, 2011. The cause of the accidental disclosure was not reported.

July 18, 2011  
**Kitchen Place**  
**Norfolk, Nebraska**  
BSR PHYS Unknown

Items on display at a bankruptcy auction involving the Kitchen Place included two cabinets with customer information and shelved boxes with employee information. Past customer credit card and bank account numbers, methods of payment and home floor plans were kept in the cabinets. Shelves for sale carried boxes of employee information which included names, Social Security numbers and other personal and payroll information. Anyone looking over the auction items could have accessed the information. At least one person purchased an item that held customer information and subsequently dumped the papers in the parking lot.

July 18, 2011  
**Beth Israel Deaconess Medical Center**  
**Boston, Massachusetts**  
MED HACK 2,012 (No SSNs or financial information reported)

Patients may call 877-615-3765 for more information.

A vendor failed to restore computer security controls following routine maintenance. A virus was later discovered on a computer that contained names, medical record numbers, genders, dates of birth, and the date and name of radiology procedures for patients. The virus transmitted encrypted data files to an unknown location. The computer was cleaned and had its software re-installed to clear the virus.

July 16, 2011  
**College Choice, UPromise Investments**  
**Indianapolis, Indiana**  
BSF INSD 300

An employee with College Choice’s program manager UPromise Investments accessed names, Social Security numbers, dates of birth and other contact information for seven months while on the job. The former employee was in charge of withdrawals and deposits. It does not appear that the employee was able to withdraw money from any of the accounts in the Indiana plan. Security measures were in place that prevented the employee from printing or emailing the information.

July 16, 2011  
**DeKalb Medical - Hillandale**  
**Hillandale, Georgia**  
MED UNKN 7,500

Patients may call 855-294-2545 or visit [www.dekalbmedical.org](http://www.dekalbmedical.org) for more information.

Patient information was stolen from the Hillandale facility and used to file fraudulent tax returns with the Internal Revenue Service. Patients who visited DeKalb’s Hillandale facility between July and October 2010 may have had their information exposed. It appears that affected individuals between the ages of 17 and 20 were the group affected by the filing of fraudulent tax returns. The United States Secret Service alerted DeKalb and it is believed that the breach was just one of many similar breaches in Georgia and Alabama. DeKalb did not reveal how the information was taken.

July 15, 2011  
**University of Maryland Medical Center**  
**Baltimore, Maryland**  
MED INSD Unknown

A former employee of the University of Maryland Medical Center and three other people collaborated to steal the identities of patients. The former medical center employee allegedly stole the patient information of people who had paid for medical treatment between July 2009 and June 2011. His co-conspirators then used the information to open credit cards, obtain cash advances and make purchases in victims’ names. The four people were arrested and face a maximum sentence of 30 years in prison for conspiracy, in addition to charges related to bank fraud and aggravated identity theft.
UPDATE (10/12/2012): A former employee was sentenced to six months of home detention and ordered to pay $22,000 in restitution. He claimed that he took the patient records home in order to conceal work that he had not completed and submit false reports. At least two other people used the patient records to commit fraud.

Information
Source: PHIPrivacy.net

July 15, 2011  Psychiatric Times
Minneapolis, Minnesota  BSO  DISC  1,400 (No SSNs or financial information reported)

Users who responded to a survey on ethical dilemmas may have had their names and email addresses exposed for approximately 16 hours. The survey results were posted on the Psychiatry Times website on June 7th. The website post contained a link to the responses to the survey questions. This somehow provided enough information for the names and emails or respondents to be determined. The link was deleted and the survey was disabled shortly after the discovery. Users were notified of the error on June 10.

Information
Source: PHIPrivacy.net

July 14, 2011  Sky Harbor PHX
Phoenix, Arizona  BSO  CARD  10

At least 10 TSA employees who worked at the same terminal had their financial information stolen when they used their credit or debit cards at a compromised machine. Investigators are unsure of the scope of the breach.

Information
Source: Databreaches.net

July 13, 2011  Meridian Health System
Asbury Park, New Jersey  MED  PORT  Unknown

Jersey Shore University Medical Center in Neptune, Riverview Medical Center in Red Bank, Ocean Medical Center in Brick, Southern Ocean Medical Center in Stafford and Bayshore Community Hospital in Holmdel are all part of the Meridian Health System.

A laptop with employee information was taken from another employee's home on June 25. An unspecified amount of employee information was exposed.

Information
Source: Databreaches.net

July 13, 2011  Metropolitan Health District
San Antonio, Texas  MED  INSD  Unknown

Two San Antonio city employees pleaded guilty to charges related to using stolen Social Security numbers. One member of the couple stole Social Security numbers from patients at a Metropolitan Health District. Multiple Social Security cards with different numbers were found during a raid of the couple's home. The other member of the couple worked for the San Antonio Public Works Department.

UPDATE (12/17/2011): One member of the couple received five months in jail, five months of house arrest, and two years of federal supervision for her crimes and for violating her position of trust as a city employee. She had been hired to work as an administrative assistant for a tuberculosis program at the Metropolitan Health District clinic through a temp agency. The other member received five years of probation with six months of home confinement.

Information
Source: PHIPrivacy.net

July 13, 2011  Walgreens.com
Deerfield, Illinois  BSR  DISC  Unknown

Walgreens customers saw the prescription information of other customers when they attempted to log into their accounts on the Walgreens.com site. The website problem existed for at least two months and also allowed customers to see the phone numbers, names of prescribing doctors, names of medications, the amount the prescriptions were purchased for and the dates of the purchases. A customer alerted a local store to the problem, but had to contact the media when the problem persisted two months later.

Information
Source: PHIPrivacy.net

July 12, 2011  Toshiba, Toshiba America Information Systems, Inc. (TAIS)
Irvine, California  BSR  HACK  7,971 (No SSNs or financial information reported)
Eleven admin email addresses with corresponding plain-text passwords and ID numbers were posted online. A total of 451 email addresses and plain-text passwords were posted. The hacking group VOID claimed responsibility.

**UPDATE (7/18/2011):** Toshiba confirmed that records of 7,520 customers were hacked. Customers may have had their email addresses, passwords and phone numbers taken. It was confirmed that 681 customers had their email addresses and passwords taken.

Information
Source: Databreaches.net

**July 12, 2011**

**Colorado Springs Hospital - Memorial Health System**
**Colorado Springs, Colorado**

A nurse from the occupational health clinic accessed the records of 2,500 Memorial Hospital patients without cause. The nurse had access to patient records through Physician Link, but was not a Memorial employee, and had no medical or work-related reason for accessing the records. She was fired and claims to have used the database to look up contact information for family and friends, as well as for other reasons. The nurse also feels that she was singled out and claims that many other employees in the medical community use databases in this way.

Information
Source: PHIPrivacy.net

**July 9, 2011**

**Geoff Gray Corporation (GGC)**
**Hampstead, New Hampshire**

GGC became aware of a potential security breach that could have occurred between June 9 and June 14. A server collocated by 14Market may have been disabled by an outside party sometime during this time frame. It appears that any attempt to hack information from the server during this time failed. Notification letters were sent to customers on July 5.

Information
Source: Databreaches.net

**July 8, 2011**

**Universal Music**
**Universal City, California**

An attack by the hacktivist group Anonymous resulted in the exposure of user names, and passwords. Anyone who signed up on the Universal Music website in order to receive updates about musicians was affected. Anonymous hacked the website as part of its AntiSec campaign, the goal of which is to expose weak spots in the internet security of governments and large businesses.

Information
Source: Databreaches.net

**July 8, 2011**

**All Pets Club**
**Branford, Connecticut**

An All Pets Club in Branford, Connecticut and an All Pets Club in Wallingford, Connecticut were affected.

A hacker infiltrated All Pets Club's computer system. Customer credit card numbers are encrypted after the computer system stores them, but are vulnerable for a short time once they have been swiped. The hacker was able to access the credit card numbers as they were swiped. Police reported that a significant portion of the complaints about fraudulent credit charges in the Branford area have come from All Pets Club customers during the past few months.

Information
Source: Databreaches.net

**July 8, 2011**

**Kiplinger Washington Editors Inc.**
**Washington, District Of Columbia**

A computer breach was discovered on June 25. Hackers may have obtained encrypted customer credit card numbers, user names and passwords.

Information
Source: Databreaches.net

**July 8, 2011**

**Capital Grille**
**Orlando, Florida**

A man hacked into the websites of multiple businesses; one of them was the Capital Grill website. He was able to obtain email addresses and passwords of registered customers. A total of 250 people from across the businesses had their information stolen. He then tried to use the login information on financial websites. He was able to access the financial accounts of people who used the same email and password combination. A federal judge sentenced him to 10 years in
July 8, 2011

**Excela Health**  
**Jeannette, Pennsylvania**  
MED PORT Unknown

A computer was stolen from the radiology department of the Jeannette campus of Excela. It contained patient names, dates of birth and types of exam performed.

July 7, 2011

**Clark College**  
**Vancouver, Washington**  
EDU HACK 250 (9 SSNs exposed)

An unauthorized access resulted in the exposure of faculty, student and staff information. Student names and identification numbers were exposed. The types of faculty and staff information that may have been exposed were not reported.

July 7, 2011

**The Tech**  
**San Jose, California**  
BSO HACK 800 (No SSNs or financial information exposed)

A hacker broke into three older files on the Museum's computer system. Member names, email addresses, home addresses and phone numbers were posted on Twitter for a period of time. People who signed up for membership events in 2006 and nominees for the Museum's tech awards in 2009 were among those affected.

July 7, 2011

**Morgan Stanley Smith Barney, New York State Department of Taxation and Finance**  
**Albany, New York**  
BSF PORT 34,000

Two CD-ROMs were lost after being mailed from Morgan Stanley to the New York State Department of Taxation and Finance. It is not clear if the CDs were never shipped, fell out of the packaging during shipping, or were lost after being received by the New York State Department of Taxation and Finance. The affected Morgan Stanley clients had their names, addresses, account and tax identification numbers, and income earned on Morgan Stanley investments in 2010 exposed. Some clients also had their Social Security numbers exposed.

July 7, 2011

**Troy Regional Medical Center (TRMC), Southern Records Management Inc.**  
**Troy, Alabama**  
MED INSD 880

Patients may call the IRS at (800) 908-4490 to determine if fraudulent income tax returns have been filed in their names. TRMC discovered that someone had removed paper records that contained the information of approximately 880 patients. The unauthorized access and removal happened in early 2011 and was reported to TRMC by law enforcement on May 20, 2011. Affected patients had their names, Social Security numbers, addresses, dates of birth and medical record numbers exposed. It appears that some of the personal information was used to file fraudulent income tax returns with the IRS.

**UPDATE (06/13/2012):** A woman was arrested on felony charges for allegedly conspiring with others to steal the information of 880 patients while she worked with Southern Records Management at TRMC. The 22-count felony indictment includes allegations of fraud against the U.S. government as part of a tax fraud scheme.

**UPDATE (10/26/2012):** A former Southern Records Management employee working for Troy between June 13, 2010 and March 25, 2011 pled guilty to one count of conspiring to defraud the government regarding claims, one count of fraud in connection with identification documents, a count of fraud in connection with computers, and a count of aggravated identity theft.

**UPDATE (02/07/2013):** The dishonest employee was sentenced to 65 months in prison.

**UPDATE (05/24/2013):** A second co-conspirator pleaded guilty to the theft of government money, fraudulent use of debit cards, and aggravated identity theft. She received 10 years in prison. A total sum of $1,198,063 was fraudulently obtained through fake tax refunds.

**UPDATE (06/13/2013):** Another conspirator was convicted of ID theft and tax fraud after pleading guilty to theft of government money, fraudulent use of debit cards, and aggravated identity theft. The court ordered a 10-year prison sentence for the conspirator.
July 7, 2011  Hurley Medical Center  
Flint, Michigan  

A laptop was discovered missing in May. It was held in a locked room in Hurley, but it was not encrypted or password protected. The laptop contained the names, heights, weights, dates of birth, medical record numbers and lung function test results of 1,938 patients who visited Hurley between 2007 and May of 2011. A total of 10 out of 150 of Hurley's laptops were not encrypted at the time of the discovery.

July 5, 2011  Sutter Gould Medical Foundation (SGMF)  
Stockton, California  

Patients with questions may call 1-877-398-1294 or email SGMFPublicRelations@sutterhealth.org.

Around 1,200 patient records were misplaced on May 27 and were buried in a landfill. The box of records contained patient names, Social Security numbers, addresses, diagnostic test results, provider notes and correspondence, disability forms and insurance information. An unnamed SGMF vendor is responsible for disposing the box.

July 3, 2011  Navos Mental Health Solutions  
Seattle, Washington  

Navos also has an outpatient service in Burien, Washington.

Paper records with sensitive information were misplaced, stolen, or improperly accessed sometime around March 15, 2011.

July 3, 2011  Tuba City Regional Health Care Corporation  
Tuba City, Arizona  

Patients who believe their information was exposed may contact Tuba City Regional at 1-928-283-2452.

Patient dietician treatment cards were discovered missing. The cards contained patient names, dates of birth, phone numbers, medical record numbers, treatment plans, progress notes, medications, diagnoses, procedures, heights, weights, visit dates, and other diagnostic findings. Tuba City Regional suspects that the cards were misplaced during a relocation and inadvertently destroyed in the facility's trash compactor. The approximate date of the disappearance was not reported; but the discovery was made on or around April 1, 2011.

July 3, 2011  Cahaba Government Benefit Administrators LLC  
Birmingham, Alabama  

On April 11, 2011, someone discovered that sensitive paper records had been disclosed to outside parties or accessed without authorization. Centers for Medicare and Medicaid Services (CMS) uses Cahaba for administration of Medicare fee-for-service programs.
A laptop containing unencrypted patient information was stolen during the weekend of December 4, 2010. It contained the names, Social Security numbers, dates of birth, addresses, phone numbers, email addresses, medical records, diagnoses, lab results, insurance information and employment information. The Siteman Cancer Center is a joint venture between Washington University and Barnes-Jewish Hospital. A group of patients is suing all three groups for notifying patients eight weeks after the theft. At least one patient experienced identity theft as a result of the breach.

**Information**

**Source:** PHIPrivacy.net

**July 1, 2011**

**Colorado Department of Health Care Policy and Financing (HCPF)**

**Denver, Colorado**

A disk with the information of medical-aid applicants was lost on its way between HCPF and another agency. It contained applicant names, state identification numbers, and addresses. The disk was discovered missing on May 6.

**Information**

**Source:** PHIPrivacy.net

**July 1, 2011**

**Concord Hospital**

**Concord, New Hampshire**

An audit of Concord’s system revealed that an employee accessed the records of 40 patients without proper authorization. It appears that the employee was checking the files of friends and family. Concord discovered the breach on May 11.

**Information**

**Source:** PHIPrivacy.net

**June 30, 2011**

**Blue Cross and Blue Shield of Florida (BCBSF)**

**Jacksonville, Florida**

An April 2011 mailing error caused 3,500 member healthcare statements to be mailed to incorrect addresses. The statements were mailed to the former addresses of members and contained names, insurance numbers, diagnoses codes and descriptions, procedure codes and descriptions, prescription names and provider names.

**Information**

**Source:** PHIPrivacy.net

**June 26, 2011**

**Public Broadcasting Service (PBS)**

**Arlington, Virginia**

Hackers managed to obtain a number of administrative usernames and passwords for the PBS website. PBS became aware of the intrusion when a phony news story was placed on the website in late May. The login information for over 200 database users was later posted on the internet.

Hackers then began releasing additional information on the PBS website and member database. The names, addresses, email addresses of subscribers. The hackers claim that they may release phone numbers and passwords of PBS members as well. Wyoming PBS was also breached.

**Information**

**Source:** Databreaches.net

**June 25, 2011**

**Nashville Zoo**

**Nashville, Tennessee**

People who made purchases on the Nashville Zoo website within the past two years are being warned about a website security breach. Investigators discovered that the website was the source of several credit card fraud incidents; the Nashville Zoo is now warning patrons to check their credit card statements. It is unclear when the breach occurred.

**Information**

**Source:** Databreaches.net

---

410
Medicare Part D beneficiaries enrolled in Prescription Drug Plans may have had their information exposed. A formatting mistake made member names, ID numbers, drug names and dates of birth viewable through the envelope window of letters sent.

**UPDATE** (7/27/2011): Current and former Molina Medicare, Healthy Advantage HMO SNP, and ChoicePartners Medicare HMO members were also affected.

**UPDATE** (10/28/2011): An additional 1,378 Windsor Health Plan enrollees were affected as well.

**Information Source:** [PHIPrivacy.net](http://www.PHIPrivacy.net)

---

**Harrisburg Project, West Aurora School District, Kaneland School District**

Palatine, Illinois

Two laptops were stolen from a car on or around June 7. The laptops were from an Illinois State Board of Education (ISBE) subcontractor called Harrisburg Project. The ISBE uses the Harrisburg Project as a subcontractor for special education reimbursement purposes. The laptops contained the personal information of over 10,000 students and staff from northern Illinois. Employees were using the laptops for training in data entry.

**UPDATE** (6/29/2011): It appears that both student and staff Social Security numbers were on the laptops. Additionally, student names, dates of birth, residential school district and other educational information were on the laptops. Staff names, demographics, teacher certification numbers and work assignments were on the laptops.

**Information Source:** [Databreaches.net](http://www.Databreaches.net)

---

**California Department of Public Health (CDPH)**

Sacramento, California

The workers’ compensation information of 9,000 current and former state employees was copied onto a private hard drive without authorization. The hard drive was removed from the state offices by an employee, but was recovered. The CDPH security system detected unusual activity on April 5 and the employee responsible was discovered. The employee was placed on administrative leave until the completion of the investigation. Most current CDPH and California Department of Health Care Services (DHCS) employees were affected. An additional 3,000 employees of the former Department of Health Services (DHS) were also affected. Names, Social Security numbers, addresses, dates of birth, ethnicity, addresses of individuals listed as next of kin of employees and other workers’ compensation information was exposed.

**Information Source:** [Databreaches.net](http://www.Databreaches.net)

---

**Arizona Department of Public Safety (AZDPS)**

Phoenix, Arizona

LulzSec has claimed responsibility for a hack of AZDPS. Hundreds of private intelligence bulletins, training manuals, personal email correspondence, names, phone numbers, addresses and passwords belonging to Arizona law enforcement and spouses were released. LulzSec targeted the AZDPS in order to protest SB1070, an Arizona policy they call racial profiling and anti-immigrant.

**UPDATE** (6/30/2011): A second computer attack affected the personal email addresses and passwords of officers. The initial breach of official AZDPS email accounts allowed a hacking group to access the outside accounts of some officers. Hackers were able to post some of the information from the personal accounts, including email messages and pictures.

**Information Source:** [Databreaches.net](http://www.Databreaches.net)

---

**University of Central Missouri**

Warrensburg, Missouri

Two former students conspired to obtain and sell large databases of faculty and alumni information, change grades and steal funds from the accounts of other students. The two students developed malware that allowed them to capture passwords and gain unauthorized access to the University’s network. The students were able to install the malware in a variety of ways. For example, the students obtained the information of other students by inserting a thumb drive into public PCs and personal laptops. Malware was installed on at least one University administrator’s computer and the login credentials of a residence hall director were stolen.
One of the men pleaded guilty to charges of computer hacking conspiracy and computer intrusion. Charges are pending against the student’s alleged accomplice.

**Information**  
Source: Databreaches.net  
Records from this breach used in our total: 0

---

**June 22, 2011**  
**Conor O’Neills Restaurant**  
**Ann Arbor, Michigan**  
BSR HACK Unknown

Conor O’Neills’ computer system was hacked. Customers may have had their credit and debit card numbers accessed. A number of the fraudulent charges came from Texas between April 22 and June 10 of 2011. There is also a possibility that the hackers originated in Europe. The date of the breach and the number of customers affected were not reported.

---

**June 21, 2011**  
**Foothills Nephrology Associates**  
**Spartanburg, South Carolina**  
MED PORT 1280 (No SSNs or financial information reported)

A company laptop was stolen from physician’s vehicle on the night of April 27. Patient names, dates of birth and clinical information were on the laptop. It did not contain Social Security numbers or financial information.

---

**June 20, 2011**  
**Dropbox**  
**San Francisco, California**  
BSR HACK Unknown

Dropbox customers with concerns about account activity may email atsecurity@dropbox.com. At least one customer reported a glitch that allowed users to log into the accounts of other users without using a valid password. The bug that affected the password authentication mechanism was active from 1:54pm to 5:46pm Pacific time on June 19, 2011.

**UPDATE** (6/30/2011): It appears that an intrusion created the security issue that allowed people to log into user accounts without using a password. Someone logged into multiple customer accounts without authorization on June 19, 2011. Fewer than 100 customers had data downloaded from their Dropbox accounts.

**UPDATE** (7/15/2011): A class-action suit was filed that claims Dropbox Inc. failed to secure users’ private data or to notify the majority of them about the breach. The plaintiff class would consist of all current or former Dropbox users as of June 19, 2011 whose accounts were breached. Dropbox Inc. is accused of violating California’s unfair-competition law, invasion of privacy (including intrusion), public disclosure of private facts, misappropriation of likeness and identity, violation of the state constitutional right to privacy, negligence, and breach of express and implied warranties. The legal citation is *Wong et al. v. Dropbox Inc.*, No. 11-CV-3092-LB, complaint filed (N.D. Cal. June 22, 2011)

---

**June 20, 2011**  
**Associated Credit Union**  
**Norcross, Georgia**  
BSF HACK 100

Associated Credit Union members are encouraged to check their accounts frequently and to call 770-448-8200 if they notice suspicious activity.

About 100 Associated Credit Union members have experienced fraudulent checking account charges. A breach of check and ATM card information may have been caused by a breach of Associated Credit’s processing company. This could mean that customers of other financial institutions connected to the transaction processing company are at risk. The customer information was used to make fake cards and the cards were sold throughout the country. The date the breach occurred is unknown.

---

**June 20, 2011**  
**Lending Company**  
**Phoenix, Arizona**  
BSF UNKN Unknown

The Lending Company’s secure database was breached on May 4. A manager reported seeing a computer transferring customer personal information to an external source. Thousands of customers and employees may have had their names, contact information, Social Security numbers and other sensitive personal information downloaded. Customers were originally told that the system had been hacked, but one or more company insiders may have been the source of the breach.
June 19, 2011

**Sega**

London, London

BSR  HACK  1.29 million (No SSNs or financial information reported)

The location listed is the European headquarters of Sega.

The SEGA Pass website was hit by hackers sometime around June 16. Sega Europe in London operates the website, but customers worldwide may have been affected. No credit card information was exposed, but names, dates of birth, email addresses and encrypted passwords were stolen by the hackers. Sega recommends that customers change login information for other sites if they used the same login information for SEGA Pass. Sega reported that 1,290,755 customers were affected.

Information Source:
Databreaches.net

June 17, 2011

**Platte Valley Medical Center (PVMC), Centura Health**

Brighton, Colorado

MED  PHYS  265

Centura Health's St. Anthony Central, St. Anthony North and Porter Adventist were affected.

PVMC patients with questions may email gfanselau@pvmc.org or call 303-498-3618.

A contract nurse who was employed by PVMC between May of 2010 and January of 2011 misused patient information. At least 76 PVMC patients became victims of identity theft. The nurse was employed at multiple locations. The former employee may have accessed a total of 142 patient records while at PVMC, and 123 while working in the Centura Health system. He faces 90 felony counts related to illegally accessing patient files and identity theft.

Information Source:
PHIPrivacy.net

June 17, 2011

**Teachers Retirement System of Texas**

Austin, Texas

GOV  DISC  Unknown

A breach of the Teachers Retirement System (TRS) of Texas has been discovered. A retired principal learned that the TRS had mailed an envelope to her bank. Due to the window-style of the envelope, her personal information was clearly visible through the TRS envelope. The number of people affected by TRS’s practice is unknown. TRS changed their procedures so that content cannot be seen from the outside of the envelope. TRS also plans to take the sensitive information off of letters in the future.

Information Source:
Databreaches.net

June 17, 2011

**Boulder Community Hospital**

Boulder, Colorado

MED  INSD  74

Patients at St. Anthony’s Hospital, Platte Valley Medical Center, and an assortment of other medical facilities in the Denver metro area and Adams County, Colorado were affected.

A contract nurse is accused of accessing patient information without authorization. He faces a 90-count felony indictment. He allegedly used the Social Security numbers and other private information found in patient files to open credit cards in patients’ names.

The nurse was hired through a staffing agency. He worked at Boulder Community between May 1, 2010 and January 7, 2011. Police later notified Boulder Community on May 11, 2011 that the former employee was suspected of stealing patient demographic information from other hospitals.

UPDATE (9/27/2011): The nurse faces five counts of identity theft and 46 counts of theft of medical records in connection to this incident. The former employee worked at a staffing agency and performed work for numerous Centura Health facilities, the Platte Valley Medical Center, and Boulder Community Hospital.

UPDATE (12/6/2011): The nurse was sentenced to six years probation after being charged with multiple felony counts of identity theft and theft of medical records. It was also revealed that the dishonest employee worked at St. Anthony’s Hospital in Lakewood, Colorado.

Information Source:
PHIPrivacy.net

June 17, 2011

**Area Agency on Aging, Inc.**

Mansfield, Ohio

MED  PORT  78,000 (No SSNs or financial information reported)

Those with questions may call 800-522-5680 ext: 1234

The June 3 theft of a laptop from an employee’s car resulted in the exposure of consumer information. The laptop was
assigned to a PASSPORT case manager. It contained the health information of 43,000 consumers and the personal contact information of 35,000 related clients' personal representatives.

Information
Source: PHIPrivacy.net

June 15, 2011  Jackson National Life Insurance Company
Lansing, Michigan  BSF DISC Unknown

On April 12, 2011 a report containing the personal information of customers was inadvertently mislabeled and emailed to an incorrect broker-dealer. The report contained information about customer transactions during March 2011. Names, policy numbers, policy values, transaction dates and transaction amounts were exposed. An internal review on May 2 uncovered the breach.

Information
Source: Databreaches.net

June 15, 2011  Office of Dr. Morgan Camp and Associates
Mill Valley, California  MED STAT Unknown

An office computer was discovered missing on the morning of June 6. A burglar entered the office and searched through papers and equipment. There was no sign of forced entry. A credit card verification machine and approximately $150 in cash were also taken. Patient information, credit card information and other personal details were stored on the computer. Patients are advised to cancel any cards they had on file with Dr. Camp's office.

Information
Source: PHIPrivacy.net

June 14, 2011  St. Louis University (SLU)
St. Louis, Missouri  EDU PHYS Unknown

Someone noticed a pile of discarded paperwork and informed a local news station after it had not been removed within a week. Documents with the personal information of dozens of former St. Louis University students were exposed near a dumpster in a back alley. Most appeared to date back to the mid 1990's and correspond to library fines for late or lost books. An SLU security team picked up the papers after hearing about the incident.

Information
Source: Databreaches.net

June 13, 2011  Jackson Memorial Hospital, Jackson Health System
Miami, Florida  MED INSD 1,800

An unidentified former employee inappropriately accessed the financial information of hospital patients. The employee was fired and the department they worked in was not revealed.

Information
Source: Databreaches.net

June 13, 2011  Bethesda Softworks
Rockville, Maryland  BSR HACK 200,000 (No financial information or SSNs reported)

The Bethesda website was hacked sometime during the weekend of June 11. User names, email addresses and passwords may have been exposed. Users should change their login information for other sites if they used the same login information for Bethesda. The hacker group LulzSec claimed that it had obtained the personal data of over 200,000 users of the game Bethesda game Brink.

Information
Source: Databreaches.net

June 12, 2011  Southern California Medical-Legal Consultants, Inc. (SCMLC)
Seal Beach, California  BSO DISC 300,000

Those with questions may call 562-493-0851 or email notify@scmlc.com.

A data security firm discovered that SCMLC data was available online. The names and Social Security numbers of around 300,000 people who applied for California workers' compensation benefits may have been accessed by unauthorized parties.

Information
Source: Databreaches.net

June 11, 2011  Penn State Altoona
Altoona, Pennsylvania  EDU HACK 12,000

414
A virus infected a Penn State Altoona computer that contained the names, addresses and Social Security numbers of alumni, faculty and staff members. The virus appeared on the computer sometime during the spring semester and was discovered on March 15. Those who were affected were not notified until June because the full list of affected people and their contact information had to be obtained by investigators. Only alumni with identical Social Security numbers and student IDs were affected.

**Information Source:** Databreaches.net

**June 11, 2011**

**Epic Games**  
Cary, North Carolina

BSR  HACK  Unknown

The Epic Games websites and forums were hacked. Hackers may have obtained the email addresses and encrypted passwords of forum users. There is a possibility that hackers may be able to decrypt the passwords. Epic Games reset all passwords and sent new ones to users. Users should also make different passwords for other accounts if their Epic password is the same as the one used for those accounts. No financial information was exposed by the attack.

**Information Source:** Databreaches.net

**June 10, 2011**

**Ravenel Elementary School**  
Seneca, South Carolina

EDU  PORT  15

A Memorial Day weekend office burglary resulted in the theft of two laptops and a flash drive. The flash drive may have contained student information. This potential exposure includes copies of Medicaid release forms with student names, parent names and Medicaid numbers.

**Information Source:** Databreaches.net

**June 10, 2011**

**Texas Department of Assistive and Rehabilitative Services**  
Austin, Texas

GOV  UNKN  4,900

Current and former employees of the Texas Rehabilitation Commission, the Commission for the Blind and the Commission for the Deaf and Hard of Hearing may have also been affected. Current and former employees may have had their personal information exposed. Notification of the incident was sent as soon as Department of Assistive and Rehabilitative Services (DARS) officials learned of the breach. Though a law enforcement investigation is taking place, no information regarding the date of the breach, the cause of the breach or the type of information exposed has been disclosed.

**Information Source:** Databreaches.net

**June 10, 2011**

**Lafrance Hospitality Corporation**  
Westport, Massachusetts

BSO  HACK  100

People who used their debit or credit cards at White’s of Westport or Bittersweet Farm from February 2011 to present may be affected. Around 100 customers have reported fraudulent charges to their financial accounts. Investigators believe that Lafrance’s credit and debit system was breached electronically in early February 2011. Lafrance Hospitality consists of many businesses. Anyone who has used a debit or credit card at White’s of Westport or Bitter sweet Farm since February could be at risk. Lafrance updated its security after the incident.

**Information Source:** Databreaches.net

**June 9, 2011**

**Burke County Courthouse**  
Morganton, North Carolina

GOV  INSD  Unknown

A night custodian made copies of sensitive documents pertaining to criminal cases. He then traded the documents to an outsider in exchange for drugs. Documents were stolen or copied from the district attorney’s office between January and June of 2011. The outsider, her boyfriend and the custodian were charged. The woman wanted to use the court records as aids to help her decide who not to sell methamphetamine to. The custodian was on an assignment from Patton Cleaning Co. Inc. The county has a monthly contract with the company.

**Information Source:** Databreaches.net

**June 9, 2011**

**Citibank**  
New York, New York

BSF  HACK  360,000

Customers may call 888-640-4982 for more information. Hackers have managed to access the information of approximately 1% of Citibank’s 21 million users. U.S. Customer names, account numbers, and contact information were exposed. Security codes and dates of birth were not exposed.
The breach occurred sometime in May.


UPDATE (6/14/2011): It has been revealed that hackers obtained customer names, account numbers and transaction information by logging into the customer credit card site and guessing the account numbers of other customers. Since the account number appeared in the web address browser bar, simply altering an account number allowed the hackers to access a different account. The hackers also utilized an automatic computer program to guess account numbers quickly. This incident appears to have occurred in early May.

UPDATE (6/14/2011): Connecticut Attorney General George Jepsen asked Citigroup Inc. to provide more information about the data breach. Jepsen feels that more information about the types of account information exposed, the cause of the breach, the steps taken to notify affected individuals and the steps to prevent future breaches is needed. He requested the additional information by June 22.

UPDATE (6/16/2011): The number of affected individuals has been raised from 210,000 to 360,000. Further investigation of and information about the breach revealed that the breach was discovered on May 10. By May 24, Citigroup officials concluded that the data thieves had captured names, account numbers, and email addresses of about 360,000 customer accounts. Social Security numbers, expiration dates, and three-digit security passwords found on the back of credit cards were not exposed.

UPDATE (6/24/2011): At least 3,400 of the customers whose credit card information was stolen have suffered a combined loss of $2,700,000.

UPDATE (09/03/2013): Citibank has agreed to pay $15,000 in civil penalties to Connecticut's Privacy Protection Guaranty and Enforcement Account and $40,000 to the General Fund of Connecticut. Citibank will also hire a third party to conduct an information security audit of the Account Online section of Citibank's website.

---

Information Source: Databreaches.net

June 9, 2011  Murphy USA  Suffolk, Virginia  BSR  UNKN  42

At least 42 people who used their debit or credit cards at the same Murphy USA gas station have reported fraudulent charges to their financial accounts. A local credit union claims that hundreds of people were affected. Reports of fraudulent charges began in late May. An investigation of the card reading devices at the gas station did not reveal any evidence that a skimmer had been used. Thieves are using the financial information of victims to make fraudulent ATM withdrawals in California.

Information Source: Databreaches.net

June 9, 2011  Healthcare Partners  Long Beach, California  MED  STAT  15,727 (16 checks stolen)

Patients with questions may call 877-427-9288.

Nineteen computers were stolen during an office burglary on Monday, April 18. Administrative information such as names, addresses, dates of birth, medical record numbers, and health insurance plan ID numbers were exposed. Sensitive medical information such as treating physician names, diagnoses, treatment plans, progress notes, prescriptions, referrals, and authorizations were also exposed. A safe with 16 patient checks and 60 patient credit card receipts was also stolen.

Information Source: PHIPrivacy.net

June 9, 2011  The VA Caribbean Healthcare System  San Juan, Puerto Rico  MED  PHYS  6,006 (1,691 people received credit monitoring services)

Veteran patients with questions may call 855-735-8888.

Veterans and staff had their personal information left unsecured in an open area in the San Juan VA Medical Center. Some of the information included patient care assignment documents with names and Social Security numbers as counseling letters. It is not clear what type of staff information was exposed. The information was supposed to have been shredded. The incident occurred sometime before March 30 and VA Caribbean placed a notification on their website on May 20.

Information Source: PHIPrivacy.net

June 8, 2011  Denver Players, Denver Sugar  Denver, Colorado  BSO  PHYS  Unknown

Hundreds of documents were stolen from the home of the former owner of the escort services. A computer and a large
container of files were stolen during the Monday, June 6 burglary. The files contained the names and numbers of clientele as well as appointment logs, schedule books and credit card receipts. Some of the clients used fake names and some had high profile status. Denver Players and Denver Sugar had previously been exposed as prostitution operations.

Information
Source: Databreaches.net

June 8, 2011  
University of Mary Washington (UMW)  
Fredericksburg, Virginia  
EDU DISC 7,566

Students with questions may call University officials at 540-654-1265 or 540-654-2246.

A student discovered student data files on a departmental EagleNet site while searching the EagleNet portal for his own information. A total of three students accessed the sensitive files and were interviewed. Student names, Social Security numbers and dates of birth were accessible. The information was accidentally placed there by a faculty or staff member and reported on May 23.

Information
Source: Databreaches.net

June 8, 2011  
LexisNexis, Onyx Collections and Locators Services Inc.  
Boca Raton, Florida  
BSO HACK 74

Onyx Collections and Locators Services Inc. is located in Atlanta, Georgia.

Sensitive information was exposed by a breach at Onyx Collections. Someone connected to Onyx Collections was misusing Onyx Collections' search account to access the personal information of people. LexisNexis discovered the problem after conducting an audit of Onyx Collections. From September 10, 2009 through March 2, 2011, Onyx Collections had access to names, addresses, dates of birth, driver’s license numbers and Social Security numbers of at least 74 people from New Hampshire. The total number of people affected nationwide has not been revealed.

Information
Source: Databreaches.net

June 7, 2011  
Victor Victoria’s Restaurant, Renteria Catering  
Bakersfield, California  
BSR INSD Unknown

A husband and wife who owned the two businesses are accused of conspiracy to commit wire fraud, wire fraud, and credit card fraud. The business owners allegedly made additional, unauthorized charges onto customer credit cards after they charged them for legitimate business transactions. Victor Victoria’s was open from August 2009 to July 2010 and Renteria was open from August 2009 to September 2010.

Information
Source: Databreaches.net

June 7, 2011  
Greenville Hospital System University Medical Center, Allen Bennett Memorial Hospital  
Greer, South Carolina  
MED PHYS Unknown

Patients of Allen Bennett Memorial Hospital who received services between 1990 and 1999 may call 1-888-558-2228 for more information.

Exposed boxes of patient information were reported to Greenville Hospital System on December 31, 2010 by someone wishing to remain anonymous. The boxes were in a storage structure behind the building of an abandoned hospital. The hospital was Allen Bennett Memorial Hospital; it closed in August of 2008. Greenville Hospital System collected the boxes and notified patients in February. The 22 boxes contained information from Allen Bennett Memorial dating from 1990 to 1999. The information in the boxes included patient names, reasons and dates for visits, amount paid, patient insurance information with diagnosis and treatment, and admission reports with patient dates of birth and some Social Security numbers. An investigation revealed that the information in the boxes was probably not used for criminal purposes and that no one was sure how the boxes had gotten there.

Information
Source: PHIPrivacy.net

June 6, 2011  
Sony Pictures, Sony Corporation of America  
New York, New York  
BSO HACK 1,000,000 (No SSNs or financial information reported)

Hackers called LulzSec obtained over one million Sony customer passwords. The hackers located data that included passwords, email addresses, phone numbers, home addresses, and dates of birth. The information was not encrypted and was posted on LulzSec’s website. People wishing to enter online sweepstakes entered their real or fake information. Anyone who used their Sony Pictures sweepstakes password for another account should immediately change their passwords so that they do not match each other.

UPDATE (08/28/2012): A second suspect has been arrested for his alleged role in a computer breach at Sony Pictures Entertainment. He faces one count of conspiracy and once count of unauthorized impairment of a protected computer.
Sony claims that 37,500 of the one million users affected had personal information exposed.

**UPDATE (04/18/2013):** One of the hackers involved in the breach was sentenced to one year in prison. He was also sentenced to 13 months of home detention and 1,000 hours of community service after release.

**UPDATE (08/08/2013):** The hacker who was sentenced on April 18 was also ordered to pay $605,663 in restitution.

Information
Source: Databreaches.net

June 6, 2011
**Ravelry.com**
**Boston, Massachusetts**
BSO  HACK  Unknown

Hackers accessed one of Ravelry’s second servers and obtained names, encrypted passwords, and possibly email addresses. Business transactions occur on the site, but no financial information was exposed during the breach. Since hackers may be able to decrypt the passwords and link them to names and email addresses, Ravelry suggested that users immediately change their Ravelry passwords. Users should also make different passwords for other accounts if their Ravelry password is the same as the one used for those accounts.

Information
Source: Databreaches.net

June 5, 2011
**Casa Grande Justic Court**
**Casa Grande, Arizona**
GOV  INSD  200

A court clerk took court documents home in an attempt to hide the fact that she had not done the work. The employee was fired and could be charged with tampering with public records. No malicious intent is suspected. It is believed that the employee hid years of backlogged records and eventually took them home to continue concealing them.

Information
Source: Databreaches.net

June 4, 2011
**Infragard**
**Atlanta, Georgia**
BSO  HACK  180 (No SSNs or financial information reported)

The Atlanta chapter of Infragard was affected.

The hacking group known as LulzSec published 180 usernames, hashed passwords, plain text passwords, names and email addresses from the organization. Infragard is a non-profit that attempts to serve as an interface between the private sector, individuals and the FBI. LulzSec targeted the organization because of its connection to the FBI.

**UPDATE (6/24/2011):** Infragard Connecticut may have also been breached during June. Lulz Security (LulzSec) claims to have the information for over 1,000 accounts.

Information
Source: Databreaches.net

June 3, 2011
**Trinity Medical Center (Montclair Baptist Medical Center)**
**Birmingham, Alabama**
MED  PHYS  4,500

A former employee woman was caught stealing patient information for the purpose of identity theft. Hundreds of pages of information with patient names, Social Security numbers, dates of birth, and some medical information such as scheduled procedure were found at the employee’s woman’s residential address. The information is from stolen surgery schedules and was taken between March 22 and April 1. The former employee woman was charged with violating the federal Health Insurance Portability and Accountability Act (HIPAA).

**UPDATE (2/01/2012):** Additional details reveal that the woman was most likely not an employee of Trinity Medical Center and stole the logs of patient information while supposedly visiting a patient. The paper documents were stolen in a flamboyant way as the woman reportedly jumped over a counter to steal the logs. The files included information from people who had visited in 2006 when Trinity was known as Montclair Baptist Medical Center. The logs were recovered on April 8 through a USPS investigation.

She pleaded guilty to the theft and was sentenced to 39 months in federal prison on February 1, 2012. She will also serve five years of supervised release after her prison time is served.

Information
Source: PHIPrivacy.net

June 3, 2011
**PMC Medicare Choice**
**San Juan, Puerto Rico**
MED  STAT  22,568 (No SSNs or financial information reported)

The March 8 theft of a computer resulted in the exposure of the protected health information of patients.
The March 8 theft of a computer resulted in the exposure of protected patient information.

A former employee stole more than 500 patient records for the purpose of using them as evidence in a legal dispute with a physician. The theft occurred in September of 2010 and included the medical information of three or four patients, as well as administrative information related to hundreds of other patients.

Those with questions may call 877-793-8262.

UPDATE (6/4/2011): More boxes have been removed from three additional residential and storage units owned by the employee. The employee was fired on June 1 and has been cooperating with investigators. Wake Forest denied that Social Security numbers were found in the former employee’s home. Based on the response of the former employee and other observations, investigators believe that the former employee is a hoarder with no desire to misuse the information. Only 3-4% of the contents of the boxes were sensitive information.

UPDATE (7/14/2011): A total of 136 patients and 221 medical center employees were affected.

Someone noticed that thousands of intact personal documents had been dumped in an unsealed dumpster. He called a local news crew and they came to recover and store the documents. The personal documents included applications, resumes, check books, federal income tax forms, and even patient diagnosis forms. The information covered a period between 2003 and 2007. A new employee of Tax Matters dumped the documents without shredding them.
Lockheed Martin experienced a “significant and tenacious attack.” Lockheed’s security team quickly detected the intrusion and updated security. No customer, program or employee data was compromised, but the attack did cause unspecified damage. A breach at RSA may have led to the Lockheed Martin breach since Lockheed Martin was using RSA’s security product or products.

Information
Source: Databreaches.net
May 27, 2011
San Juan Unified School District
Carmichael, California
EDU DISC 4,000

A human resources employee of San Juan Unified uploaded sensitive employee information onto a flash drive. Somehow the information was uploaded onto a website when the employee used the flash drive to perform volunteer work at her church. An employee who Googled their own name discovered that they could also see their Social Security number and other sensitive information. The information was available for six months. San Juan Unified decided to ban flash drives as a result of the incident.

Information
Source: Databreaches.net
May 27, 2011
LA Boxing
Ahwatukee, Arizona
BSO PHYS Unknown

Someone threw out hundreds of customer documents after the local LA Boxing was taken over by corporate. The documents were found and reported by someone who witnessed another person going through the dumpster. Names, addresses, credit card numbers and account numbers of people who were once gym members were left in a dumpster.

Information
Source: Databreaches.net
May 27, 2011
Valley National Bank
New York, New York
BSF CARD 348

A man pleaded guilty to conspiracy to commit bank fraud and aggravated identity theft. He admitted to installing skimmers and cameras on Valley National ATMs in September of 2008. He then used the account and identification information to make fake ATM cards. The man and his co-conspirators accessed around 348 accounts and defrauded Valley National of $278,144.

Information
Source: Databreaches.net
May 27, 2011
Spartanburg Regional Hospital
Spartanburg, South Carolina
MED PORT 400,000

The March 28 theft of a laptop resulted in the exposure of patient information. The laptop was stolen from an employee’s car on March 28. It contained patient names, Social Security numbers, addresses, dates of birth and medical billing codes. Spartanburg Regional has not revealed the number of affected patients.

UPDATE (7/03/2011): Spartanburg Regional notified HHS that 400,000 patients were affected.

Information
Source: PHIPrivacy.net
May 27, 2011
Loyola University Medical Center
Chicago, Illinois
MED PORT Unknown

A flash drive was stolen from an employee’s car. It contained the names, dates of birth, Social Security numbers, addresses and phone numbers of fewer than 100 patients.

Information
Source: PHIPrivacy.net
May 25, 2011
Bank of America
New York, New York
BSF INSD 300

The location listed is Bank of America’s headquarters.

An employee leaked customer information to members of an identity theft ring. Customer names, Social Security numbers, driver’s license numbers, bank account numbers, PINs, account balances, dates of birth, addresses, and phone numbers were obtained. More than $10 million was lost. Bank of America first learned about the breach in 2010; but waited until 95 suspects had been arrested. The group of thieves used the information to modify bank account information and hide the fraudulent accounts they were creating in the names of victims.

Information
Source: Databreaches.net
May 27, 2011
Bethesda, Maryland
BSO HACK Unknown
Records from this breach used in our total: 0

May 27, 2011
San Juan Unified School District
Carmichael, California
EDU DISC 4,000

A human resources employee of San Juan Unified uploaded sensitive employee information onto a flash drive. Somehow the information was uploaded onto a website when the employee used the flash drive to perform volunteer work at her church. An employee who Googled their own name discovered that they could also see their Social Security number and other sensitive information. The information was available for six months. San Juan Unified decided to ban flash drives as a result of the incident.

Information
Source: Databreaches.net
May 27, 2011
LA Boxing
Ahwatukee, Arizona
BSO PHYS Unknown

Someone threw out hundreds of customer documents after the local LA Boxing was taken over by corporate. The documents were found and reported by someone who witnessed another person going through the dumpster. Names, addresses, credit card numbers and account numbers of people who were once gym members were left in a dumpster.

Information
Source: Databreaches.net
May 27, 2011
Valley National Bank
New York, New York
BSF CARD 348

A man pleaded guilty to conspiracy to commit bank fraud and aggravated identity theft. He admitted to installing skimmers and cameras on Valley National ATMs in September of 2008. He then used the account and identification information to make fake ATM cards. The man and his co-conspirators accessed around 348 accounts and defrauded Valley National of $278,144.

Information
Source: Databreaches.net
May 27, 2011
Spartanburg Regional Hospital
Spartanburg, South Carolina
MED PORT 400,000

The March 28 theft of a laptop resulted in the exposure of patient information. The laptop was stolen from an employee’s car on March 28. It contained patient names, Social Security numbers, addresses, dates of birth and medical billing codes. Spartanburg Regional has not revealed the number of affected patients.

UPDATE (7/03/2011): Spartanburg Regional notified HHS that 400,000 patients were affected.

Information
Source: PHIPrivacy.net
May 27, 2011
Loyola University Medical Center
Chicago, Illinois
MED PORT Unknown

A flash drive was stolen from an employee’s car. It contained the names, dates of birth, Social Security numbers, addresses and phone numbers of fewer than 100 patients.

Information
Source: PHIPrivacy.net
May 27, 2011
Bank of America
New York, New York
BSF INSD 300

The location listed is Bank of America’s headquarters.

An employee leaked customer information to members of an identity theft ring. Customer names, Social Security numbers, driver’s license numbers, bank account numbers, PINs, account balances, dates of birth, addresses, and phone numbers were obtained. More than $10 million was lost. Bank of America first learned about the breach in 2010; but waited until 95 suspects had been arrested. The group of thieves used the information to modify bank account information and hide the fraudulent accounts they were creating in the names of victims.
May 25, 2011  United Healthcare Inc.  Pleasant Grove, Alabama  MED UNKN Unknown

A man was sentenced to six years in prison for his role in an identity theft scheme. The man and an unknown number of accomplices somehow obtained the personal information of people who had Flexible Spending Accounts administered by United Healthcare Inc. The group then created counterfeit prescriptions for controlled substances by using the information of patients covered by a prescription drug plan sponsored by the Federal Employees Health Benefit Plan. The group sold the prescribed drugs to third parties from September 2008 through April 2009. The Federal Employees Health Benefit Plan lost $72,746 on drugs and services obtained by the criminals.

Information
Source:  PHIPrivacy.net
records from this breach used in our total: 0

May 24, 2011  Soy Capital Bank and Trust  Decatur, Illinois  BSF CARD Unknown

Those who spot fraudulent charges or who have questions may call 217-428-7781.

Five Midwest financial institutions have seen fraudulent charges show up on their customers' MasterCard-issued debit cards. Soy Capital Bank and Trust is responding quickly to the breach; it appears to have occurred over the weekend of May 21. Fraudulent charges that emptied the accounts of some customers have been appearing in places ranging from Australia to Texas. Soy Capital is blocking transactions on old MasterCards and giving clients new debit cards. Soy Capital expects minimal losses from the breach and will be able to reinstate customer funds within 10 days. Customers who were affected could end up paying as much as $50.

Information
Source:  Media
records from this breach used in our total: 0

May 21, 2011  Keith & Fisher, DDS, PA  Greensboro, North Carolina  MED UNKN

On February 16, 2011, an IT incident caused patient information to be exposed. It is not known if the breach resulted from a hack or an accidental release of information. The type of patient information exposed was not revealed.

Information
Source:  HHS via PHIPrivacy.net
records from this breach used in our total: 0

May 21, 2011  Methodist Charlton Medical Center  Dallas, Texas  MED PORT 6,000 (No SSNs or financial information reported)

Those with questions may call 1-866-584-8105.

The April 16 theft of a laptop resulted in the exposure of patient information. Multiple items were taken during the office burglary. Patients who were part of Methodist Charlton's palliative care program between June 6, 2006, and September 30, 2010 were affected. Patient names, ages, sexes, race, marital status, admission and discharge information, hospital account number, physician, insurance company, date of death, chief complaint and type of cancer may have been revealed. Patient religion may have also been exposed. It does not appear that any Social Security numbers were attached to hospital account number or insurance company information.

Information
Source:  HHS via PHIPrivacy.net
records from this breach used in our total: 1,500

May 21, 2011  Office of Dr. Edalji and Dr. Komer  Brookline, Massachusetts  MED PORT 563 (No SSNs or financial information reported)

The April 12 theft of a laptop resulted in the exposure of patient PHI.

Information
Source:  HHS via PHIPrivacy.net
records from this breach used in our total: 0

May 21, 2011  TRICARE Management Activity  Aurora, Colorado  MED PHYS 4,500 (No SSNs or financial information reported)
Paper records with sensitive information were stolen on June 25, 2010. The types of information the paper records contained was not revealed. The breach does not appear to have been disclosed until May of 2011.

Information
Source: HHS via PHIPrivacy.net
May 21, 2011 Community Action Partnership of Natrona County
Casper, Wyoming MED UNKN 15,000 (No SSNs or financial information reported)

On February 23, 2011, The Community Action Partnership experienced a breach that involved unauthorized access to the information of 15,000 clients. The type of information and the cause of the breach are currently not available; however a notice that has since been removed appeared on their website on April 7.

Information
Source: HHS via PHIPrivacy.net
May 20, 2011 Excel Academy
Castroville, Texas EDU INSD Unknown

A group of employees left Excel Academy and took student information with them to a rival organization. School district superintendents were solicited by the rival academy, Eagle Wings, and shown student information that Eagle Wings should not have possessed. Student names and Social Security numbers were exposed. Excel reported the incident and police launched an investigation. Excel has student information from 33 districts.

Information
Source: Databreaches.net
May 20, 2011 HarborOne Credit Union
BSF PHYS 800

A courier was attacked on May 9. The attacker managed to steal the courier’s bag and its contents. The transaction records of 800 bank customers were exposed. The information was from May 5 transactions and includes names, addresses, account numbers and any other information on checks processed at the bank. Although a suspect was apprehended, the bag was not found. HarborOne flagged the accounts of customers who may have been affected by the incident.

Information
Source: Databreaches.net
May 20, 2011 LaMar’s Donuts
Kokomo, Indiana BSR HACK 50

Additional businesses in the Omaha area were affected by this breach. The exact cause of the breach and the number of businesses affected are unclear.

Someone may have hacked into LaMar’s credit card processing system and used the information to make fraudulent credit and debit cards. Other businesses in the Omaha area who use a similar credit card processor may be at risk.

Information
Source: Databreaches.net
May 20, 2011 Flanigan’s
Loma Linda, California BSR INSD 85

Four people were sentenced for their roles in an identity theft operation. Between April 30, 2010 and May 29, 2010 an employee of the restaurant was paid $20 per card to use a skimmer to collect customer credit card numbers. The stolen credit card information was used to make fraudulent purchases. The criminals managed to cause between $120,000 and $200,000 in fraudulent charges.

Information
Source: Databreaches.net
May 19, 2011 Comfort Dental Offices
Indianapolis, Indiana MED PHYS Unknown

Someone broke into a storage barn on or around Monday, May 16 and took some of its contents. The thief took a bike and may have taken medical records as well. There were several years worth of medical records from dental patients of Comfort Dental. Unfortunately, the owner had not properly secured the barn and could not determine how many records were taken.
Thousands of patients had their medical records compromised by the theft of a laptop. It was being used by an expert witness in a court case between Delta Dental and The Smile Center. The laptop contained a disc with patient information. Names, Social Security numbers, dates of birth and health information were on the disc. Patients of the St. Paul office of The Smile Center who used Delta Dental between January 1, 2003 and June 30, 2010 were affected by the breach.

The theft happened in early 2011, but patients were not notified until May. Neither organization is claiming responsibility for the breach, but Delta Dental is offering credit monitoring services to affected patients.

UPDATE (5/31/2011): Delta Dental first learned of an incident on February 24. The theft occurred on February 22. The Smile Center has refused to notify patients of the incident.

On May 4, a contractor working for the Interior Department’s National Business Center accidentally sent an unencrypted email. There was a security feature in the system software that was designed to prevent such mistakes, but it failed to stop the email from going through. Any information in the unencrypted email was vulnerable for about 60 seconds. The email contained agency employee Social Security numbers and other payroll information.

Information
Source: Databreaches.net

Patients with questions may call 925-866-2020.

A laptop with a lock to prevent theft was stolen from the ophthalmology office on the night of May 8. It contained eye photos and names of 611 patients. The laptop was not recovered.

Information
Source: Databreaches.net

A computer virus called W32.QAKBOT infected various computer terminals and individual computers at the Department of Unemployment Assistance, the Department of Career Services, and multiple One Stop Career Centers. The virus first infected the computers and network on April 20. Though the virus was detected within a short period of time and stopped, it was later discovered that it had not been completely eradicated. Names, Social Security numbers, email addresses, residential or business addresses, Employer Identification Numbers (EIN) and employer bank information may have been exposed. Twelve hundred employers who manually filed with the EOLWD may be affected. If a staff member keyed in sensitive claimant information at a work station infected with the virus then that claimant’s information may have been exposed.

UPDATE (5/18/2011): Approximately 210,000 people were affected by the breach.

Information
Source: Databreaches.net

A woman who worked at Regions is accused of creating 184 fraudulent bank accounts by using the names, dates of birth and Social Security numbers of 149 customers. The woman then filed fraudulent tax returns totaling more than a million dollars and deposited the money into accounts. Her boyfriend withdrew more than $65,000 of this money before the couple was arrested.

Information
Source: Databreaches.net

A hotline has been set up at 1-877-232-6200.

A computer virus called W32.QAKBOT infected various computer terminals and individual computers at the Department of Unemployment Assistance, the Department of Career Services, and multiple One Stop Career Centers. The virus first infected the computers and network on April 20. Though the virus was detected within a short period of time and stopped, it was later discovered that it had not been completely eradicated. Names, Social Security numbers, email addresses, residential or business addresses, Employer Identification Numbers (EIN) and employer bank information may have been exposed. Twelve hundred employers who manually filed with the EOLWD may be affected. If a staff member keyed in sensitive claimant information at a work station infected with the virus then that claimant’s information may have been exposed.

UPDATE (5/18/2011): Approximately 210,000 people were affected by the breach.

Information
Source: Databreaches.net

A woman who worked at Regions is accused of creating 184 fraudulent bank accounts by using the names, dates of birth and Social Security numbers of 149 customers. The woman then filed fraudulent tax returns totaling more than a million dollars and deposited the money into accounts. Her boyfriend withdrew more than $65,000 of this money before the couple was arrested.

Information
Source: Databreaches.net

A hotline has been set up at 1-877-232-6200.

A computer virus called W32.QAKBOT infected various computer terminals and individual computers at the Department of Unemployment Assistance, the Department of Career Services, and multiple One Stop Career Centers. The virus first infected the computers and network on April 20. Though the virus was detected within a short period of time and stopped, it was later discovered that it had not been completely eradicated. Names, Social Security numbers, email addresses, residential or business addresses, Employer Identification Numbers (EIN) and employer bank information may have been exposed. Twelve hundred employers who manually filed with the EOLWD may be affected. If a staff member keyed in sensitive claimant information at a work station infected with the virus then that claimant’s information may have been exposed.

UPDATE (5/18/2011): Approximately 210,000 people were affected by the breach.

Information
Source: Databreaches.net

A woman who worked at Regions is accused of creating 184 fraudulent bank accounts by using the names, dates of birth and Social Security numbers of 149 customers. The woman then filed fraudulent tax returns totaling more than a million dollars and deposited the money into accounts. Her boyfriend withdrew more than $65,000 of this money before the couple was arrested.
An employee is accused of stealing more than $170,000 from several customers. The woman was indicted on 15 counts of theft by a bank employee and four counts of aggravated identity theft. While employed at SunTrust between October 2006 and August 2008 the woman allegedly created a loan for someone without their knowledge and forged the person's signature in order to use $15,175 of their money for herself. At least five other people were victimized in similar ways. Another customer had the money from their CD taken.

Information Source: Databreaches.net
May 14, 2011
Oregon Department of Motor Vehicles
Indianapolis, Indiana
GOV DISC Unknown

The Oregon DMV sold DMV database information to marketing companies prior to the late 1990s. A man gained access to this information and used it to create fake Oregon identification cards and print fake checks. He was charged with 26 counts of aggravated identity theft; this represents one count per victim for each letter of the alphabet. The databases includes 1.6 million names, addresses, dates of birth, genders and ages of people who registered with the DMV. The database of publicly available information is over a decade old. The Oregon DMV says it is not the first time one of their databases has been used illegally.

Information Source: Databreaches.net
May 13, 2011
Anthem Blue Cross
Westlake Village, California
BSF DISC 31,125

Letters soliciting dental and vision coverage were mailed to current Anthem customers. A priority code composed of the customer's Social Security number and two extra digits was printed on the outside of each envelope. One customer noticed the error and contacted the media. Anthem admits that an error occurred, but did not reveal the cause. Anthem is working to prevent this type of breach from happening again and was in the process of notifying customers of the error as of May 12.

UPDATE (10/01/2012): Anthem experienced the marketing mailer error on April 27, 2011. The State of California settled with Anthem in September of 2012. Anthem agreed to pay $150,000 and to make significant improvements to its data security procedures to prevent future errors of a similar type.

Information Source: Databreaches.net
May 12, 2011
Domino’s Pizza, KB Pizza
Fishers, Indiana
BSR PHYS Unknown

A woman looking for coupons in a grocery store dumpster found folders of hundreds of employment applications. Insurance information, copies of Social Security cards, driver's licenses and birth certificates were left in the dumpster along with typical information found in employee records. The information was from employees who worked for KB Pizza and the Domino’s Pizza stores that were at one time owned by KB Pizza. Neither Domino’s nor KB know what caused the information to end up in the dumpster. The Attorney General’s office launched its own investigation into KB Pizza to find out how the files ended up in the dumpster.

Information Source: Databreaches.net
May 12, 2011
Ohio Auditor of State Dave Yost
San Antonio,
GOV PORT Unknown

A state-owned laptop was stolen from the home of a regional auditor for the state Auditor’s Office. Financial audits of public offices in northwest Ohio were on the laptop. The employee was suspended for 15 days because a password that opens the password-protected information on the computer was attached to the computer. This was in violation of the office policy and allowed access to the financial records on the laptop.

Information Source: Databreaches.net
May 11, 2011
Michaels Stores Inc.
New York, New York
BSR CARD 94,000

The location listed is Michaels headquarters. Customers from multiple states were affected.

Those with questions may call 800-MICHAELS (642-4235).

A number of PIN pads in Chicago-area Michaels stores were found to have been tampered with. Michaels checked 7,200 PIN pads in 964 US stores. Fewer than 90 pads were found to have been compromised, but the affected pads were in 20 states. Michaels expects the process of replacing the pads to last about 15 days. The number of affected customers is in the tens of thousands. PIN pads in Canada will also be checked.

The Chicago-area was the hardest hit; 14 stores had compromised PIN pads. Customers who used their debit or credit cards at Michaels are encouraged to monitor their transaction records. Michaels Stores released an official statement.

UPDATE (05/19/2011): A suit seeks class-action status and more than $5 million in damages for people whose credit and
debit accounts were compromised by the breach. The lawsuit claims that Michaels failed to protect customers from "cyber-pickpockets" who stole sensitive banking information from checkout keypads at stores in 20 states. Michaels is accused of knowingly violating federal and state law by failing to take reasonable steps to safeguard customers' personal information. Michaels is also accused of failing to alert customers as soon as the security breach was discovered. There is now a theory that thieves used a combination of "false card readers", wireless cameras or electronic membranes placed over keypads to collect the PINs and card information of Michaels' customers. This allowed them to create fraudulent debit and credit cards.

UPDATE (05/31/2011): A second lawsuit was filed in late May. The new suit also seeks class-action status. It alleges that Michaels failed to safeguard shoppers' credit and debit PINs and other information. The second lawsuit was filed by an Illinois resident who saw over $1,000 in fraudulent charges after making an $18.16 purchase at Michaels.

UPDATE (06/20/2011): An extensive fraud case has hit multiple areas of Oregon. Over 250 people have reported fraudulent charges related to cards that were used at Michaels stores.

UPDATE (06/27/2011): Four suspects were caught making fraudulent debit card transactions on camera. The images have been distributed by investigators hoping that someone in the Beaverton, Oregon area will recognize one or more of the people.

Additionally, Michaels now faces a total of four lawsuits related to the data breach.

UPDATE (07/13/2011): A number of Iowa residents began reporting debit card fraud that could potentially be related to the Michaels breach.

UPDATE (03/21/2012): Two men will be sentenced for their roles in setting up phony debit and credit card pads in the 84 Michaels stores. Each pleaded guilty to one count of conspiracy to commit bank fraud, one count of bank fraud, and one count of aggravated identity theft. A total of 94,000 credit and debit card account numbers were stolen.

UPDATE (07/30/2012): The two men were each sentenced to 36 months in prison for conspiracy to commit bank fraud. An additional 24 months were added for aggravated identity theft. They must also pay $42,000 in restitution and will have five years of supervised release.

Information Source: Databreaches.net

May 10, 2011  Dunes Family Health Care P.C.
Sacramento, California

MED  PORT  16,000 (Unknown number of SSNs)

Current and former patients with questions may call 1-855-569-2669.

The March 11 theft of an external hard drive used for backing up the Clinic’s electronic files may have exposed patient information. The hard drive was stored in a locked, fire-protected building with very limited access. Many of the files contained patient Social Security numbers in addition to names, dates of birth, addresses and other clinical information. There was a delay in notification due to the fact that there were duplicate files and patient contact information had to be updated. The Clinic has begun to encrypt records and raised the physical security of the files since the incident.

Information Source: Databreaches.net

May 10, 2011  Fox.com
Winchester, Virginia

BSO  HACK  363 (No SSNs or financial information exposed)

Hackers accessed the email accounts of 363 Fox.com employees and managed to deface the Linkedin accounts of 16 of them. This same group has attacked multiple Fox related groups such as the Twitter account of Fox15 TV, and the names, phone numbers and email addresses of 73,000 people auditioning for The X-Factor television show on Fox. A text file of the information from The X-Factor participants was placed on a site called Pirate Bay. The hacking group calls themselves Lulzsec. Four Lulzsec hackers searched Fox.com’s servers for vulnerabilities and attacked on April 19. Fox.com noticed the breach a week later. Lulzsec claims that it plans to release more hacked information soon.

Information Source: Media

May 9, 2011  Assurant Employee Benefits
Schenectady, New York

BSF  DISC  Unknown

Policy holders in the Kansas City area were notified that their personal information was accidentally made available to another business client administrator. An employee error causes customer names, addresses, Social Security numbers, dates of birth and types of coverage to be made available to a business client other than the employer of those customers. The incident occurred in March and was corrected within a few minutes. Affected policy holders were notified in early May.

Information Source: Databreaches.net

May 9, 2011  Eastern Illinois University
Las Vegas, Nevada

EDU  PHYS  Unknown
Partially-shredded personnel records were dumped alongside a roadside. Names and Social Security numbers from University employees employed during 2002 were exposed.

A student employee from the Records Management Office had taken two bags of personnel documents for use in a prank. Both bags were eventually found.

**Information**

Source: Databreaches.net

**May 9, 2011**

**Huntington National Bank**

**Bellwood, Illinois**

BSF  INSD  2,000

Several employees of Huntington Bank resigned and took customer information to a competing financial business. The employees had been downloading and printing confidential customer records from Huntington’s secure database for weeks before they departed. The customer records included customer names, addresses, telephone numbers, Social Security numbers, dates of birth, bank account numbers and additional personal information. Former employees also took the files of some customers who had filed active mortgage loan applications. These files would have included customer pay stubs, W-2s, tax returns and other sensitive information.

Huntington is suing the ex-employees for theft of trade secrets.

**Information**

Source: Databreaches.net

**May 9, 2011**

**Reid Hospital**

**Milford, Connecticut**

MED  STAT  20,000  (Unknown number of SSNs)

A computer was stolen from an employee’s home during an early April burglary. It may have contained information from patients who visited the hospital between 1999 and 2008. Patients covered under Medicaid or Medicare may have had their Social Security numbers as well as unspecified information contained in patient reports.

**Information**

Source: PHIprivacy.net

**May 7, 2011**

**Central Oregon Community College (COCC)**

**Montpelier, Vermont**

EDU  HACK  Unknown

Those with questions may call 541-383-7599.

COCC’s website experienced an unauthorized intrusion. Students who applied to the COCC nursing program for the current school year, and for a COCC Foundation scholarship for the following school year may have had their personal information exposed. The potentially exposed information does not include Social Security numbers, credit card numbers, email addresses or COCC ID numbers. It is unclear which information may have been exposed.

**Information**

Source: Databreaches.net

**May 7, 2011**

**Office of Dr. Jeffry Barnes**

**, Illinois**

MED  PHYS  60

A woman found the sensitive information of more than 60 people in a recycling bin. Social Security numbers, prescription information, patient names and medical histories were all easily accessible. The employee responsible for the incident resigned after the mistake and Dr. Barnes agreed to upgrade his shredding practices.

**Information**

Source: PHIprivacy.net

**May 7, 2011**

**Allina Hospitals and Clinics**

**Hartford, Connecticut**

MED  INSD  11 (No SSNs or financial information reported)

The location listed is that of Unity Hospital. Employees of Mercy Hospital in Coon Rapids were also involved.

Twenty-eight employees from Unity Hospital and four from Mercy Hospital were fired for snooping. The employees each accessed patient medical information without authorization. Eleven teens and young adults were taken to the two hospitals on March 17 after overdosing at a party. Allegations that employees were accessing electronic medical records for no legitimate reason first surfaced in April.

**UPDATE** (6/1/2011): It appears that a total of 32 employees, including 15 nurses, were fired in a single day for snooping.

**Information**

Source: PHIprivacy.net

**May 6, 2011**

**Newington Police Department**

**GOV  PORT**  Unknown  426
A marked cruiser was left at an autodealership for service. Its on-board camera was damaged and a laptop used for duty was stolen. The vehicle was left outside after hours because the dealership manager expected a police officer to pick the vehicle up after hours.

Information
Source: Databreaches.net

May 6, 2011
Best Buy
San Francisco, California
BSR HACK Unknown

Though Best Buy was affected by the large Epsilon breach, it had a second, separate breach of customer emails. A former third party vendor experienced a breach that may have exposed customer email addresses. Best Buy is pursuing legal action and had already ended its business relationship with the vendor. It is unclear why the vendor still had Best Buy customer information. It is likely that the unnamed vendor’s breach affected customers of other businesses as well.

Information
Source: Databreaches.net

May 6, 2011
E-Pro Tax Service, Emory Healthcare
Chicago, Illinois
BSF INSD 13,079

An investigation into a few stolen Social Security checks that had been fraudulently deposited into Duluth banks uncovered three separate identity theft rings. At least six conspirators managed to defraud 5,779 people. A former real estate broker created a tax service company in order to access credit reports from a third-party credit reporting agency. Names, dates of birth and Social Security numbers were exposed. The former real estate agent then made about $2.5 million by stealing Social Security checks, filing 393 fraudulent tax returns and passing counterfeit checks. After police linked her to the stolen Social Security checks, they searched her home and found boxes of financial documents which included old mortgage applications, tax forms and HUD documents. Investigators have not charged any other conspirators and do not believe that the woman was the head of the operations.

UPDATE (10/24/2011): More organizations were linked to the breach when investigators searched the dishonest employee’s home. The dishonest employee had a connection with a someone who used to work as a clerk at the hospital. More than 3,000 patient bills containing names, Social Security numbers, dates of birth, and other confidential information were printed by the inside contact. The hospital bills of at least 32 Emory orthopedic clinic patients were stolen and used to file fraudulent tax returns. Nine patients became identity theft victims. Emory notified 7,300 employees of the breach and had fired the dishonest clerk in July.

Information
Source: Databreaches.net

May 6, 2011
Lockerman Family Chiropractic
New Orleans, Louisiana
MED INSD Unknown

Dr. Christopher Lockerman was arrested and charged with eight counts of financial identity fraud and one count of theft by deception. Victims lost over $264,000 due to identity theft. Patients of Lockerman’s clinic had fraudulent J.P. Morgan Chase lines of credit established in their names. The period during which this took place was not revealed.

Information
Source: PHIPrivacy.net

May 5, 2011
Private Legal Practice, Baker Moving and Storage
San Rafael, California
BSO PHYS Unknown

Twenty boxes of documents with sensitive medical and financial information were lost during transportation sometime around Saturday, April 30. The information was mostly from the office of a family lawyer, but other sensitive documents may have been lost on Highway 101 during the incident. The boxes were being transported to a new Baker storage facility. Baker did not inform the lawyer that the documents had been lost and the incident was discovered when the lawyer’s son saw a news report about the incident. The documents appear to be from the 1980’s and early 1990’s. An unknown amount of Social Security numbers were also exposed.

Information
Source: PHIPrivacy.net

May 5, 2011
Park Avenue Obstetrics and Gynecology, PC
Atlanta, 635 (No SSNs or financial information reported)

A portable electronic device was discovered stolen on March 25, 2011. It contained personal and health information.

Information
Source: PHIPrivacy.net

May 5, 2011
Private Legal Practice, Baker Moving and Storage
San Rafael, California
BSO PHYS Unknown

Twenty boxes of documents with sensitive medical and financial information were lost during transportation sometime around Saturday, April 30. The information was mostly from the office of a family lawyer, but other sensitive documents may have been lost on Highway 101 during the incident. The boxes were being transported to a new Baker storage facility. Baker did not inform the lawyer that the documents had been lost and the incident was discovered when the lawyer’s son saw a news report about the incident. The documents appear to be from the 1980’s and early 1990’s. An unknown amount of Social Security numbers were also exposed.

Information
Source: PHIPrivacy.net

May 5, 2011
Park Avenue Obstetrics and Gynecology, PC
Atlanta, 635 (No SSNs or financial information reported)

A portable electronic device was discovered stolen on March 25, 2011. It contained personal and health information.

Information
Source: PHIPrivacy.net
May 5, 2011  Union Security Insurance Company  Las Vegas, Nevada  BSF  UNKN  935 (No SSNs or financial information reported)

On February 18 of 2011, it was discovered that patient health and personal information had accidentally been disclosed.

Information  Source:  HHS via PHIPrivacy.net

May 4, 2011  Merlin Information Services  Kalispell, Montana  BSO  HACK  Unknown

One of Merlin's customers had their login information compromised. Merlin detected inappropriate search activity on March 22, 2011. Someone without authorization was able to access Merlin's databases for 21 hours. Names, addresses, phone numbers and Social Security numbers were exposed. Merlin began sending notification letters on April 11, 2011.

Information  Source:  Databreaches.net

May 4, 2011  Netflix  Redwood City, California  BSR  INSD  Unknown

The call center where the employee worked was not revealed. The location listed is that of Netflix's headquarters.

An employee working in a call center accessed customer credit card information for two months without authorization. Customer names, credit card numbers and other credit card information could have been misused by the employee. The employee's actions were discovered on April 4, the employee was terminated, and a criminal investigation was launched.

Information  Source:  Databreaches.net

May 4, 2011  Rape and Brooks Orthodontics, P.C.  Columbus, Ohio  MED  STAT  20,744 (unknown number of SSNs)

Information from patients who were seen at the dentists' other practices (Luther T. Cale and W. Gregory Rape, Orthodontics, P.C.; St. Clair Orthodontics, LLC and Luther T. Cale, DMD Orthodontics, P.A.) may have also been exposed.

An office burglary was discovered on the morning of February 4. A server with patient personal and health information was among the stolen items. Patients who were seen by the dentists during the past 30 years were affected. The names of patients and patient guardians, home addresses and dates of birth for patients under 18 were on the server. Account holders who provided insurance information may have had their Social Security numbers and dates of birth on the server. Patients who used AllKids with Blue Cross & Blue Shield of Alabama may have had their Social Security number included in the exposed insurance information. An unspecified amount of customer credit card numbers were also stored on the server.

Information  Source:  PHIPrivacy.net

May 4, 2011  Catholic Social Services  EDU  PORT  1,700 (No SSNs or financial information reported)

The February 1 theft of a contractor's laptop may have exposed client personal and health information. The laptop was stolen from the car of an out of state contractor working for the Pregnancy Support and Adoption Services program. It contained personal information that included names, addresses, phone numbers, email addresses, dates of birth, driver's license information, health information, family histories, financial statuses and recommendation for readiness to adopt. Individuals who requested a home study in order to adopt a child between 2008 and 2010 were among those affected.

Information  Source:  HHS via PHIPrivacy.net

May 3, 2011  Office of Dr. Leslie Coleman, Staff Providers  Atlanta, Georgia  MED  INSD  Unknown

A temporary employee from Staff Providers misused patient information. The temporary employee took co-payments from patients while the manager was out of the office. The temporary employee did not have authorization to collect the financial information and made print copies of each customer's credit card during transactions. Patients later called the medical office and complained about fraudulent charges. The temporary employee made at least $1,400 worth of fraudulent charges, but was caught and charged with 11 counts of third-degree identity theft, illegal use of a credit card,
and sixth-degree larceny almost immediately.

**Information**

**Source:** PHIPrivacy.net

**May 3, 2011**

**Speare Memorial Hospital**

Gambrills, Maryland

MED PORT 6,000 (No SSNs or financial information exposed)

Concerned patients may call 866-331-1226 or email patientinfo@spearhospital.com.

The April 3 theft of a laptop from an employee's locked car resulted in the exposure of patient information. The information on the laptop's hard drive should not have been moved from the Hospital's secure server. The employee resigned after the theft of the laptop. Names, addresses, hospital account numbers, medical record numbers, physician names, dates of service, procedure codes, and diagnosis codes were exposed. Speare has committed to checking for the misuse of patient information.

**UPDATE (5/12/2011):** People who were not patients of Speare may have also been affected by this breach. Names, New Hampshire Medical License Numbers, Drug Enforcement Administration (DEA) numbers and National Provider Identifiers may have also been exposed.

**Information**

**Source:** PHIPrivacy.net

**May 2, 2011**

**Woman to Woman Healthcare**

San Francisco, California

MED INSD 26

Two women were arrested for their part in an identity theft ring. At least 26 patients who visited Woman to Woman had their identities stolen by a receptionist. Another worker at the clinic was spotted withdrawing money by using fake IDs. Both women had prior fraud convictions. The two women stole a total of $125,000. It does not appear that the owner of Woman to Woman Healthcare was involved in the identity theft operation.

**Information**

**Source:** PHIPrivacy.net

**April 29, 2011**

**Office of Brian J. Daniels, D.D.S. and Paul R. Daniels D.D.S.**

Phoenix, Arizona

MED PORT 10,000 (No SSNs or financial information reported)

Those with questions may call 602-265-8751.


**Information**

**Source:** HHS via PHIPrivacy.net

**April 29, 2011**

**Omnicare Inc.**

Covington, Kentucky

MED PORT 8,845

The location listed is the headquarters. The breach affected patients in South Carolina.

Those with questions may call a representative at 800-949-6337 ext 10622.

The January 19, 2011 theft of a laptop resulted in the exposure of patient information. The laptop was used by a Consultant Pharmacist who routinely visits nursing homes and rehabilitation facilities in South Carolina to assist physicians in prescribing appropriate medication therapies. Social Security numbers and an undisclosed amount of health information from residents were stored in a database on the laptop.

**Information**

**Source:** PHIPrivacy.net

**April 29, 2011**

**Peace Officers Research Association of California (PORAC)**

Sacramento, California

BSO HACK 2,000

Hackers stole the names, Social Security numbers, dates of birth, phone numbers, email addresses, mailing addresses and credit card information of around 2,000 retired public safety officers who were part of the Peace Officers Research Association of California (PORAC). Hackers breached the PORAC data server in early April. Retired associate members from the present back to 2008 were affected by the breach.

**Information**
Subscribers to the ISP news and review site DSLReports.com have been notified that their email addresses and passwords may have been exposed during a hacker attack on the website during the last part of April. The site was targeted in an SQL injection attack and about eight percent of DSLReports.com subscriber emails and passwords were taken. There are around 9,000 active DSLReports.com accounts and 90,000 inactive accounts.

The location listed is the U.S. headquarters of Sony. Additional information reveals that a Sony data center in San Diego was attacked by cyber criminals.

Sony discovered an external intrusion on PSN and its Qriocity music service around April 19. Sony placed an outage to block users from playing online games or accessing services like Netflix and Hulu Plus on Friday April 22. Sony says the outage will continue until the situation is addressed, which will likely be within the next week. Sony believes an unauthorized person has obtained names, addresses, email addresses, dates of birth, PlayStation Network/Qriocity password and login, and handle/PSN online IDs for multiple users. The attacker may have also stolen users’ purchase history, billing address, and password security questions. User credit card numbers may have also been obtained. Sony has hired a security firm to investigate the incident and strengthen the network infrastructure by re-building their system to provide greater protection of personal information.

An individual filed a class action lawsuit on behalf of all PSN users following seven days of a Sony PlayStation Network outage. The lawsuit alleges that Sony “failed to encrypt data and establish adequate firewalls to handle a server intrusion contingency, failed to provide prompt and adequate warnings of security breaches, and unreasonably delayed in bringing the PSN service back on line.” It also accused Sony of violating the Payment Card Industry (PCI) security standard, which prohibits companies from storing cardholder data.

UPDATE (5/3/2011): A review of Sony’s network breach revealed that it was larger than first thought. Sony turned the SOE system off. Hackers may have taken personal information from an additional 24,600,000 user accounts in Austria, Germany, the Netherlands and Spain. Names, addresses, genders, email addresses, login name and associated password, phone numbers and birth dates of SOE gaming customers, as well as data from about 12,700 credit card accounts and 10,700 bank accounts from an outdated 2007 database could have been accessed. The outdated account information that may have been obtained by hackers includes credit card numbers, debit card numbers, expiration dates, bank account numbers, customer names, account names and customer addresses.

The SOE network hosts games that are played over the Internet on personal computers and is separate from the PlayStation network. Sony has not clearly indicated if credit card numbers were compromised. At least one report indicates that the numbers were encrypted. These breached records will not be added to the total until more is known.

UPDATE (5/6/2011): Sony now indicates that some credit card numbers were compromised. Twelve million credit card numbers were unencrypted and could easily be read.

UPDATE (5/7/2011): Sony discovered that hackers had placed customer information online. Sony removed the information. It included customer names and addresses from a 2001 Sony database.

Service restoration for the PlayStation network was indefinitely delayed. Additionally, the CEO issued an apology letter.

UPDATE (5/17/2011): Hackers began changing user passwords by using PSN account emails and dates of birth within two days of the partial restoration of the PlayStation Network. Sony failed to alter the password reset system to account for hackers having obtained user email addresses and dates of birth. Users who changed their passwords, but not the email associated with their PlayStation Network accounts, were vulnerable to the hacker exploit. Sony shut down the PlayStation Network again and released a short statement about the incident.

UPDATE (5/23/2011): Sony headquarters expects to spend about $171 million on its personal information theft protection program, welcome back programs, customer support, network security enhancements and legal costs associated with the breach.

UPDATE (6/2/2011): Sony fully restored all Playstation Network services in all areas except Japan. The Playstation Store and Qriocity divisions are now functioning properly.


UPDATE (7/21/2011): Zurich American, one of Sony’s insurers, is suing to deny releasing data breach coverage funds to Sony. Sony expects the breach to lower operating profit by $178 million in the current financial year. A total of 55 class action complaints have been filed.

UPDATE (10/11/2011): Sony Online Entertainment became aware of a large number of unauthorized sign-in attempts. The...
Attempts took place between October 7 and 10. About 93,000 PlayStation Network, Sony Entertainment Network, and Sony Online Entertainment services accounts may have been compromised. The unauthorized parties appear to have verified valid sign-in IDs and passwords after a number of failed attempts. Sony temporarily locked those accounts. It is unclear if the email addresses were obtained from a previous breach.

Update (10/19/2012): A federal judge found that Sony users signed a privacy policy informing them that Sony’s security was not perfect. Sony was cleared of negligence, unjust enrichment, bailment, and violations of California consumer protection statutes. The judge ruled that plaintiffs could not claim that Sony violated consumer-protection laws because PSN services were free of cost. This dismissed much of the lawsuit.

Update (12/16/2013): Sony agreed to drop an insurance claim over litigation related to the 2011 breach.

Update (7/30/2014): “Sony recently offered to settle a class action lawsuit over the 2011 breach of its PlayStation Network. According to the terms of the proposed $15 million settlement, the money will be paid out in the form of games. Class members who didn’t take advantage of initial "Welcome Back" package of games and memberships offered in 2011 will receive on of the 14 PlayStation 3 or PlayStation Portable games, as well as three of six PS3 themes or a three-month PlayStation Plus subscription. Qriocity users will get one month of free access.”

Information Source: Databreaches.net

April 22, 2011

U.S. District Court for the Middle District of Alabama
Montgomery, Alabama

GOV DISC

40 (No SSNs or financial information exposed)

U.S. District Court personnel mistakenly believed that sealed records could be made available on a system called PACER. PACER is a web-based records system. Nearly a million defense lawyers, prosecutors, journalists, private investigators, government officials and researchers who use PACER could have accessed about 40 sealed records for as long as nine months. The records were sealed court applications filed by 10 separate federal prosecutors in Alabama. Information in the records included installing hidden surveillance cameras, examining Facebook records, obtaining credit information, procuring telephone records and tracking calls. Specific names, addresses, and phone numbers were exposed. The information was removed from PACER on April 21.

Information Source: Databreaches.net

April 21, 2011

ABM Industries
Atlanta, Georgia

BSO STAT

91

Televisions, mobile telephones and computers were stolen during a March 5, 2011 office burglary. One of the stolen computers contained tax reporting information, including Social Security numbers, for individuals employed by ABM in 2007 and 2008. One suspect was arrested sometime around March 22. The stolen computer was not recovered and ABM began notifying current and former employees of the breach on April 15.

Information Source: Databreaches.net

April 21, 2011

Infogroup
Omaha, Nebraska

BSO HACK Unknown

A small number of computers used to process customer orders were discovered to be infected with a virus. The virus may have compromised a small number of payment transactions which included credit card numbers and related information collected to process transactions. The total number of customers affected and the date the computers were first infected with the virus were not disclosed.

Information Source: Databreaches.net

April 21, 2011

GoGrid LLC.
San Francisco, California

BSO HACK

40

Forty New Hampshire residents were notified of the breach. The total number of individuals affected was not revealed.

An unauthorized third party may have viewed account information sometime between November 2008 and the end of March 2011. The intrusion was discovered during a regular review of system activity by GoGrid’s Security Team. Names, addresses, and payment card data such as cardholder name, card account number and expiration date were involved. The number of unauthorized access incidents between November 2008 and March 2011 was not revealed.

Information Source: Databreaches.net

April 21, 2011

Qdoba Mexican Grill
Clive, Iowa

BSR HACK

12

Over a dozen customers of Qdoba discovered fraudulent charges to their bank accounts after making purchases at the restaurant. The number of affected individuals appears to be 12-18 as of April 21. People discovered charges ranging from a few hundred dollars to one thousand dollars. The cause of the breach may be a computer hacker who somehow accessed the financial clearing house used by Qdoba to process credit and debit card transactions.
Texas Health Arlington Memorial Hospital
Arlington, Texas

Those with questions may call Texas Health at 1800-227-3597 or Sandlot's compliance officer, Vera Blanc, at (817) 810-5237.

Patient information was exposed during the process of converting information systems and processes to the same system as the other hospitals in the Texas Health group. A switch between Texas Health Arlington and SandlotConnect was turned on December 23, 2010. This allowed health information to go to SandlotConnect, a health information exchange, after patients signed an authorization form and the patients' accounts were marked to permit the exchange of information. It was later determined that the SandlotConnect authorization form was not presented to patients at the time of registration since Texas Health Arlington employees were not aware that the switch had been turned on; registration employees were also marking patients' accounts incorrectly.

The switch was turned off and no further health information was sent after the breach was discovered on January 26, 2011. Each of the affected patients had their accounts marked as not participating in the health information exchange and Texas Health Arlington worked with Sandlot to shield the information from being further used or disclosed. Texas Health Arlington registration employees also received additional training on the Sandlot Connect health information exchange process. It appears that a majority of the accounts were accessed by Sandlot employees in order to shield the affected patients' health information. Some SandlotConnect accounts were accessed by authorized health care providers for treatment purposes.

Institute of Electrical and Electronics Engineers (IEEE)
New York, New York

Notifications of a mailing error are being sent to an unknown number of members who signed up for Term Life insurance underwritten by New York Life Insurance. Offers to upgrade insurance plans were sent to the homes of other members.

People's names, member numbers and coverage amounts were exposed.

In mid December of 2010, IEEE learned that its database had been compromised multiple times. On or around February 10 of 2011, a team of investigators discovered that a file containing customer credit card information had been deleted on or around November 17, 2010. An unauthorized person may have obtained access to credit card numbers and the associated names, expiration dates and security numbers located on this file.

Blockbuster Inc.
San Diego, California

A box of employee files and completed job applications was found outside of a Blockbuster store by a concerned citizen. The store was scheduled to close. The documents inside the boxes should have been shredded.

Names, addresses, Social Security numbers and other information associated with employees and job applicants were exposed. Some of the information included surveillance descriptions about and confessions from employees who were fired from the Blockbuster. Blockbuster stated that the incident was against their corporate policies and agreed to shred the information.

Central Ohio Technical College (COTC)
Newark, Ohio

An enclosed file cabinet with student registration cards was left unattended for a short period of time. The cabinet was moved to a temporary storage facility while the Student Records Management Office prepared to move to a new location in the same building. The cabinet should not have been left unattended; it contained Social Security numbers for students who registered for the fall quarter of 2010 at any COTC campus. The incident occurred on March 10 and notifications were sent to students on April 14.
Employees were able to access the pay stub information of other employees at shared workstations. Any UMass Memorial employee who accessed their HRConnect by using one of the 10 malfunctioning kiosks or shared workstations between October 7 and March 11, 2011 may have been affected. The problem was fixed as of March 16. Employees were able to access the names, bank names, bank transit numbers and bank account numbers of previous employees who had used the kiosks to connect to HRConnect. The portion of the 13,500 employees who were affected is unknown.

Information
Source: Databreaches.net
April 18, 2011  Southwest Ambulance
Mesa, Arizona
MED INSD 581

Patient files dating back several years were discovered in the vacated residence of a former employee of Southwest Ambulance. The employee used the records for training purposes. The records included patient names, financial information and medical treatment information. There is no evidence that the information was used in an inappropriate manner.

Information
Source: PHIPrivacy.net
April 15, 2011  Jade House Restaurant
Richmond, Indiana
BSR DISC 15

Anyone who used their credit card at the Jade Restaurant and noticed unauthorized purchases should call (765) 983-7247.

Restaurant employees were fooled by a scam artist calling and pretending to be a representative of the credit card service provider that the restaurant uses. The scammer claimed there was a problem with the system. One or more restaurant employees disclosed sensitive information to the individual. Customers and the restaurant began seeing fraudulent credit card charges.

Information
Source: Databreaches.net
April 15, 2011  Rolling Stone, Radar, Corrupted Justice, Nettica, the Rick Ross Institute of
New Jersey
BSO HACK 100,000 (No SSNs or financial information reported)

Any website that mentioned a September 2006 article called “Strange Bedfellows” from Radar Magazine or a July 2007 article entitled “To Catch a Predator: The New American Witch Hunt for Dangerous Pedophiles” may have been affected.

After a falling out among members of Perverted Justice, a former member attempted to bury two unflattering articles about himself. The articles were about his infidelity and were originally published in Rolling Stone and Radar Magazine. The former member created a virus that spread over the internet and infected computers across the world. Approximately 100,000 computers were affected and a botnet was created. The botnet’s goal was to attack websites that published the two articles so that no one could access them. The former member was sentenced to three years of supervised release and ordered to pay $90,386.34 in restitution.

Information
Source: Databreaches.net
April 14, 2011  Social Security Administration (SSA)
Baltimore, Maryland
GOV DISC 63,587

The Social Security numbers of living people were made available on the Social Security Administration’s Death Master File. This happened twice. Between July of 2006 and January of 2009 26,930 people had their Social Security numbers and other identifying information exposed. A warning from the SSA’s Office of the Inspector General about privacy risks associated with the report was not enough to prevent the second incident. Between May 2007 and April of 2010 36,657 people had their full names, Social Security numbers, dates of birth, and last known ZIP code exposed.

Information
Source: Databreaches.net
April 14, 2011  WordPress
San Francisco, California
BSO HACK 18 million (No SSNs or financial information reported)

Hackers accessed several of WordPress’s servers. All information on the servers could have been accessed. Source code, API keys and social media passwords may have been exposed. Blog comments from WordPress spokespeople reveal the stage of the investigation and that phone numbers and financial information were unlikely to have been exposed.

Information
April 14, 2011  **Private Medical Practice**, Oklahoma

A desktop computer, a portable electronic device, or both were discovered lost on November 24, 2010. It is unclear who the data belonged to and what kind of information was lost.

Information Source: HHS via PHIPrivacy.net

April 14, 2011  **Central Brooklyn Medical Group PC, Preferred Health Partners**, New York, New York

On August 3, 2010 paper records were discovered stolen. It is not clear who the paper records belonged to, where they were stolen from, and what type of information the records contained.

Information Source: HHS via PHIPrivacy.net

April 14, 2011  **Fairview Health Services**, Minneapolis, Minnesota

About 1,200 patient records were stored in a box and marked for shipping to a new office location. The box never arrived and was reported missing on February 21, 2011. Patient billing records with names, dates of birth and medical information may have been exposed. The records are used to process insurance claims. Any patient admitted to Fairview Southdale Hospital in Edina between April of 2010 and February of 2011 may have had their information exposed.

Information Source: PHIPrivacy.net

April 13, 2011  **Private Medical Practice**, San Antonio, Texas

A man was linked to the theft of at least 100 medical records. A surgeon had taken old records home to be shredded; they were stolen from his garage. There were 34 names, 19 driver’s license numbers and many dates of birth. The thief was caught attempting to sell the information for $250 in June of 2010. The man pleaded guilty to possessing numerous medical files.

Information Source: Databreaches.net

April 13, 2011  **Urban Institute, Internal Revenue Service**, Washington, District Of Columbia

About 2,300 operating and defunct, small non-profits were victims of identity fraud. The affected non-profits are all falsely linked to a William Alexander and are mostly religious in orientation.

An Urban Institute online system for the IRS had a loophole that allowed users to register under any false or actual name, enter any non-profit’s name and tax ID number and then change the contact information of that non-profit. The IRS may have identified the affected group of non-profits by publicly targeting them (non-profits with an annual revenue lower than $25,000) and encouraging them to file a yearly tax return. Anyone could have read the published list of non-profits facing revocation of non-profit status and realized that there was an opportunity to register under their name.

Information Source: Databreaches.net

April 13, 2011  **PNC Automated Teller Machines**, Pittsburgh, Pennsylvania

During April and May 2010, two men placed skimmers on PNC ATMs in Harmar and Waterworks Plaza. Both men were arrested in April 2011 and face charges of conspiracy, access device fraud and attempt to commit access device fraud. One man resided in Pompano Beach, Florida and the other in Astoria, New York.

UPDATE (5/11/2011): One of the two men was sentenced to 23 months in prison and three years of supervised release for conspiring to commit bank fraud and access device fraud.
Court records reveal that the two men installed electronic skimming equipment onto multiple PNC ATMs in the Western Pennsylvania area. The illegally installed equipment allowed them to record customer bank account information contained on the magnetic strips of debit and credit cards used at ATMs. Fraudulent debit and credit cards were created with this information and approximately $208,000 was skimmed from at least 211 accounts.

Information
Source: Databreaches.net

April 13, 2011
Albright College
Reading, Pennsylvania

EDU PORT 10,000

Two laptops were stolen from the College’s financial aid office in February. The first laptop was stolen between February 11 and 14. The second was stolen between February 18 and 20. College officials delayed notifying the public of the incident until a risk management firm had assessed the extent of the breach. The laptops contained names, Social Security numbers, dates of birth and addresses. The information may have belonged to faculty, staff, graduates, current and prospective students, spouses of any of these groups and parents of students. The laptop believed to have the most personal information was recovered from a man who was selling the item for drug money.

Information
Source: Databreaches.net

April 12, 2011
Oklahoma State Department of Health
Oklahoma City, Oklahoma

GOV PORT 133,000

People who might have been affected may call 1-888-278-7134 or email contactosdh@health.ok.gov.

An agency laptop and 50 pages of medical information were stolen from an employee's car on April 6. A database with information from the Oklahoma Birth Defects Registry was on the laptop. Data from hospital medical records were recorded on the laptop. The Oklahoma Birth Defects Registry uses the information to track and reduce the prevalence of birth defects. Notifications of the breach state that parent and child names, Social Security numbers, addresses, birth dates, medical records and medical test results may have been exposed. Notifications also warn that any phone calls or mail sent to home addresses that request Social Security numbers should be thoroughly investigated.

Information
Source: PHIPrivacy.net

April 11, 2011
Texas Comptroller’s Office
Austin, Texas

GOV DISC 3.5 million

The data came from the Teacher Retirement Center of Texas, the Texas Workforce Commission and the Employees Retirement System of Texas.

Those who have questions about the breach may call 1-855-474-2065.

The information from three Texas agencies was discovered to be accessible on a public server. Sometime between January and May of 2010, data that was not encrypted was transferred from the Teacher Retirement Center of Texas, the Texas Workforce Commission (TWC) and the Employees Retirement System of Texas. It ended up on a state-controlled public server as early as April 2010 and was not discovered until March 31, 2011. Sensitive information such as names, Social Security numbers, addresses, dates of birth and driver's license numbers could have been exposed. A spokesperson from the Texas Comptroller’s Office claims that the breach occurred because numerous procedures were not followed. Some employees were fired for their roles in the incident.

UPDATE (4/13/2011): Approximately two million of the 3.5 million possibly affected are unemployed insurance claimants who may have had their names, Social Security numbers and mailing addresses exposed. The birth dates and driver’s license numbers of some of these people were also exposed. The information was accidentally disclosed on a Comptroller’s publicly accessible server. TWC provided uninsured claimant records from December 31, 2006 December 31, 2009 to the Comptroller’s office in April of 2010 to assist in identifying individuals who may have unclaimed property. The information, was sent in a protected manner using Secure File Transfer Protocol (SFTP), which encrypts the data during transmission over a state controlled network used by state agencies and universities.

UPDATE (5/6/2011): Two class action lawsuits have been filed on behalf of 3.5 million Texans who had their information exposed by the breach. The second class action lawsuit seeks a $1,000 statutory penalty for each affected individual.

UPDATE (2/13/2012): The cost of the credit monitoring services provided to those affected has passed $600,000. Currently, no taxpayers have linked fraudulent charges to the breach.

Information
Source: Databreaches.net

April 11, 2011
Private Dental Practice
Longmont, Colorado

MED PHYS Unknown

On April 10, a man looking for scrap metal found a stack of patient records from a dental office. The man reported the incident to local news because of the sensitive nature of the information on the documents. The old records were meant to be shredded, but a new office assistant may have accidentally placed them in the trash instead. Names, Social Security numbers and other information were exposed. The dentist immediately responded to the breach after being notified of the mistake. The trash bin where the documents were dumped was brought into the office to prevent further access and remove the documents.
Former employees of GunnAllen Financial have been fined by the U.S. Securities and Exchange Commission (SEC) for failing to adequately protect customer data. The former president and national sales manager broke privacy by transferring the information of GunnAllen Financial clients over to a new business after or during GunnAllen’s November 2010 liquidation. The sales manager was authorized by the president to take a thumb drive with the information of about 16,000 clients with him to his new job. The two former employees were fined $20,000 each and a third former chief compliance officer was fined $15,000 for failing “to ensure that the firm’s policies and procedures were reasonably designed to safeguard confidential customer information.” The fines are based on violations of the SEC’s Safeguard Rule, which requires institutions and financial advisers under SEC jurisdiction to protect customer data and give customers the opportunity to opt out of having their information shared with unaffiliated third parties.

The list of affected people includes patients who visited any of these various locations: The Children’s Hospital of Philadelphia between May 1, 2010 and September 30, 2010, any of the Public Health Management Corporation facilities which include PHMC Care Clinic, PHMC Health Connection, Rising Sun Health Center, Mary Howard Health Center, Community Court, Project Salud and several emergency housing location in Philadelphia between July 16, 2009 and October 29, 2010, Spectrum Health Services, Inc. which operates Haddington Health Center and the Broad Street Health Center between October 31, 2009 and November 30, 2010, Planned Parenthood Southeastern Pennsylvania between July 1, 2009 and October 30, 2010, and Planned Parenthood Association of Bucks County between July 1, 2009 and October 31. Those who may have been affected should call 1-888-414-8020 and enter reference number 3720040811 between 8:00 am-5:00 pm Eastern Time.

A flashdrive was discovered missing from an office on December 28, 2010. It and other items that did not contain patient personal information are presumed to have been stolen by a former employee who left at the end of December. The former employee has an extensive criminal background and was arrested on February 9. Authorities involved in the criminal investigation requested that notification of the breach be delayed due to the investigation. The flash drive contained the personal and medical records of about 70,000 patients. Patient names, Social Security numbers, addresses, phone numbers, dates of birth and other information, including insurance information and medical information was exposed. As a result of the breach, The Family Planning Council will no longer allow unencrypted information to be stored on removable hardware.

Please call (706) 729-5893 for more information.

Two former employees from different private medical practice offices were charged with providing confidential patient information to other members of an identity theft and fraud ring. Both of these people participated in the identity theft and fraud ring from early 2009 until February 2, 2011. A former employee who worked for the Broward County School Board passed along information from a teacher certification database, which included names, Social Security numbers and dates of birth. The information was used to fraudulently add people as authorized users to the victims’ credit card and bank accounts. The bank accounts of victims were depleted and one person discovered fraudulent credit card charges of $128,000. In addition to the three former employees, eight other people and the ringleader were also indicted on March 15, 2011.

UPDATE (9/30/2011): The former Broward School District employee was sentenced to just over five years in federal prison for accessing and selling teacher personal information to identity thieves. At least 42 people in Florida had their information stolen; the fraudulent credit card charges that resulted totalled $408,000. The former employee admitted to selling five to 10 Social Security numbers and dates of birth at a time for $100.
The prisoner also stayed in an Arizona state prison and may have misused prisoner information from that location.

A prisoner filed false individual income tax returns by using the names and Social Security numbers of other prisoners without their permission. On February 4, 2011 the man pleaded guilty to charges related to submitting 117 false tax returns between 2005 and December 2009. He was sentenced to an additional 57 months in prison and three years of supervised release. The prisoner filed for $515,000 in false tax refunds while incarcerated.

Information Source: Databreaches.net

Spyware was discovered on a computer used at the town offices. A payroll program was affected. It is not clear if Social Security numbers and other personal information were accessed. About 150 people may have had their personal information exposed. Current and former town employees were notified about the breach via mail.

Information Source: Databreaches.net

People who logged into Hartford’s server between February 22 and February 28 are being notified of a possible breach. The firm’s Windows servers were hacked and employee, contractor and some customer information may have been exposed by the breach. Social Security numbers, user account logins and passwords, bank account numbers and credit card numbers may have been exposed.

Information Source: Databreaches.net

The US Airlines Pilot Association (USAPA) is upset that US Airways failed to reveal a breach of sensitive and confidential pilot information. A management pilot obtained and sent a sensitive database that contained the personal information of thousands of US Airways pilots. Names, Social Security numbers, and addresses were exposed. The database was given to a third party pilot group. The FBI has not determined the extent of the breach. A USAPA member said that there is a possibility that the sensitive information of pilot family members was also exposed since US Airways collects this information as well. US Airways also collects the credit card numbers of passengers, but there were no reports of this information being exposed by the breach.

USAPA has been working with the FBI since November of 2010 to determine the scope of the breach. It is possible that someone could use pilot passport numbers and residential addresses to pose as a pilot and create a threat to national security. USAPA is accusing US Airways of denying the breach and failing to discipline the employee responsible for the breach. US Airways has informed USAPA that it is relying on the assurances of the parties responsible for the data breach that the confidential information will not be misused.

Information Source: Databreaches.net

People with comments or questions regarding this incident may call (855) 398-6435.

A former Hartford Hospital employee misplaced a computer hard drive on February 15. It contained patient names, Social Security numbers, addresses, dates of birth and medical record numbers. Not all of the patients who were affected had their Social Security numbers exposed.

UPDATE (04/07/2011): Connecticut’s Attorney General and Consumer Protection Commissioner are investigating the breach and data security policies of Hartford Medical Center and Midstate Medical Center. Additional details reveal that the hospital employee misplaced the computer hard drive after taking it home. The Connecticut Attorney General is asking that affected patients receive two years of credit monitoring services, identity theft insurance and reimbursement for placing and lifting security freezes.

UPDATE (07/10/2012): The Connecticut Attorney General has decided to end an investigation of MidState’s practices. The Attorney General claimed to base his decision to close the investigation with no further action on the fact that the Hospital had taken significant actions on behalf of the affected patients.
The February 23, 2011 theft of a laptop may have exposed the names and Social Security numbers of current and former employees. The laptop was stolen from an employee’s car. Those who were affected were sent notification on March 23.

**Information Source:** Databreaches.net

**April 4, 2011**

**Sunnyvale, California**

Epsilon, an email service provider for companies, reported a breach that affected approximately two percent of its 2,500 clients. Only e-mail addresses and names were stolen. Epsilon has not disclosed the names of the companies affected or the total number of names stolen. However, millions of customers have received notices from a growing list of affected companies (http://www.databreaches.net/?p=17374), making this the largest security breach ever.

The Secret Service is investigating this breach. Customers are expected to receive targeted spam that has their name and email address, and appears to come from one of the affected companies. These phishing attempts could result in further loss of consumer personal information. People who receive spam should report it to phishing-report@us.cert.gov.

**UPDATE (05/02/2011):** The original estimate of companies affected was changed from 2% to 3% of Epsilon customers. A total of 75 companies were affected and these companies may end up paying a combined amount of $412 million in damage control. Epsilon itself could pay $225 million. Some estimate the total cost of the Epsilon breach could run as high as $3-$4 billion in forensic audits and monitoring, fines, litigation, and lost business for provider and customers. Conservative estimates place the number of customer email addresses breached at 50-60 million. The total of customer emails exposed could reach 250 million.

**Information Source:** Databreaches.net

---

**April 2, 2011**

**Epsilon**

**Irving, Texas**

Epsilon, an email service provider for companies, reported a breach that affected approximately two percent of its 2,500 clients. Only e-mail addresses and names were stolen. Epsilon has not disclosed the names of the companies affected or the total number of names stolen. However, millions of customers have received notices from a growing list of affected companies (http://www.databreaches.net/?p=17374), making this the largest security breach ever.

The Secret Service is investigating this breach. Customers are expected to receive targeted spam that has their name and email address, and appears to come from one of the affected companies. These phishing attempts could result in further loss of consumer personal information. People who receive spam should report it to phishing-report@us.cert.gov.

**UPDATE (05/02/2011):** The original estimate of companies affected was changed from 2% to 3% of Epsilon customers. A total of 75 companies were affected and these companies may end up paying a combined amount of $412 million in damage control. Epsilon itself could pay $225 million. Some estimate the total cost of the Epsilon breach could run as high as $3-$4 billion in forensic audits and monitoring, fines, litigation, and lost business for provider and customers. Conservative estimates place the number of customer email addresses breached at 50-60 million. The total of customer emails exposed could reach 250 million.

**Information Source:** Databreaches.net

---

**April 1, 2011**

**iTunes (Apple)**

**Cupertino, California**

Following a wave of iTunes fraud in 2010, iTunes users are experiencing another wave of hackers using their accounts to make fraudulent purchases. The hackers purchase music, gift cards, games, ringtones, and apps by accessing customer credit card information and modifying billing addresses. Some of these incidents result in hundreds of dollars of fraudulent purchases. Apple has yet to comment on the situation.

**Information Source:** Databreaches.net

---

**March 31, 2011**

**Adult Industry Medical Healthcare Foundation (AIM Medical Associates P.C.)**

**Sherman Oaks, California**

Over 12,000 current and former adult film performers had their names, home addresses and other personally identifying information posted on the internet. It appears that information from people who tested for HIV and other sexually transmitted diseases at the Adult Industry Medical Healthcare Foundation (AIM) was obtained somehow and misused.

**UPDATE (5/3/2011):** A privacy lawsuit and other troubles caused AIM Healthcare to shut down and file for bankruptcy.

**UPDATE (7/26/2011):** The website that contained the personal and medical information of porn actors, PornWikiLeaks, was forced to shut down after being targeted by hackers.

**Information Source:** PHIPrivacy.net

---

**March 30, 2011**

**NYU Langone Medical Center**

**New York, New York**

Patients with questions may call 1-877-698-2333.

A desktop computer was stolen from an NYU School of Medicine Faculty Group Practice physician’s office on January 27, 2011. It contained names, dates of birth, medical record numbers, home addresses and patient occupations. Information from 670 patients who visited the Langone Medical Center between April 4, 1999 and September 30, 2008 was stored on the computer.

**Information Source:** PHIPrivacy.net

---

**Information Source:** records from this breach used in our total: 0

**514,330 (No SSNs or financial information involved)**
The March 11 theft of a desktop resulted in the exposure of patient names, dates of birth, ages, Eisenhower medical record numbers and the last four digits of patient Social Security numbers. A television was also stolen during the burglary. Patient information from as far back as the 1980’s may have been exposed.

**UPDATE (5/22/2014):** A California appellate court ruled Wednesday that Eisenhower Medical Center did not violate California’s Confidentiality of Medical Information Act.

According to the Fourth District Court of Appeals, “names on a hospital patient index are not “medical information” if they’re not coupled with medical histories, condition or treatment”. If the court had found the medical center in violation, they could have been faced with damages as high as $500 million dollars.

Information Source: PHIprivacy.net

**March 29, 2011**  
**BP Global**  
**New Orleans, Louisiana**  
BSO  PORT  13,000

An employee lost a laptop that contained the personal information of people who were seeking compensation for damages caused by BP’s 2010 oil spill. The laptop was lost on March 1 of 2011 while the employee was traveling for business. It contained a spreadsheet with claimant names, Social Security numbers, addresses and phone numbers.

Information Source: Databreaches.net

**March 28, 2011**  
**The Briar Group LLC**  
**Boston, Massachusetts**  
BSR  HACK  Unknown

Ned Devine’s, Green Briar, City Bar Solas, The Harp, and MJ O’Connor’s experienced customer credit card problems in 2010 and are part of the Briar Group restaurant chain.

Here is a link to the settlement: [http://tinyurl.com/4tmifyx](http://tinyurl.com/4tmifyx)

A series of breaches at Briar Group restaurants dating back to 2009 led the company to pay $110,000 in civil penalties to the Commonwealth of Massachusetts. Briar Group was fined for failing to protect the payment card data of tens of thousands of consumers. In addition to having poor data protection practices like allowing employees to share computer passwords and failing to secure network wireless connections, Briar Group was determined to have not responded appropriately when customer data was compromised. A lawsuit alleges that hackers installed and used malicious software to obtain customer debit and credit card information from the Briar Group’s computers. The malicious software was on the computers from April 2009 to December of 2009 and the company continued to allow the use of credit and debit cards despite being aware that their computer system had been compromised. The Briar Group agreed to comply with Massachusetts data security regulations, comply with the Payment Card Industry Data Security Standards, develop a secure password management system and implement information security measures.

Information Source: Databreaches.net

**March 26, 2011**  
**Memorial Health Services, MemorialCare Health System**  
**Long Beach, California**  
MED  INSD  2,250

Patient information was inappropriately accessed by a former employee. The information included patient names, Social Security numbers, addresses, phone numbers, dates of birth, account numbers and reasons for admission. The former employee appears to have caused breach incidents in 2009 and 2010.

Information Source: HHS via PHIprivacy.net

**March 26, 2011**  
**Maryville Academy**  
**Des Plaines, Illinois**  
GOV  PORT  3,897

Three secondary back-up portable hard drives were taken from a locked room sometime between January 25, 2011 and February 1, 2011. The personal information that may have been exposed includes names, dates of birth, family history, medical and behavioral health services, medications, treatment plans, and for some people, Social Security numbers. Residents and clients who received services between 1992 and January of 2011 may have been affected.

Information Source: PHIprivacy.net
March 26, 2011  Killeen Independent School District (KISD)  Killeen, Texas EDU PHYS 58

A man found student documents near a freeway. A list of student names and their Social Security numbers was found; but it is unclear if teacher evaluations and grade books were also found. KISD said that there were no specific policies for shredding confidential KISD information.

UPDATE (4/13/2011): Notification letters were sent to the homes of 58 students. The Social Security numbers of those students may have been exposed.

Information Source: Databreaches.net
records from this breach used in our total: 58

March 26, 2011  Portland Center for the Performing Arts (PCPA)  Portland, Oregon BSO HACK 864

The PCPA website was hacked sometime between December 20, 2010 and March 15, 2011. Ticket purchases for PCPA events were not involved since the Ticketmaster website is responsible for those purchases. Information from a total of 864 gift card purchases from the PCPA website between January 1, 2006 and March 15, 2011 was compromised. The total number of customers affected is likely to be lower than 864 since some customers purchased more than one gift card.

Information Source: Databreaches.net
records from this breach used in our total: 864

March 24, 2011  TripAdvisor  Newton, Massachusetts BSO HACK Unknown

TripAdvisor community members received notification that an unauthorized third party had obtained a list of user emails. Passwords and financial information were not exposed. Only a portion of users were affected and TripAdvisor is not sure when the breach occurred. TripAdvisor.com is the world’s largest travel related site.

Information Source: Media
records from this breach used in our total: 0

March 22, 2011  Laredo Independent School District  Laredo, Texas EDU PORT 24,903

A disk that contained the Social Security numbers of all students in the Laredo Independent School District was lost or stolen sometime prior to February of 2011.

UPDATE (4/7/2011): Between August 2010 and January 2011, CDs that were mailed to the Texas Education Agency (TEA) were lost. The CDs were unencrypted and contained student Social Security numbers, dates of birth and ethnicity. The CDs were sent to TEA so that identifying information could be removed and the information could be passed along to the University of Texas at Dallas Education Research Center. According to a TEA spokesperson, Laredo ISD’s data set is missing from a set of other district information that was sent. Though the TEA claims that only Laredo student information was exposed, the information of 164,406 students from eight Texas school districts was sent. The information on the unencrypted disks goes back 20 years. This information includes current and former students in the top 10% of their class who graduated between 1992-2010 from Crowley, Harlingen, Round Rock, Killeen, Richardson, Irving, Mansfield, and Grand Prairie school districts.

Information Source: Databreaches.net
records from this breach used in our total: 24,903

March 22, 2011  Lone Star Business Solutions  Wichita, Kansas BSO PHYS Unknown

Thousands of personnel documents were found in a dumpster. W-4 forms, employment applications, and other employee documents were found by the news team FactFinder 12. Social Security numbers, addresses, and phone numbers of people across the country were exposed. It appears that the files were dumped because the office was closing.

UPDATE (11/29/2011): Lone Star Funds (LSF) owned Lone Star Business Solutions. Lone Star Business Solutions managed the LSF restaurants which included Lone Star Steakhouse & Saloon, Texas Land & Cattle Steak House, Del Frisco’s Double Eagle Steak House, and Sullivan’s Steakhouse. The documents exposed in this breach were left behind after LSF decided to move the restaurant management business to Dallas.

The Kansas attorney general’s office investigated the breach and Lone Star Steakhouse (LS Management Inc.) was fine $200,000 for the improper disposal of confidential employee records.

Information Source: Databreaches.net
records from this breach used in our total: 0

March 22, 2011  Bloomfield Hills School District  Bloomfield, Michigan GOV DISC 321

An Excel document with the names and Social Security numbers of 321 staff personnel was sent to two parents. Only limited information of staff with salaries of $100,000 or more should have been disclosed. The two parents are upset that they were named in the notification since they played no part in the District’s mistake.
March 21, 2011  Portland Veterans Affairs Medical Center  Portland, Oregon

Between 50 and 75 patient ID cards were lost in January. Social Security numbers, dates of birth and other personal information were on the cards. The cards had previously been mailed to the wrong addresses and were being stored in the hospital’s enrollment office.

March 21, 2011  Tesoro High School  Las Flores, California

A 21-year old was sentenced to jail after it was discovered that he had broken into his high school’s computer system in 2008. He stole tests and changed his grades. He was ordered to pay $15,000, serve 30 days in jail and serve 500 hours of community service.

UPDATE (8/26/2011): The former student successfully paid the fine in August.

March 18, 2011  City of Cleveland, Texas  Cleveland, Texas

Someone found 10 completed job applications in a public recycling dumpster. The applicants had applied for a position as a municipal court judge with the city of Cleveland and had been rejected. The applications included names, Social Security numbers, contact information, driver’s license numbers, reference contact information and other information typically found on a job application.

March 18, 2011  Spoiled Rotten Spa  Aptos, California

Those with questions or who bought an invalid gift certificate for Spoiled Rotten Spa may contact the Santa Cruz Property Crimes Unit at (831) 454-2311.

The Spoiled Rotten Spa owner was arrested and charged with fraudulently using customer credit card information. Additionally, the owner sold gift certificates to her spa after she had been evicted and could no longer honor them.

March 18, 2011  Wheeler and Associates CPA  Boca Raton, Florida

The law firm is based in Boca Rotan, but the incident may have occurred elsewhere.

Computers and hard drives were stolen during an office burglary that occurred on or around January 3, 2011. The computers contained names, Social Security numbers and addresses. All of the stolen hardware was recovered shortly thereafter, but some of it had already been overwritten with new programs was ready to be resold by the thieves.

March 18, 2011  Randstad Professionals  Wakefield, Massachusetts

A file with images of 1099 tax forms was sent as an attachment in an email to an outside contractor for Randstad Professionals. It contained the names and Social Security numbers of an unspecified number of consultants. The mistake was realized in less than forty minutes and the contractor was asked to destroy the information from the email.

March 18, 2011  Instant Tax Service  Anderson, Indiana

A pile of burned tax documents was found outside of Instant Tax Service. Names, Social Security numbers, wages and contact information were still visible on the documents. Employees denied that they were responsible and claimed that
their office possessed a shredder.

**Information**  
**Source:** Databreaches.net

**March 17, 2011  Walnut Township School District**  
**Millersport, Ohio**  

GOV  HACK  80

A hacker accessed the District’s payroll records sometime between March 14 and March 15. Names, Social Security numbers, and other information found on payroll records may have been exposed. The breach affected 2008 school personnel.

**Information**  
**Source:** Databreaches.net

**March 16, 2011  Cancer Care Northwest**  
**Spokane, Washington**

GOV  DISC  3,150 (No SSNs or financial information reported)

A January mistake in mailing led to brochures being mailed to the wrong current and former patients. Everyone who was meant to receive a brochure did; but patients were able to see the name and address of another patient. The brochure and letter provided information on a breast education and support program.

**Information**  
**Source:** PHIPrivacy.net

**March 16, 2011  Jefferson Center for Mental Health**  
**Wheat Ridge, Colorado**

MED  PORT  546 (No SSNs or financial information reported)

Those with questions may call 1(800)-201-5264.

A list with patient information was stolen from an employee’s locked car on December 13, 2010. The employee’s purse and work bag were also stolen.

**Information**  
**Source:** HHS via PHIPrivacy.net

**March 16, 2011  St. Louis University**  
**St. Louis, Missouri**

EDU  HACK  12,800

The University’s network was hacked on December 12, 2010. The breach was discovered on December 13 and a statement was available on the University’s website on January 31, 2011. Eight hundred students and 12,000 current and former employees and contractors were affected. Only people who worked for Saint Louis University at some point had their Social Security numbers exposed. Some students who received counseling through the University’s Student Health Services may have had their names, dates of birth, tests, diagnosis and treatment information exposed.

**Information**  
**Source:** PHIPrivacy.net

**March 15, 2011  Health Net Inc., International Business Machines (IBM)**  
**Rancho Cordova, California**

MED  PORT  1.9 million

Customers with questions may call (855) 434-8081.

Health Net’s statement about the breach can be read [here](#).

Nine disc drives that contained sensitive health information went missing from Health Net’s data center in Rancho Cordova, California. The drives contained the personal information of 1.9 million current and former policyholders, compromising their names, addresses, health information, Social Security numbers and financial information. The 1.9 million victims include 622,000 California residents enrolled in Health Net HMOs, 223,000 Californians enrolled in Health Net PPOs and people enrolled in Medicare and other plans. The drives were discovered missing on January 21, but affected individuals were not notified until March 14.


**UPDATE** (08/09/2011): Health Net’s chief operating officer apologized to customers after it was discovered that the original analysis of the breach was flawed. Around 124,000 Oregon residents who were current members, former
members, or employees were believed to have been affected. Health Net discovered that an additional 6,300 Oregonians had their personal information on the stolen computer drives.

Information
Source: PHIPrivacy.net

March 15, 2011 Nation’s Giant Hamburgers Vacaville, California

Over 200 cases of identity theft were traced to Nation’s Giant Hamburgers in Vacaville, CA. The cause of the breach was said to be a problem with the credit card machines in the store. The time period when customers using credit cards would have been affected was not reported.

Information
Source: Databreaches.net

March 14, 2011 Virginia Polytechnic Institute and State University (Virginia Tech) Blacksburg, Virginia

A virus infected a Virginia Tech computer on February 15 and sent Social Security numbers and some financial information overseas. The virus was discovered on February 23. Certain current and former employees were affected.

Information
Source: Databreaches.net

March 11, 2011 Walgreens Co. Deerfield, Illinois

According to a complaint filed against Walgreens, Walgreens sold confidential information of customers to data mining companies who resold it to pharmaceutical companies. Walgreens is accused of receiving payment for prescription information that only patients had the right to sell. Walgreens sells patient data that includes sex, age group, state, ID number of the providing doctor and the name of the drug that is taken.

Information
Source: PHIPrivacy.net

March 11, 2011 OrthoMontana Billings, Montana

The loss or theft of a laptop may have exposed the information of current and past patients.

UPDATE (3/16/2011): About 37,000 patients had their information on the laptop. The types of patient information exposed were not reported, however the laptop did not contain financial information.

Information
Source: PHIPrivacy.net

March 10, 2011 TD Bank Elmwood Park, New Jersey

This incident appears to be related to the breach reported on March 13, 2010 at another TD Bank in New Jersey.

A dishonest employee was charged with selling the account information of seven to ten customers. The former employee sold account numbers between November of 2010 and February. Approximately $39,000 in fraudulent charges may have been caused because of the former employee’s actions.

Information
Source: Databreaches.net

March 10, 2011 Se San Diego Hotel San Diego, California

Malicious software was uploaded to the Hotel’s computer system sometime around September of 2010. Customer credit card information was obtained and sold to a group of seven people who used the information to make fraudulent charges primarily in Central Florida.

Information
Source: Databreaches.net

March 10, 2011 University of Massachusetts Amherst, University Health Services Amherst, Massachusetts

A workstation at the campus University Health Services (UHS) was infected with malware. The work station contained...
patient names, health insurance company names, medical record numbers, and prescription information from January 2, 2009 to November 17, 2009. There is no evidence that the data was copied from the workstation. The malware was on the computer from June 30, 2010 to October 28, 2010. Patients were notified in March.

Information Source: PHIPrivacy.net
March 9, 2011 CVS Caremark Corp.
Woonsocket, Rhode Island

According to a complaint filed against CVS, CVS used the confidential information of customers to push certain drugs. CVS is accused of receiving payment for promoting certain pharmaceutical drugs to targeted groups of people. CVS may have violated consumer privacy by sending promotions for specific medications to the physicians of customers. The complaint was filed on March 7.

Information Source: PHIPrivacy.net
March 9, 2011 Shell, Chevron
Mountain View, California

Two men were arrested for using skimmers to obtain and use credit cards. Skimmers were found in three Shell and one Chevron gas pumps in Mountain View. The men were charged with conspiracy, altering a computer and acquiring credit card information with the intent to defraud. The breach was first discovered on December 6 of 2010 when a gas attendant found a skimming device on a gas pump.

Information Source: Databreaches.net
March 9, 2011 Penn Mutual Life Insurance
Philadelphia, Pennsylvania

In late January or early February, Penn Mutual sent notification that a dishonest employee is likely to have accessed and disclosed customer information. Names, Social Security numbers, addresses, dates of birth and bank account information may have been exposed. Penn Mutual was unable to determine which customers were affected.

UPDATE (4/21/2011): The employee and 15 others involved in an identity theft ring have been identified. The Penn Mutual employee and insiders from other organizations sold customer information to the ring leader.

Information Source: Databreaches.net
March 9, 2011 Chapman University
Orange, California

A file that should have only been available to certain University system users was available to all users. It contained the names, Social Security numbers, student ID numbers and financial aid information of students who applied for financial aid for the 2009-2010 school year.

Information Source: Databreaches.net
March 9, 2011 Navy Federal Credit Union
Norfolk, Virginia

Two men obtained account information from account holders at NFCU in 2009 and 2010. The men then applied for loans in the names of the account holders. Approximately $460,000 in fraudulent charges were made. Both men pled guilty.

Information Source: Databreaches.net
March 9, 2011 Eastern Michigan University
Ypsilanti, Michigan

Two former student employees may have obtained student information and provided it to outsiders. Names, Social Security numbers and dates of birth may have been exposed.

UPDATE (10/25/2011): A former student was charged with eight counts of felonies related to the breach. The charges include identity theft and using a computer to commit a crime. A warrant was issued for a second student.

Information Source: Databreaches.net
March 8, 2011 Western Michigan University
Kalamazoo, Michigan

Two former student employees may have obtained student information and provided it to outsiders. Names, Social Security numbers and dates of birth may have been exposed.

UPDATE (10/25/2011): A former student was charged with eight counts of felonies related to the breach. The charges include identity theft and using a computer to commit a crime. A warrant was issued for a second student.

Information Source: Databreaches.net
March 8, 2011 Western Michigan University
Kalamazoo, Michigan

Two former student employees may have obtained student information and provided it to outsiders. Names, Social Security numbers and dates of birth may have been exposed.
A backup hard drive that contained student and faculty information was discovered missing on January 25. Hundreds of current and former students and faculty members had their names and Social Security numbers exposed by the breach. Academic records were also on the hard drive.

Information Source: Databreaches.net

March 7, 2011  Blue Cross Blue Shield Florida
Jacksonville, Florida
MED DISC 7,366 (No SSNs or financial information reported)

Members concerned about the breach may call 1-877-526-1013.

A system error caused mail to be sent to the wrong addresses. Current and former addresses were mixed up and mail containing an explanation of benefits was sent to incorrect (former) addresses.

UPDATE (4/15/2011): The mailing error occurred on October 16, 2010 and was discovered in late January of 2011.

Information Source: PHIPrivacy.net

March 6, 2011  Alaska Department of Education and Early Development
Juneau, Alaska
GOV PORT 89,519 (No SSNs or financial information reported)

A hard drive with the information of students was stolen. Most of the affected students reside in Fairbanks. Names, dates of birth, student identification numbers, genders, ethnicity, disability status, grade levels, test scores and enrollment information were exposed. The theft is believed to have occurred in early February.

Information Source: Databreaches.net

March 5, 2011  Rancho Los Amigos National Rehabilitation Center
Downey, California
MED PORT 667 (No SSNs or financial information reported)

Anyone with questions about the breach can call (877) 726-2461.

A stolen laptop contained patient information. Patient names, dates of birth and medical record numbers may have been exposed. The laptop was connected to diagnostic machinery. The laptop was stolen from the Center on or around February 24.

Information Source: PHIPrivacy.net

March 4, 2011  University of South Carolina
Sumter, South Carolina
EDU HACK 31,000

A computer security problem may have exposed the information of faculty, staff, retirees and students on eight University system campuses. Social Security numbers and other private information could end up on the internet.

Information Source: Databreaches.net

March 3, 2011  Cord Blood Registry
San Francisco, California
MED PORT 300,000

Backup tapes were stolen from an employee’s car in San Francisco on December 13, 2010. Names and Social Security, driver’s license and credit card numbers were on the tapes. The tapes were not encrypted. Customers began receiving notification on February 14 of 2011. A computer and other personal property were stolen during the burglary.

Information Source: PHIPrivacy.net

March 3, 2011  Missouri State University
Springfield, Missouri
EDU DISC 6,030

Nine student lists were accidentally placed on an unsecured server in October and November of 2010. The problem was noticed on February 22. The College of Education lists of students between 2005 and 2009 contained names and Social Security numbers.
March 3, 2011  
**Racetrac, Seacoast National Bank**  
Fort Pierce, Florida  
BSR  CARD  Unknown

The Seacoast National Bank issued thousands of new debit and credit cards after some customers became victims of skimming. Some customers noticed fraudulent charges after making purchases at Racetrac gas station.

March 2, 2011  
**Beebe Medical Center**, Florida  
MED  PHYS  113

The theft occurred while the employee was traveling from a vacation somewhere in Florida. People in Lewes, Delaware were affected.

An employee placed a briefcase with sensitive documents in her car. The briefcase was stolen from the employee’s car on January 1. It contained the names and Medicaid numbers of patients seen at the Beebe Medical Center in Lewes, Delaware. Only a small number of people who were seen between 2005 and 2009 were affected. Around 35 of the patients affected by the breach are deceased.

February 28, 2011  
**Delray Beach and Oakland Park Fire Fighters and Police Officers**  
Oakland Park, Florida  
GOV  UNKN  400 (31 confirmed cases)

Fire fighters and police officers in Delray Beach may also be affected.

A Miami man was caught using fraudulently obtained debit cards. The investigation began when 31 Oakland Park firefighters discovered fraudulent tax returns had been filed in their names. The cause of the breach is unknown, but current and former firefighters and police officers of Oakland Park and Delray Beach had the same retirement plan administrator at one point.

February 24, 2011  
**Cambridge Who’s Who Publishing, Inc.**  
Uniondale, New York  
BSO  PORT  400,000

A former employee made accusations that Who’s Who experienced a breach of 400,000 data tapes with customer information. It is not clear what happened, but the tapes were misplaced during the shipping process sometime before October 20, 2010. The information on the tapes included customer names, Social Security numbers, addresses, driver’s license numbers, payroll data, checking account numbers and credit card information may have been exposed.

February 24, 2011  
**Snow Creek**  
Weston, Missouri  
BSO  HACK  Unknown

It appears that a hacker was able to obtain unencrypted customer credit card information around Friday February 18. Online customers of the ski resort were not affected. Information from electronic card transactions that were performed on-site was exposed.

February 24, 2011  
**Private Medical Practice**  
Olathe, Kansas  
GOV  INSD  Unknown

An Attorney General who investigated the controversial Dr. Tiller is facing allegations that patient records were improperly stored. The AG admitted that sensitive patient records from the case had been temporarily stored in a former employee’s home at one point.

February 24, 2011  
**Henry Ford Health Center**  
Detroit, Michigan  
MED  PORT  2,777 (No SSNs or financial information reported)

An employee misplaced a flash drive with sensitive patient information. The flash drive was lost on January 31 and
Investigators began the process of determining what happened and what information was on the flash drive on February 8. Patients tested for urinary tract infections between July and October of 2010 may have had their names, medical record numbers, test information and results exposed.

**February 24, 2011**

**Prudential Patterson Realtors**
**Hazelwood, Missouri**

Real estate records dating back to 2005 were found in a condominium dumpster by a resident. The records included addresses, phone numbers and copies of personal checks. Prudential Patterson Realtors was sold to Prudential Select Properties in December 2010. Prudential Select said that shredding sensitive documents is their policy.

**February 23, 2011**

**Chapman University, Brandman University**
**Los Angeles, California**

A student discovered a document with sensitive information in an unsecured folder. It contained names, Social Security numbers, student ID numbers and financial aid information. Around 11,000 current and former Chapman students, 1,900 applicants and an unspecified number of Brandman students were affected. Only students and people affiliated with the University could have accessed the file, and it appears that the student who reported the incident was the only one who accessed the file.

**February 22, 2011**

**Emory Healthcare**
**Atlanta, Georgia**

Seventy-seven patients had their Social Security numbers stolen and used for fraudulent tax returns. Patient names and possibly addresses, dates of birth, clinic numbers, limited health information and health insurance companies were exposed. Patients who were seen in orthopaedics between May of 2008 and January of 2009 for something other than physical therapy were affected.

**February 22, 2011**

**Jack in the Box**
**Pearland, Texas**

Investigators determined that a Jack in the Box location had been visited by multiple victims of fraudulent credit and debit card charges. Law enforcement visited the store and found a drive-thru employee with a skimmer in his pocket.

**February 22, 2011**

**Integrity Bank Plus, MicroBilt Corp**
**Kennesaw, Georgia**

Someone gained access to Integrity Bank Plus' MicroBilt account and was able to view the information of consumers connected with MicroBilt. The breach occurred between December 23 and December 28. Consumer credit report information may have been exposed.

**February 20, 2011**

**Howard Brown Health Center**
**Chicago, Illinois**

Call (773) 388-8793 for more information.

A donor database may have been breached. It would have revealed phone numbers and email addresses. It appears that one or more disgruntled organization insiders distributed a libelous letter to people who had their information on the donor database. Several of these people reported receiving the letter.
The office theft of a computer may have exposed names and Social Security numbers of current and former employees. Some other items had been taken from the office too. The theft was discovered on November 15.

**Information**
**Source:** Databreaches.net

**February 18, 2011**  
**The Cigarette Box, Colton's General Store**  
**Las Vegas, Nevada**  
BSR  CARD  Unknown

The Cigarette Box in Las Vegas and The Cigarette Box in Laughlin are associated with the suspect.

A suspect was arrested and charged with fraudulent use of a credit card. The suspect is associated with three businesses and investigators are checking to see if customers of those businesses were victims of fraud. Several card skimmers were recovered at the three businesses.

**Information**  
**Source:** Databreaches.net

**February 17, 2011**  
**Winamp**  
**New York, New York**  
BSO  HACK  Unknown

The location listed is AOL's headquarters. AOL owns Winamp.

Hackers were able to access forum information, user accounts and emails. The attack is believed to have been limited to the Winamp forums. All users are advised to change their Winamp passwords and any similar passwords for other accounts.

**Information**  
**Source:** Databreaches.net

**February 17, 2011**  
**American Airlines**  
**San Jose, California**  
BSO  INSD  350

An airline employee used a skimming device to obtain customer credit card information and make fraudulent purchases. The employee participated in the fraudulent activity between December of 2007 and October of 2010. Over 2,800 fraudulent transactions using 350 credit card numbers were made. The former employee worked at American Airlines for 20 years and now faces 48 years of prison time.

**Information**  
**Source:** Databreaches.net

**February 16, 2011**  
**Charleston Area Medical Center (CAMC)**  
**Charleston, West Virginia**  
MED  DISC  3,655

Someone discovered that they could find information about a relative's name, address, patient ID, date of birth, Social Security number and other sensitive information through an online search that brought up WVChamps.com. WVChamps.com is a CAMC website relating to respiratory and pulmonary rehabilitation for seniors. The information was accidentally posted in a report on September 1, 2010 and appears to have been accessed a total of 94 times. The error was discovered on February 8 of 2011. The breach occurred within the CAMC subsidiary CAMC Health Education Research Institute.

**UPDATE** (5/5/2011): Five patients who were affected by the breach filed a lawsuit seeking class action status for all affected patients. The lawsuit alleges four counts against the hospital: breach of the duty of confidentiality, invasion of privacy by intrusion upon the seclusion of the plaintiffs, invasion of privacy by unreasonable publicity into the plaintiff’s private life, and negligence.

**Information**  
**Source:** PHIPrivacy.net

**February 16, 2011**  
**Alabama Department of Motor Vehicles**  
**, Alabama**  
GOV  DISC  Unknown

All Alabama DMV offices could have been affected.

The Alabama DMV used an online tool that allowed people to access personal information of other drivers. There is a record of these individuals since the online search tool required people who used this feature to register their name and credit card information. Users without legal authorization were able to obtain others' personal information association with vehicle registration for approximately three months.

**Information**  
**Source:** Databreaches.net

**February 15, 2011**  
**Baptist Memorial Hospital**  
**Huntingdon, Tennessee**  
MED  UNKN  4,800 (No SSNs or financial information reported)
A number of patients were notified after a breach occurred on November 27, 2010.

Information Source: HHS via PHIprivacy.net

February 15, 2011  Lake Woods Nursing and Rehabilitation Center  Muskegon, Michigan

The December 28 theft of a computer may have exposed the health information and other types of information of certain individuals.

Information Source: HHS via PHIprivacy.net

February 15, 2011  Baylor Health Care Systems, Baylor Heart and Vascular System, Baylor University Medical Center  Dallas, Texas

A portable ultrasound machine was stolen from the Baylor Jack and Jane Hamilton Heart and Vascular Hospital in Dallas. The machine was stolen from a patient’s room sometime between December 2 and December 3. Patients who were seen at the hospital between December 26 of 2006 and the date of the theft may have had their names, dates of birth, blood pressure, height, weight and ultrasound images of their hearts on the machine. It is believed that only a fraction of the 8,000 patients who are at risk actually had their information on the machine at the time of the theft.

Information Source: PHIprivacy.net

February 15, 2011  Day’s Jewelers  Waterville, Maine

The location listed is the headquarters of Day’s Jewelers.

Those with questions can call Day’s at (800) 439-3297.

A number of Maine residents have experienced credit, bank account and credit union fraud after shopping at Day’s Jewelers. An investigation has revealed that a hacking incident caused the breach and the approximate time of the breach.

Information Source: Databreaches.net

February 15, 2011  Affiliated Computer Services (ACS)  Columbus, Ohio

ACS handles the state of Ohio’s automated system for paying and tracking child care providers. An ACS mistake meant that over 8,000 providers were mailed letters with Social Security numbers visible from the outside of the envelope. Some of the providers were childcare centers and only had ID numbers revealed; smaller providers who had their Social Security numbers as IDs face a greater risk.

Information Source: Databreaches.net

February 13, 2011  Bank of America  Charlotte, North Carolina

An unknown number of customers were able to see the information of other customers when attempting to access their accounts online. The problem appeared to involve customers who had the same last name. The mistake exposed information for credit, mortgage and home equity accounts. All access to problem accounts was suspended within hours of the discovery.

Information Source: Databreaches.net

February 12, 2011  Jacobi Medical Center, North Central Bronx Hospital, Tremont Health Center, and Gunhill Health Center  New York, New York

Health and Hospital Corporation is the group that runs the affected hospitals and clinics.
The New York City Health & Hospitals Corporation's North Bronx Healthcare Network experienced a breach. Backup tapes were stolen from an unsecured and unlocked van during transport by GRM Information Management Services. The theft occurred during December of 2010. The information on the tapes was from patients, staff members and associated employees and dated back to 1991. Names, Social Security numbers, addresses, patient health information and other patient and employee information may have been exposed.

Information
Source: PHIPrivacy.net
Records from this breach used in our total: 1,700,000

February 12, 2011
Saint Francis Broken Arrow (Broken Arrow Medical Center)
Broken Arrow, Oklahoma
MED STAT 84,000

A computer that had not been used since May of 2004 was stolen from a secured information systems room. Patient billing information and some employee records were exposed. The information would have included names, Social Security numbers, dates of birth, addresses and patient insurance and diagnostic information.

Information
Source: PHIPrivacy.net
Records from this breach used in our total: 84,000

February 11, 2011
First Transit, FirstGroup America
Cincinnati, Ohio
BSO PORT Unknown

A flash drive with First Transit applicant personal information was lost on a bus on January 21. Applicant names, Social Security numbers, addresses, dates of birth and possibly other employment information such as conviction record and drug test results may have been on the flash drive.

Information
Source: Databreaches.net
Records from this breach used in our total: 0

February 9, 2011
Oregon Department of Corrections
Madras, Oregon
GOV PORT 550 (300 SSNs exposed)

Payroll reports from Warner Creek Correctional Facility in Lakeview, Deer Ridge Correctional Institution in Madras, and Shutter Creek Correctional Institution in North Bend were exposed.

An outsider with a thumb drive that contained confidential payroll information contacted the agency on January 27. The thumb drive contained payroll reports with the information of around 550 staff members. Pay stub data with names, Social Security numbers and other payroll information were exposed. People employed at Warner Creek between July 31, 2005 and September 30, 2007 had their Social Security numbers exposed. People employed by Deer Ridge between August 31, 2006 and September 30, 2007 had their Social Security numbers exposed. People employed at Warner Creek, Shutter Creek and Deer Ridge between October 1, 2007 and the time of the breach had personal information other than Social Security numbers exposed. The drive was damaged before being returned to the department and it is unclear what, if any, additional types of information may have been exposed.

Information
Source: Databreaches.net
Records from this breach used in our total: 300

February 7, 2011
HBGary Federal
Sacramento, California
BSO HACK 60,000 business emails (No SSNs or financial information reported)

HBGary announced that it had information about the Anonymous hackers collective. Anonymous supporters hacked into HBGary's network in order to learn what information had been gathered during the investigation. Over 60,000 business emails were extracted and the company's website was defaced. HBGary's leader also had his Twitter account hacked and his personal information exposed. Anonymous supporters claim the attack was to prevent HBGary from selling trivial information to the FBI. The hackers published a 23-page document online and claimed that it was the information HBGary was going to sell. HBGary's email database was also published. Sensitive information about customers may have been exposed.

Information
Source: Databreaches.net
Records from this breach used in our total: 0

February 7, 2011
Marriott Vacation Club International
Orlando, Florida
BSR PHYS Unknown

An unknown number of customer payment slips were lost during shipping. Timeshare maintenance fee payment slips were processed by a bank and shipped back to Marriott. The box of slips arrived damaged and had some of the slips missing. Timeshare owners' names, credit card numbers and expiration dates, and addresses were exposed.

Information
Source: Databreaches.net
Records from this breach used in our total: 0

February 5, 2011
Human Services Agency of San Francisco
GOV INSD 2,400 450
A former city employee emailed the information of her caseload to her personal computer, two attorneys and two union representatives. The former employee wanted proof that she was fired for low performance because she had been given an unusually high number of cases. Certain MediCal recipients in San Francisco had their names, Social Security numbers and other personal information exposed.

Information
Source: PHIPrivacy.net

February 4, 2011
Twitter, Facebook and PayPal
Rapides Parish, Louisiana

A 17-year old hacker was charged with various computer crimes. He somehow managed to access the Twitter, Facebook, PayPal and email accounts of multiple celebrities and other people. The teen was charged with cyberstalking, computer fraud, computer tampering and extortion.

Information
Source: Databreaches.net

February 3, 2011
University of Washington Hospital
Seattle, Washington

A customer purchased a piece of furniture from the University’s Surplus Store that had the medical records of patients. The information in the records was mostly x-ray and MRI images of spines.

Information
Source: PHIPrivacy.net

February 3, 2011
SettlementOne Credit Corporation, Sackett National Holdings Inc., ACRAnet Inc., Fajilan and Associates Inc. (Statewide Credit Services and Robert Fajilan)

No location is listed since the incidents involve several organizations and their information security systems.

http://www.ftc.gov/opa/2011/02/settlement.shtm

Three companies who resell consumer credit reports have agreed to settle with the FTC over charges that computer hackers could easily access consumer data through their weak information security systems. Hackers accessed more than 1,800 credit reports via security flaws in the computer networks used by the companies’ clients.

UPDATE (8/22/2011): FTS has approved the final orders settling charges against the three credit report resellers. The approval comes after a period of public comment. The companies will be required to strengthen their data security procedures and submit to audits for 20 years.

Information
Source: Databreaches.net

February 2, 2011
University Book Exchange
Greenville, North Carolina

People who used their credit or debit cards to make purchases at the University Book Exchange may have had their financial information taken. A number of victims have contacted the police, but investigators are still not completely sure that the source of the fraudulent activity is a breach at the U.B.E. store. All or nearly all of those affected by the breach were connected to East Carolina University.

UPDATE (2/13/2011): At least 100 East Carolina University students have reported fraudulent charges to their accounts. The breach is believed to have occurred between January 5 and 25.

Information
Source: Databreaches.net

February 2, 2011
Texas Children's Hospital
Houston, Texas

On December 29, the Harris County District Attorney's Office notified Texas Children's Hospital that its Accounts Payable system may have been breached. Vendors and employees who received checks between 1999 and 2011 may have had their names and Social Security numbers accessed by an unauthorized third party. The information seems to have been used to open electricity accounts.

Information
Source: Databreaches.net

January 30, 2011
JP Morgan Chase, Citibank
New York, New York

100

451
A Staten Island resident somehow obtained the personal information of JPMorgan Chase Bank and Citibank customers. The woman then used the names, addresses, dates of birth and bank account numbers of the people to steal more than $300,000 from Chase and $30,000 from Citibank. The woman visited banks in and around Manhattan between November 26, 2007 and April 29, 2010. She used forged driver's licenses to make fraudulent withdrawals.

**Information**
**Source:** Databreaches.net

**January 30, 2011**
**The Minnesota Department of Education**
**Roseville, Minnesota**

The transcripts of 20 online BlueSky Charter School students were accidentally released in November of 2010. The breach was not discovered until the week of January 30 when a new data request for the school was being processed.

**Information**
**Source:** Databreaches.net

**January 29, 2011**
**Bend Ophthamology**
**Bend, Oregon**

Five desktop computers were stolen from the Bend office during a robbery sometime between January 26 and 27. The office is located in the Pilot Butte Medical Clinic. How much information and the kinds of information exposed were not reported.

**Information**
**Source:** PHIPrivacy.net

**January 29, 2011**
**Southern Perioperative Services, P.C.**
**Pelham, Alabama**

The breach may not have occurred at the Pelham office and may have affected other offices in Alabama.

**Information**
**Source:** HHS via PHIPrivacy.net

**January 29, 2011**
**Friendship Center Dental Office**
**Ocala, Florida**

A laptop that contained the protected health information of patients was stolen on or around December 20, 2010.

**Information**
**Source:** HHS via PHIPrivacy.net

**January 29, 2011**
**Franciscan Medical Group**
**Tacoma, Washington**

The breach may have occurred outside of Tacoma and affected patients who were seen at other hospitals and clinics.

**Information**
**Source:** HHS via PHIPrivacy.net

**January 29, 2011**
**Benefits Resources, Inc.**
**Cincinnati, Ohio**

A computer that contained the protected health information of patients was stolen on or around November 18, 2010.

**Information**
**Source:** HHS via PHIPrivacy.net
The location listed is the headquarters of Benefits Resources, Inc. The breach occurred in South Carolina.

A portable electronic device was lost or stolen on or around November 22, 2010. It contained the PHI of patients.

**Information**

**Source:**

HHS via PHIPrivacy.net

**January 29, 2011** Veteran's Affairs Medical Center

**White River Junction, Vermont**

GOV DISC

114 (No full SSNs or financial information reported)

A client device owned by Dartmouth allowed an unknown amount of people to anonymously log on to a computer network. A document that contained Veteran and Dartmouth patient information could be viewed once people had logged on using the client device. The document contained a list of Dartmouth and Veteran patients. Last names, last four digits of Social Security number, clinical diagnosis and comments were exposed. At least one patient had their full name and date of birth exposed. The problem had existed for an unknown amount of time.

**Information**

**Source:**

PHIPrivacy.net

**January 29, 2011** Dermatology Clinic

**Durham, North Carolina**

MED PHYS

55 (No full SSNs or financial information reported)

A log book with patient appointment information was discovered missing. Patients had their names, last four digits of Social Security number, telephone numbers and names of procedures scheduled exposed. Two searches did not lead to the recovery of the log book; there is a possibility that a patient took the book.

**Information**

**Source:**

PHIPrivacy.net

**January 29, 2011** Texas Health Harris Methodist Hospital Azle

**Azle, Texas**

MED PORT Unknown

Those with questions may call (800) 277-3597.

The loss of a back-up computer disc with patient information was confirmed on April 22, 2010. The disc contained laboratory chemistry exam results. Patients who were treated at the Hospital’s lab between July 2008 and February 2010 were affected.

**Information**

**Source:**

PHIPrivacy.net

**January 29, 2011** Ankle and Foot Center of Tampa Bay, Inc.

**Tampa Bay, Florida**

MED HACK

156,000 (No SSNs or financial information reported)

The Center experienced a hacking or IT incident on or around November 10 of 2010. The protected health information of patients was exposed.

**UPDATE** (2/3/2011): Names, Social Security numbers, dates of birth, home addresses, account numbers, and health care services and related diagnostic codes may have also been exposed.

**Information**

**Source:**

HHS via PHIPrivacy.net

**January 29, 2011** Amazon.com

**Seattle, Washington**

BSR DISC Unknown

A security flaw that allows some Amazon customers to log in with variations of their actual passwords was recently discovered. Lowercase and uppercase letters are not distinguished and people could even use passwords with extra characters as long as the incorrect characters came after the 8th character of the password. An example of this problem is that Amazon would accept "PASSWORD", "password" and "passwordpassword" as correct if someone had a password of "Password". The problem appears to affect older Amazon.com passwords that have not been changed recently.
University officials launched an investigation to determine if electronic medical records of 13 Iowa Hawkeyes football players receiving care at the facility were accessed inappropriately. Speculation about the health of the football players and the causes of their illness had been in the media.

**UPDATE (2/3/2011):** It appears that three workers will be fired and two will be suspended because they inappropriately accessed football player information.

**UPDATE (2/7/2011):** One of the fired workers is challenging allegations that she viewed patient information without authorization. She and her representative claim that she did nothing wrong, and that if the accusations were true, viewing computerized medical records for a few seconds should be treated as a minor infraction.

**UPDATE (4/5/2011):** The nurse who challenged her termination has agreed to resign rather than be fired.

---

**Information Source:**

PHIPrivacy.net

---

**January 28, 2011  Five County Credit Union**

**Bath, Maine**

Five County decided to send 3,000 credit and debit cards to customers after discovering a breach that affected a third party. Some customers noticed suspicious transactions on their debit cards. About 2,500 debit cards were reissued and 500 Visa credit cards were reissued. The organization that experienced the breach and the number of customers affected were not reported.

**Information Source:**

Databreaches.net

---

**January 26, 2011  Temple University School of Medicine**

**Philadelphia, Pennsylvania**

A former Chair of the University’s Department of Ophthalmology and Assistant Dean for Medical Affairs faces 144 counts of health care fraud and making false statements in health care matters. The former faculty member and doctor is accused of causing thousands of false claims to be submitted to health care benefits programs between 2002 and 2007. The former faculty member allegedly instructed staff members to bring patient charts from other doctors to his office. Patient charts were improperly stored outside of his office and then fraudulently edited to make it seem as though the former faculty member had seen and evaluated the patients. The prosecution claims that after falsifying the documents, the former faculty member collected fees for services he had never performed. The former faculty member is also accused of falsifying the records of patients he had seen. The false claims may total more than $3,000,000.

**Information Source:**

PHIPrivacy.net

---

**January 26, 2011  North Carolina Department of Health and Human Services**

**Raleigh, North Carolina**

A set of computer disks may have been accidentally discarded during an office renovation. The disks contained data from the Division of Services for the Deaf and Hard of Hearing and would have been taken to a landfill if they were accidentally discarded. Those who applied for services from the Division’s Equipment Distribution Service between January of 2005 and December of 2008 may have had their information exposed.

**Information Source:**

PHIPrivacy.net

---

**January 26, 2011  Warner Pacific College**

**Portland, Oregon**

A laptop was stolen from an employee’s home on January 3. It contained the names, Social Security numbers, dates of birth, telephone numbers and addresses of students.

**Information Source:**

Databreaches.net

---

**January 26, 2011  Universal Technical Institute**

**Phoenix, Arizona**

The names and Social Security numbers of recent applicants were on a stolen laptop. The laptop was stolen from UTI’s Phoenix office on November 18. Some applicants may have had their dates of birth and contact information exposed as well.

**Information Source:**

Databreaches.net

---

**January 26, 2011  Ember Corporation**

**Boston, Massachusetts**

---
Ember received a package that had been sent from Ceridian via Federal Express. The package appeared to have been tampered with. Ceridian processes Ember’s payroll information and the package contained individual W-2 forms for current and former Ember employees. Two corners of the package had opened and the contents were wrinkled, but no documents appeared to be missing or opened. Ember warned its employees that their names, Social Security numbers, addresses and 2010 payroll information may have been exposed.

Information Source: Databreaches.net
January 26, 2011 Hamilton Beach Brands, Inc.
Glen Allen, Virginia

Hacker code was discovered on a server that hosts www.hamiltonbeach.com and www.proctorsilex.com. The server was breached on or around January 5. Customer names, credit card information, addresses, telephone numbers and email addresses were captured. The captured information was sent to hmtbccc@gmail.com and prosilexcv@gmail.com

Information Source: Databreaches.net
January 26, 2011 J. Press
New Haven, Connecticut

An unauthorized party gained access to records of customer online orders placed between January 5 and January 10. Customer names, credit card information, order information and addresses may have been exposed. The website was temporarily shut down after J. Press learned of the breach.

Information Source: Databreaches.net
January 26, 2011 KBR, Inc.
Houston, Texas

People with questions regarding this incident may call 1-877-311-6112 or email response@kbr.com.

A company laptop that contained the personal information of current and former KBR employees and contractors was stolen. Names, Social Security numbers, addresses, dates of birth and employee ID numbers may have been accessed.

Information Source: Databreaches.net
January 25, 2011 Presbyterian Health Care Services
Albuquerque, New Mexico

Between May and June of 2008, a PHS pharmacy employee misused the names and identification information of customers. The former employee had fraudulent prescription reimbursement checks mailed to her friends and relatives, who then gave the proceeds back to the pharmacy employee. The employee allegedly generate 17 fraudulent checks for a total of $27,129.63. The woman was sentenced to two years in prison and four years of supervised release. She will also have to pay restitution to PHS and Medicaid.

Information Source: PHIPrivacy.net
January 25, 2011 Plainfield Board of Education
Plainfield, New Jersey

Someone posted administrative login information and a link to the login page of the Plainfield District’s Genesis Student Information System on a popular online message board. Plainfield did not disclose how the admin user name and password were discovered. An unknown number of people would have had access to student records and maybe even student and parent contact information. The breach was discovered and addressed within 24 hours.

Information Source: Databreaches.net
January 25, 2011 MetLife
Loves Park, Illinois

Metlife representatives can be reached at 888-383-5257.

Thousands of papers with names, addresses, Social Security numbers, birth dates and account balances were thrown in a dumpster. The breach appears to be the result of an insurance office moving from one location to another. A man searching for metal in dumpsters made the discovery. Most of the files belonged to one insurance agent.

UPDATE (3/1/2011): MetLife has been ordered to provide credit fraud protection for everyone affected by the mistake. MetLife must also pay a $75,000 fine to the State of Illinois Director of Insurance. The information had sat in the dumpster for at least four days. The former insurance agent who was responsible for most of the accounts says that he left 17 filing cabinets with MetLife before he departed the company. He estimated that the filing cabinets contained a
thousand accounts.

**Information**
**Source:** Databreaches.net

**January 24, 2011**  
**Grays Harbor Pediatrics**  
**Aberdeen, Washington**  
MED PORT 12,000

People with questions about the incident may call 1-877-810-7248.

A backup tape was stolen from an employee’s car sometime around November 23. The device was used for storing copies of paper records. Patients may have had their names, Social Security numbers, insurance details, driver’s license information, immunization records, medical history forms, previous doctor records and patient medical records scanned and placed on the backup tape.

**Information**
**Source:** PHIPrivacy.net

**January 24, 2011**  
**Wentworth Institute of Technology**  
**Boston, Massachusetts**  
EDU DISC 1,300

On December 22 of 2010, Wentworth became aware of a breach that left sensitive student information online. A file was accidentally placed on Wentworth’s website at some point. Current and former students may have had their names, Social Security numbers, dates of birth and medical information exposed.

**Information**
**Source:** PHIPrivacy.net

**January 24, 2011**  
**University of Missouri, Coventry Health Care**  
**Columbia, Missouri**  
EDU DISC 750 (No SSNs or financial information reported)

A Coventry Health Care computer malfunction caused the names of University of Missouri health insurance program participants to be aligned with incorrect mailing addresses. Names, member numbers and birth dates were on mailed documents like benefits statements, health services letters and new ID cards. The erroneous mail was sent out to employees between January 6 and 10. An employee notified the University on or around January 14.

**Information**
**Source:** PHIPrivacy.net

**January 20, 2011**  
**Chase Bank**  
**San Luis Obispo, California**  
BSF CARD 100

A Chase ATM in Atascadero was also tampered with.

Three people were arrested for tampering with ATMs and making fraudulent charges on customer cards. They allegedly accomplished this by placing small cameras and card readers on at least two ATMs in the San Luis Obispo area. Over 100 people discovered that fraudulent charges had been made on their cards. Investigators first became aware of the situation on January 13.

**Information**
**Source:** Databreaches.net

**January 19, 2011**  
**Abbott Medical Optics, Baylor College of Medicine Department of Ophthalmology**  
**Malpitas, California**  
MED PORT Unknown

More information is available at (713) 798-2667.

Backup tapes with information from Ophthalmology department equipment were stolen from Abbott’s office after being collected from Baylor. The information on the tapes included the eye contour measurement charts, names and physician names of patients who were preparing for Lasik surgery.

**Information**
**Source:** PHIPrivacy.net

**January 19, 2011**  
**Ingenix**  
**Eden Prairie, Minnesota**  
BSO DISC 142

A search of health care providers on the Ingenix website revealed that Social Security numbers were sometimes attached to the names of providers as ID numbers. It appears that some health plans or preferred providers had listed the Social Security numbers as ID numbers. People searching for providers covered by their plans would have seen the numbers. Some health care providers may have had their Social Security numbers used as ID numbers for five years. At least 142 New Hampshire residents were affected, but the number of affected individuals nationwide was not revealed.
The back door of a contractor truck popped open during its journey between a St. Louis distribution center and Memphis, Tennessee. Hundreds of pieces of U.S. mail were scattered across 70 miles of highway. A recovery effort was launched by police officers and postal workers within 24 hours. Most of the mail included statements and bills that were headed for the West Coast.

---

Michael's Rock Hill Grille
Rock Hill, South Carolina

Michael's appears to be the common thread in a number of credit card fraud cases in the Southeast. It is believed that someone accessed credit card information by using malware on or obtaining passwords for the system on which the information was stored. The group of affected people most likely includes customers who used their card between September 16 and early December. Many of the cases involved Florida residents, but people in Texas, Kentucky, Tennessee, Georgia and Washington were also affected.

---

Tulane University
New Orleans, Louisiana

A University issued laptop was stolen from an employee's car on December 29. The laptop was used to process 2010 tax records for employees, students and others who will receive a 2010 W-2. The information included names, Social Security numbers, salary information and addresses.

---

Iowa Telecommunications, Experian
Newtown, Iowa

One of Experian's clients experienced a breach that gave unauthorized users access to Experian's pool of consumer names, Social Security numbers, dates of birth and account numbers. Someone gained access to the Experian login information for Iowa Telecommunications and was able to obtain consumer report information in the company's name.

---

South Carolina State Budget and Control Board Employee Insurance Program
Columbia, South Carolina

People who are covered by South Carolina's state insurance program may have had their personal information obtained. A virus affected one of the Insurance Program's computers. The breach occurred sometime between November 8 and November 18. Insured current and former employees, dependents and survivors may have had their names, Social Security numbers, health information, addresses and dates of birth exposed.

---

Omaha School Employees Retirement System
Omaha, Nebraska

A breach of Omaha School Employees Retirement System's website was discovered on December 21. The incident occurred because of an attempt to access administrator log-in information. The hacker or hackers may have obtained a database with names, Social Security numbers, dates of birth, years of service and beneficiary information of current and former Omaha Public Schools employees. The website was shut down within two hours of the discovery.

---

California Therapy Solutions
California

The breach could have affected four different offices in southern California. No city is listed.

The November 15 theft of a device resulted in the exposure of protected patient health information.
<table>
<thead>
<tr>
<th>Date</th>
<th>Organization</th>
<th>Location</th>
<th>Detail</th>
<th>Affected Patients</th>
<th>SSN Information</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 14, 2011</td>
<td>Osceola Medical Center, Hils Transcription Service</td>
<td>Osceola, Wisconsin</td>
<td>The November 25 hack of a Hils Transcription server exposed the health information of 500 patients.</td>
<td>MED HACK</td>
<td>500 (No SSNs or financial information reported)</td>
<td></td>
</tr>
<tr>
<td>January 14, 2011</td>
<td>International Union of Operating Engineers Health and Welfare Fund, Zenith Administrators, Inc.</td>
<td>Baltimore, Maryland</td>
<td>Papers pertaining to Union's employee benefits program were stolen from Zenith's office on November 3. Zenith administers the benefits program. The papers contained health information.</td>
<td>NGO PHYS</td>
<td>800 (No SSNs or financial information reported)</td>
<td></td>
</tr>
<tr>
<td>January 14, 2011</td>
<td>Azure Acres</td>
<td>New York, New York</td>
<td>People in Sebastopol, California were affected. Concerned patients may call (855) 252-3784. The November 12 theft of a physician's laptop resulted in the exposure of client information. The information included full name and billing information, but did not include addresses or Social Security numbers. Azure Acres is a drug and alcohol abuse facility.</td>
<td>MED PORT</td>
<td>699 (No SSNs or financial information reported)</td>
<td></td>
</tr>
<tr>
<td>January 14, 2011</td>
<td>Blue Cross Blue Shield of Michigan (BCBSM), Tstream Software</td>
<td>Harper Woods, Michigan</td>
<td>The location listed is the headquarters of Tstream Software. Members with questions may call (866) 519-5876. A BCBSM website created by Tstream was the source of a breach. A BCBSM found her personal information online when searching her name. People applying for individual health insurance between 2006 and an unclear date had their names, Social Security numbers, addresses and dates of birth exposed. BCBSM was notified of the error on November 17, 2010. The information was accessible for an unspecified amount of time. Though 6,500 BCBSM members were notified, only 2,979 were affected.</td>
<td>MED DISC</td>
<td>2,979 (No SSNs or financial information reported)</td>
<td></td>
</tr>
<tr>
<td>January 13, 2011</td>
<td>St. Vincent Hospital</td>
<td>Indianapolis, Indiana</td>
<td>St. Vincent encouraged patients who received letters to call 800-805-7004. In November, Saint Vincent officials learned that several associate email accounts had been breached. A third party managed to obtain email logins. Patient names, dates of service and clinical information may have been accessed.</td>
<td>MED UNKN</td>
<td>1,800 (No SSNs or financial information reported)</td>
<td></td>
</tr>
<tr>
<td>January 13, 2011</td>
<td>Green River District Health Department, Fox Technology Group (now part of Intergranetics)</td>
<td>Owensboro, Kentucky</td>
<td>The personal information of people who visited Green River District Health Department was accidentally placed online by Fox Technology. A resident notified the Department after discovering personal information online. Many visitor names were given with dates of birth; around half included Social Security information as well. The information was exposed</td>
<td>MED DISC</td>
<td>18,871 (more than half with SSNs)</td>
<td></td>
</tr>
</tbody>
</table>
sometime in October of 2010 or before. The problem was fixed soon after the Department was notified.

**UPDATE** (3/16/2011): There were 18,871 visitors who were affected, not 9,986.

**Information Source:**
 PHIPrivacy.net

**January 13, 2011**

**New Mexico National Guard**
**Sante Fe, New Mexico**

A computer with the deployment records and Social Security information of soldiers throughout the state was stolen from the National Guard Headquarters in Sante Fe. The theft occurred sometime between December 23 and 28.

**Information Source:**
 PHIPrivacy.net

**January 12, 2011**

**Kadlec Regional Medical Center**
**Richland, Washington**

Those with questions may call (877) 451-9363.

**Information Source:**
 Databreaches.net

**January 12, 2011**

**Seacoast Radiology**
**Rochester, New Hampshire**

http://www.seacoastprivacy.com/

On November 12, Seacoast discovered that a server had been breached. Patient names, Social Security numbers, addresses, phone numbers and other personal information may have been exposed by the breach. Credit card and other financial information were not exposed. The estimated number of individuals who received notification is 231,400. Not all people who received a notification letter were affected. Patients and people serving as insurance guarantors were affected. It is believed that the hackers were utilizing Seacoast's bandwidth to play a popular game called Call of Duty: Black Ops.

**Information Source:**
 PHIPrivacy.net

**January 12, 2011**

**Universal Medical Center**
**Tucson, Arizona**

Three staff members and one contract employee were fired for viewing sensitive patient information without cause. The electronic medical records of patients who were injured during a terrorist shooting spree may have intrigued the workers. There were no reports of confidential patient information being released to the public.

**Information Source:**
 PHIPrivacy.net

**January 11, 2011**

**University of Connecticut, HuskyDirect.com**
**Storrs, Connecticut**

Customers who used their credit cards on UConn's Huskydirect.com sports gear website may have had their personal information exposed in a data security breach. A hacker was able to access the Huskydirect.com customer database and may have viewed billing information with names, addresses, telephone numbers, credit card numbers, expiration dates, security codes and email addresses. The Huskydirect.com database is run by an outside vendor. People who made purchases offline are not at risk.

**UPDATE** (1/31/2011): Some people who were affected by the breach have recently reported fraudulent charges.

**UPDATE** (2/19/2011): Additional details reveal the exact number of names that were on the customer database, the fact that the perpetrator used an administrative password, and the fact that Fandotech, the company that was hosting and managing the site, was not following correct web security procedures.

**Information Source:**
 Databreaches.net

**January 10, 2011**

**Entertainment Software Rating Board (ESRB)**
**New York, New York**

1,000 (No SSN or financial information exposed)
People who contacted ESRB to complain about a Blizzard Entertainment change in privacy were sent a response that included the emails of other people who had contacted ESRB with similar concerns. Blizzard had proposed implementing Real ID (required usage of real first and last name) for participation in forums, but abandoned it after a backlash.

Information Source: Databreaches.net
January 8, 2011 Race Trac Melbourne, Florida BSR CARD 600

People with questions may call (321) 259-1211.

Authorities investigating fraudulent debit and credit card charges discovered a skimming device inside of a gas pump. Only one pump at the station was found to have a skimming device. Gas station employees first learned about the possible existence of a skimmer at their store in December.

Information Source: Databreaches.net
January 8, 2011 Campus Suite Apartments West Lafayette, Indiana BSO PHYS 30

In November of 2008, documents with tenant Social Security numbers and dates of birth were stolen from the office. Many of the tenants were able to avoid fraudulent charges by immediately placing fraud alerts on their accounts. One man pleaded guilty to stealing the information and another pleaded guilty to using the information to commit fraud and identity theft.

Information Source: Databreaches.net
January 8, 2011 Washington State Employment Security Division Olympia, Washington GOV PHYS 1,000

Authorities discovered that names and Social Security numbers of hundreds of Employment Security Division state employees were in the possession of a man who intended to misuse and profit from the information. The man was arrested and held on 50 counts of identity theft. It appears that the employee information was stolen from a car parked on the state Capital campus sometime in 2009. Authorities are still notifying those who were affected by incident.

Information Source: Databreaches.net
January 8, 2011 Duval Clerk of Courts Jacksonville, Florida GOV DISC Unknown

People who want to check their information in the Duval system must go to http://www.duvalclerk.com, scroll to the bottom of the page, click "search court and official records", click "OnCore" and type in their name.

Someone discovered sensitive information on the government website. Some Social Security numbers and bank account numbers were viewable. Records entered after and around 2002 are carefully checked for Social Security numbers and bank accounts, but some records prior to that time still contain sensitive information. The clerk's office removed sensitive information from several records after being notified of the problem.

Information Source: Databreaches.net
January 6, 2011 Adventist Behavioral Health Rockville, Maryland MED PHYS Unknown

Patients whose information was compromised may call (301) 251-4567.

An employee error caused sensitive patient documents to be sent to a recycling facility. Some of the documents, which should have been shredded instead of recycled, were found on December 29 after being blown out of a recycling truck. The documents included patient names and dates of birth. The papers that fell off the truck were shredded by Adventist and any documents that remained at the facility were destroyed there. The employee responsible for the mistake was not fired.

Information Source: PHIPrivacy.net
January 6, 2011 Grant Medical Center, OhioHealth Columbus, Ohio MED INSD 501 (No SSNs or financial information reported)

Affected individuals may call 1 888-845-0818.
On November 5, several out-of-service computers were determined to be missing from a storage facility. An investigation revealed that a dishonest employee had stolen the computers, attempted to clear the hard drives and was in the process of reselling them. Information from patients treated at Grant between 2008 and November 5 of 2010 may have remained on the stolen computers.

**UPDATE (1/14/11):** The breach affected 501 individuals.

---

### Information Source: PHIPrivacy.net

**January 6, 2011**

**Heraeus Incorporated**  
**New York, New York**

BSO  PORT  514

The location listed is Heraeus Incorporated's headquarters. The incident may have occurred elsewhere.

A steel cabinet was discovered missing on November 18. The cabinet had a safe which contained IT data and software backup tapes. Personal information on the backup tapes included names, Social Security numbers, addresses, financial account numbers, driver’s license numbers, medical information and other personal information. The cabinet was most likely thrown out during a cleaning. If so, the cabinet and its contents would have been taken to a transfer station, crushed, and then transported to a landfill for further destruction and disposal.

---

### Information Source: PHIprivacy.net

**January 6, 2011**

**Marsh U.S. Consumer, Seabury and Smith, ITT Corporation**  
**Tulsa, Oklahoma**

BSO  DISC  Unknown

Some ITT Corporation employees may have been able to view unencrypted personal information of other ITT employees when accessing an ITT website serviced by Marsh U.S. Consumer. The incident resulted from a programming issue and occurred from November 1 through November 8. Employees and their spouses may have had their Social Security numbers and medical history information exposed. Marsh U.S. Consumer is a service of Seabury and Smith. At least nine New Hampshire residents were affected by the breach, but the total number of individuals affected nationwide was not revealed.

---

### Information Source: PHIPrivacy.net

**January 6, 2011**

**Private Dental Practice**  
**Germantown, Maryland**

MED  HACK  1,000

The office discovered a hacking incident after the computer system shut down on October 14. A hacker accessed the computer system and server. Patient names, Social Security numbers, addresses, dates of birth, dental care and X-ray records, dental insurance member numbers and health insurance member numbers may have been exposed.

---

### Information Source: HHS via PHIprivacy.net

**January 6, 2011**

**PinnacleHealth System, Gair Medical Transportation Services**  
**Harrisburg, Pennsylvania**

MED  DISC  1,086

Affected patients may call 1-877-825-4485.

Pinnacle became aware that outpatient information may have been accessed through an independent medical transcription company. Gair provides transcription services for Pinnacle and may have experienced a breach in 2008 that involved its computer server. Gair’s server appears to have been open to access through the Internet. Pinnacle became aware of the incident in mid-August when someone reported seeing patient information on the Internet. The information included Social Security numbers, medications, dates of birth, dates of interviews and dates of examinations.

---

### Information Source: PHIprivacy.net

**January 6, 2011**

**Pentagon Federal Credit Union (PenFed)**  
**Alexandria, Virginia**

BSF  HACK  514

The location listed may not be the location of the breach.

On December 12, a laptop was found to be infected with malware. PenFed current and former employees, beneficiaries, current and former members and joint owners may have had their names, Social Security numbers, addresses, credit and debit card numbers, and PenFed account numbers exposed. At least 514 New Hampshire residents were affected, but the total number of affected individuals nationwide was not reported.

**UPDATE (1/18/11):** The breach affected 674 New Hampshire residents and an unknown number of people nationwide.

---

### Information Source: Databreaches.net

**January 5, 2011**

**Taco Bell**  
**50 461**
January 5, 2011  Grand Rapids, Michigan

Two Taco Bell employees were paid to use skimming devices at their store or stores. Between 50 and 100 customers had their credit card information obtained. It is likely that the scam lasted several weeks during the second half of 2010. Two of the men who bought information from the Taco Bell employees were arrested and charged after one of them was recorded buying pre-paid cards.

Information
Source: Databreaches.net

January 4, 2011  White Rock Networks
Plano, Texas

Nearly 50 boxes of medical records, Social Security numbers, addresses, phone numbers and other personal information were found in a paper recycling dumpster behind a library. White Rock personnel records from 2000 to 2005 were in the boxes. The company went bankrupt in 2006 and was purchased. A local news crew contacted at least one of the affected people so that she could retrieve her information.

Information
Source: PHIPrivacy.net

January 3, 2011  EVG Quality Gas
Sierra Madre, California

On December 27, a customer reported fraudulent charges on her credit card after using it at the station. Later cases of identity theft were also traced to the gas station.

UPDATE (1/6/11): The gas station closed shortly before customers started reporting fraudulent charges. The former owner and two other people are being sought for questioning. Customers had their debit and credit card information captured by a skimming device when they used their cards at a store ATM or inside the store.

UPDATE (1/10/11): The total number of victims is now at 380 and over $109,000 in fraudulent charges have been made.

Information
Source: Databreaches.net

January 3, 2011  Half Hitch Tackle
Panama City, Florida

A breach of the systems security resulted in the exposure of customer credit and debit cards. It is possible that the breach originated overseas.

Information
Source: Databreaches.net

January 1, 2011  Kinetic Concepts Inc, (KCI)
San Antonio, Texas

A call center employee with authorization to access a customer payment card database used some of the information to make fraudulent purchases. The database contained names, addresses, insurance information and dates of birth. The Social Security numbers and payment card information of some customers were also in the database.

Information
Source: PHIPrivacy.net

December 31, 2010  Sovereign Bank
Wyomissing, Pennsylvania

The Bank became aware of suspicious online activity on October 15. On December 15, it was determined that a key logger had been installed on a company laptop. Customer names, Social Security numbers and addresses may have been accessed by unauthorized parties. At least 2 New Hampshire residents were affected, but the total number of affected individuals nationwide was not revealed.

Information
Source: Databreaches.net

December 31, 2010  Samuels, Green, and Steel, LLP
Irvine, California

An unauthorized party obtained the law firm’s login information and accessed consumer credit reports.

Information
Source: Databreaches.net

December 31, 2010  CHS, Inc.
St. Paul, Minnesota


PATR-1099 forms were mailed with names and Social Security numbers visible from the outside of the envelope. The company became aware of the problem after a recipient notified them of the mistake. The error did not affect all recipients.

**Information**
**Source:** Databreaches.net

December 31, 2010  
**Armstrong Atlantic State University**  
**Savannah, Georgia**

EDU PORT Unknown

Affected individuals may call (912) 344-3529.

A portable hard drive was stolen from the nursing department in early October. It contained the Social Security numbers of several hundred alumni.

**Information**
**Source:** Databreaches.net

December 28, 2010  
**Apothecary of Colorado**  
**Denver, Colorado**

MED PHYS Unknown

A man handling recyclables near his home found a conspicuous binder in a dumpster. It turned out that medical marijuana records had been placed there. The names, Social Security numbers, dates of birth, addresses and phone numbers of patients were in the binder. The current owners believe the records are from the previous owner or owners. "Dozens" of people were affected.

**Information**
**Source:** PHIPrivacy.net

December 28, 2010  
**Geisinger Health System**  
**Wilkes-Barre, Pennsylvania**

MED DISC 2,928 (No SSNs or financial information reported)

A former physician emailed patient medical information to his home email account in an unencrypted manner. The information included patient names, medical record numbers, procedures and indications. The physician deleted the information from his computer, home network and servers. The incident occurred on or around November 3.

**Information**
**Source:** PHIPrivacy.net

December 27, 2010  
**Riverside Mercy Hospital, Mercy Health Partners**  
**Toledo, Ohio**

MED PHYS 1,000 (No SSNs or financial information reported)

Concerned current and former patients and employees may call 1-877-451-9361 for more information.

Patient and employee records were left in the Hospital after the facility was sold to Toledo Public Schools in 2003. The Hospital closed in 2002 and was sold in 2003. Records were left unsecured in the facility from 2003 until the discovery in November of 2010.

**Information**
**Source:** PHIPrivacy.net

December 27, 2010  
**American Honda Motor Company**  
**Torrance, California**

BSR HACK 4.9 million (No SSNs or financial information reported)

A Honda vendor maintaining a customer mailing list for My Acura and Honda's Owner Link websites was hacked. Names, email addresses, vehicle identification numbers and user IDs may have been exposed. There is speculation that this breach is connected to a hack of Silverpop that exposed the information of McDonald's and deviantART subscribers.

**UPDATE** (1/24/11): Around 2.2 million Honda customers had their information exposed. Around 2.7 million Acura customers had their email addresses exposed, but names and other information were not breached.

**Information**
**Source:** Databreaches.net

December 25, 2010  
**Dallas Police Department**  
**Dallas, Texas**

GOV PORT Unknown
Laptops were stolen from ten decommissioned Dallas police cars. The decommissioned squad cars were burglarized sometime during the last six months. The laptops were used to check license plates, receive calls, and check people's records. Officials believe there is little chance of sensitive information on the laptops or Dallas police network being accessed by unauthorized persons.

**Information**

*Source:* Databreaches.net

**December 23, 2010**

**Mankato Clinic**

*Mankato, Minnesota*

3,159 (No SSNs or financial information reported)

Patients who received a notification letter may call 1-800-657-6944 X8633 or 625-1811 X8633.

A laptop was stolen from the car of a registered nurse sometime between November 1 and 2. It contained a spreadsheet with patient names, dates of birth, medical record numbers, health provider names and diagnosis information. Patients were notified in late December because it took nearly two months to notify patients because the Clinic was determining what was on the laptop.

**Information**

*Source:* PHIPrivacy.net

**December 23, 2010**

**Stens Corporation**

*Jasper, Indiana*

BSF INSD Unknown

Former employees continued to use passwords to access Stens' computer system after they left the company. Both employees left to work for a competitor and are thought to have used information on the computer system for commercial advantage and personal benefit. Stens employees became suspicious and changed the passwords, but the former employees guessed the new passwords. One of the men pleaded guilty to computer intrusion.

**Information**

*Source:* Databreaches.net

**December 23, 2010**

**Louisiana Horsemen’s Benevolent and Protective Association (HBPA)**

*New Orleans, Louisiana*

NGO INSD Unknown

A former employee admitted that she conspired with others to send fraudulent votes. The woman falsified election ballots for members unlikely to vote, enclosed them in envelopes and marked the envelopes with the members’ Social Security numbers. The purpose was to rig the outcome of the 2008 March HBPA election.

**Information**

*Source:* Databreaches.net

**December 22, 2010**

**Zarzamora Family Dental Care**

*San Antonio, Texas*

800 (No SSNs or financial information reported)

The October 15 theft of a desktop computer affected 800 patients.

**Information**

*Source:* HHS via PHIPrivacy.net

**December 22, 2010**

**Hospital Auxilio Mutuo**

*Hato Ray, Puerto Rico*

1,000 (No SSNs or financial information reported)

The Hospital experienced a breach of one or more computers on or around November 19. The exact nature of the breach was not reported and could have been theft, unauthorized access, hacking, or an IT incident.

**Information**

*Source:* HHS via PHIPrivacy.net

**December 22, 2010**

**Cook County Health and Hospital Systems**

*Chicago, Illinois*

556 (No SSNs or financial information reported)

A desktop computer was found to be missing on or around November 1. It contained the medical record identification numbers, names, dates of birth, clinic names, physician names, and lab results of some patients.

**Information**
The location listed is the residence of the hacker.

A hacker accessed the SWReg computer system. The SWReg system is used by Digital Rivers to pay contractors. The
system was altered to transfer money to the hacker’s bank account instead of the accounts of contractors. The hacker
faces 20 years on wire fraud charges and 10 years on computer hacking charges.

The location listed is the office of Community First Credit Union.

Cambrium Group, a contractor for Community First Credit Union, placed an unsecured Community First job applicant SQL
database online. The database was discovered on October 20 of 2010. The employment information included names,
dates of birth, education, addresses, telephone numbers, Social Security numbers and other information typical of
applications.

The names, Social Security numbers and treatment locations of about 140 veterans were mixed in with other paperwork.
The paperwork was sent to an EEOC office and viewed by multiple persons there. It appears that the names should not
have been visible.

Fifty-eight VA guardianship files were accidentally shared by a federal fiduciary office. Fifty-seven veterans were affected
when the fiduciary office accidentally sent the files to another fiduciary office that was not authorized to receive the
information. The information included names and Social Security numbers.

A digital camera with veteran information was discovered missing on November 21. It contained the names, Social
Security numbers, dates of birth and images of patients. Images of veterans who had been photographed in the last three
weeks were on the camera.

The Orthopedics Department was using Yahoo.com to keep track of patient scheduling. The information had been stored
on Yahoo.com since July of 2007 and multiple current and former residents of the center had access to the password and
account. Patients had their name, date and type of surgery and final four digits of Social Security number exposed. The
information was deleted from the web page on November 29.
A former employee is accused of stealing patient information and using it to commit identity theft. The former employee is charged with 15 counts of identity theft and criminal enterprise. Investigators believe the employee stole the information of cancer patients and used it to obtain credit cards.

Information
Source: PHIPrivacy.net

December 20, 2010  Saint Louis University  St. Louis, Missouri

St. Louis University's network was breached during the week. At least some Social Security numbers and personal information of employees were exposed, but students also received notification of the breach. Employees who had been with the University for at least five years were affected.

Information
Source: Databreaches.net

December 20, 2010  Centra  Alpharetta, Georgia

A laptop was stolen from the trunk of an employee's rental car overnight on November 11. Patient names and billing information were on the laptop. The delay in notification occurred because of the time it took to determine what information was on the stolen laptop.

UPDATE (1/14/11): The total number of affected individuals was changed from 13,964 to 11,982.

Information
Source: PHIPrivacy.net

December 20, 2010  Dean Clinic and St. Mary's Hospital  Madison, Wisconsin

A laptop was stolen during a home invasion on or around November 8. Patient names, dates of birth, medical record numbers, dates and types of procedures, diagnoses, and some pathology data were on the laptop.

Information
Source: Databreaches.net

December 20, 2010  Dino’s Pizza, M&T Pizza Inc.  Fayetteville, North Carolina

The former owner of the restaurant was sentenced to five years and five months in prison for identity theft and skimming charges. The former owner was found to have used more than 183 credit numbers from patrons and generally added a fraudulent charge of $15 to $30 to each credit or debit card.

Information
Source: Databreaches.net

December 19, 2010  Stony Brook University  Stony Brook, New York

Student and faculty network and student IDs were posted online on sbuchat.com. A file with all registered student and faculty ID numbers could be downloaded in a PDF or Excel format. A systems engineer undergraduate discovered a flaw in the SOLAR system that allowed him to change students’ NetID passwords without knowledge of the original password. The student then accessed the complete list of student and faculty IDs and posted the information.

Information
Source: Databreaches.net

December 17, 2010  Integrated Biometrics Technology (IBT)  Waco, Texas

A former employee who had worked as a live scan operator took thousands of background check applications she had processed and used them to obtain fraudulent credit cards and financial accounts. The applications were from Fingerprint Applicant Services of Texas (FAST) and used for Texas licensing and certification. The former employee is
alleged to have conspired with at least three other people.

Information
Source: Databreaches.net

December 17, 2010
deviantART, Silverpop Systems Inc.
Hollywood, California
BSO HACK
13,000,000 (No SSNs or financial information exposed)

Mirroring the Gawker and McDonald's breaches earlier this month, hackers exposed the email addresses, user names and birth dates of the entire deviantART user database. Hackers were able to breach deviantART's marketing company Silverpop Systems Inc. Passwords and sensitive information were not exposed, but the breach is expected to increase spam for registered users.

Information
Source: Databreaches.net

December 16, 2010
Azteca
Okeechobee, Florida
BSR INSD Unknown

A convenience store clerk was indicted on federal conspiracy, wire fraud, credit card fraud and aggravated identity theft charges. He is accused of using a skimmer device to obtain credit card information during normal customer credit card transactions. The stolen information was used to recreate gift cards and other credit cards with magnetic strips to create counterfeits. The employee was outed after selling a card to someone who then informed the FBI.

Information
Source: Databreaches.net

December 16, 2010
Twin America LLC, CitySights NY
New York, New York
BSO HACK 110,000

On or around October 25 a web programmer discovered that malicious script had been placed on the server. The script appears to have been uploaded on September 26 and had allowed access to the customer database multiple times between that date and October 19. Customer names, credit card numbers, credit card expiration dates, CVV2 data, addresses and email addresses may have been exposed.

Information
Source: Databreaches.net

December 16, 2010
Wackenhut
Palm Beach Garden, Florida
BSO PORT Unknown

Hard drives were stolen during shipment between Iraq and the US. The company became aware of the loss on November 29. The hard drives contained former employee full names, Social Security numbers, passport numbers, addresses and dates of birth.

Information
Source: Databreaches.net

December 16, 2010
Concur Technologies Inc.
Redmond, Washington
BSO STAT 1,017

Computer equipment and software with employee information were stolen during a November 27 or 28 office burglary. The information included names, Social Security numbers, addresses and dates of birth.

Information
Source: Databreaches.net

December 15, 2010
California Department of Public Health
West Covina, California
MED PORT 2,550 (Unknown number of SSNs)

A magnetic tape was lost during shipping between West Covina and Sacramento on or around September 27. The health care facility staff and residents who were determined to have been affected were notified on November 23. Employee emails, employee background reports, investigative reports, names and diagnosis information on health care facility residents and Social Security numbers for CDPH workers were on the tape.

Information
Source: PHIprivacy.net

December 15, Ohio State University

750,000 (Unknown number of SSNs)
Affected individuals can find more information at www.osu.edu/creditsafety

Students, professors and other University affiliates were notified that their information may have been accessed by a hacker. University officials discovered the breach in late October. Unauthorized individuals logged into an Ohio State server and had access to names, Social Security numbers, dates of birth and addresses of current and former students, faculty, staff, University consultants and University contractors.

UPDATE (1/14/11): 517,729 former students and 65,663 current students were affected. Exact numbers for current and former faculty, staff, consultants and contractors were not given.

UPDATE (2/22/2011): As of February 22, OSU was still attempting to find and inform affected individuals of the breach. Around 226,000 notification letters were mailed to alumni in February.

Information Source: Databreaches.net  
records from this breach used in our total: 750,000

---

March 15, 2010  
Social Security Administration Office of Temporary Disability Assistance  
New York, New York  
GOV INSD  
15,000

A subcontractor illegally downloaded around 15,000 Social Security numbers while performing upgrades. People who had made Social Security disability claims may have been affected.

UPDATE (1/4/2011): Dates of birth, addresses and phone numbers may have also been accessed.

Information Source: Databreaches.net  
records from this breach used in our total: 15,000

---

December 14, 2010  
Home Depot  
Tallahassee, Florida  
BSR INSD Unknown

A loss prevention officer reported that an employee was using a skimming device to steal the credit card information of customers. The officer reported the employee on December 8 and the employee was caught in the act of using a skimmer on December 10. The number of customers affected by these incidents and the length of time the employee worked at the store have not been reported.

Information Source: Databreaches.net  
records from this breach used in our total: 0

---

December 14, 2010  
Department of Education Federal Student Aid (FSA) Division  
Dolton, Illinois  
GOV INSD Unknown

A former FSA employee repeatedly accessed the National Student Loan Database System (NSLDS) during her employment. The employee searched and viewed confidential student loan records of several hundred people without reason between April of 2006 and May of 2009. The former employee pleaded guilty and is scheduled to be sentenced on February 22 of 2011.

Information Source: Media  
records from this breach used in our total: 0

---

December 14, 2010  
McDonald's, Arc Worldwide, Silverpop Systems Inc.  
Atlanta, Georgia  
BSR HACK Unknown

The location listed is Silverpop's headquarters.

Hackers were able to access the information of McDonald's customers. People who signed up for online promotions or newsletter subscriptions may have had their email addresses, contact information and birth dates exposed. McDonald's uses a company called Arc Worldwide for its marketing services. The breach was through Arc Worldwide's business partner Silverpop Systems Inc.

Information Source: Databreaches.net  
records from this breach used in our total: 0

---

December 13, 2010  
Mountain Vista Medical Center  
Mesa, Arizona  
MED PORT  
2,284 (No SSNs or financial information reported)

On October 13, multiple memory data cards were discovered to be missing from two endoscopy machines. The information of patients who had procedures performed between January of 2008 and October 12 of 2010 was on the data cards. The information included full name, hospital record number, date of birth, gender, age, date and type of procedure and image(s) related to the procedure.

Information Source:  
records from this breach used in our total: 468
December 13, 2010  
**Liberty Tax Service**  
Portsmouth, Virginia  
BSF  
PHYS  
Unknown

Personal tax documents were left exposed in a dumpster. The tax documents had Social Security numbers, addresses and financial information. The company did not reveal how the documents may have found their way into the dumpster, but said that it was against company policy to leave them exposed and intact. At least one person had their tax information from 2008 exposed. The number of documents was described as "mounds".

December 12, 2010  
**Gawker**  
New York, New York  
BSO  
HACK

Hackers gained access to the Site's database. Staff and user emails and passwords, the site code and staff messages were made accessible to anyone. The group claiming responsibility calls themselves Gnosis. Gawker encouraged users to change their passwords after their information was exposed. This may also mean changing passwords for other sites where users have similar screen names and passwords. Gnosis claims they had access to the site for a long time and exposed Gawker's information "because of their outright arrogance."

December 11, 2010  
**Kaplan University**  
Chicago, Illinois  
EDU  
INSD  
Unknown

The former dean of law and legal studies was convicted of making threats to students, staff and executives via email. The former University employee hacked into a colleague's email account and sent threats about identity theft and more to people during 2007. The former employee claims he was framed after threatening to expose the University's misconduct.

December 10, 2010  
**Memorial Hospital of Gardena**  
Gardena, California  
MED  
PHYS  
771 (No SSNs or financial information reported)

The Hospital reported that the unauthorized access or disclosure of paper records affected patients. The incident occurred on or around October 14.

December 10, 2010  
**Albert Einstein Healthcare Network**  
Philadelphia, Pennsylvania  
MED  
STAT  
613 (No SSNs or financial information reported)

The October 21 theft of a desktop computer may have exposed the protected health information of patients.

December 10, 2010  
**Kings County Hospital Center**  
Brooklyn, New York  
MED  
STAT  
542 (No SSNs or financial information reported)

The August 22 theft of a desktop computer may have exposed the protected health information of patients.
Clinical reports with patient names, medical record numbers, hospital account numbers, physician names, dates of birth, diagnosis and other clinical information were accidentally placed on a website by PTC. It is possible that the reports were accessible from January 1 through September. PTC assists the Medical Center in transcribing dictated physician reports.

Information Source: HHS via PHIPrivacy.net

The location listed is Ochsner’s headquarters. Patients may call 1-877-365-1663 with questions. The senior public relations specialist can be reached at 504-842-9143.

On October 4, Ochsner was contacted by several patients claiming they had received the patient information of someone else. Letters had been sent on by HELP on September 27 that included incorrect names, medical record numbers, account numbers and account balances. HELP assists Ochsner patients with payment arrangements for outstanding hospital and clinical account balances. A programming error at HELP caused the mistake. No patient will be able to access another patient’s medical or financial records using the incorrect information from the letters they received.

Information Source: HHS via PHIPrivacy.net

UPDATE (8/10/2011): One of the people associated with the restaurant-related fraud ring was sentenced to four years in prison. He pleaded guilty in May to access device fraud and was ordered to pay nearly $95,000 in restitution. He was caught when law officers discovered counterfeit charge card making equipment and hundreds of fraudulent cards during a raid of his home.

UPDATE (11/02/2011): The dishonest Chicken Express employee who skimmed customer credit card numbers was sentenced to two years in prison and ordered to pay $95,000 in restitution to victims.

Information Source: Databreaches.net

Customers who used credit or debit cards at United States Journeys, Journeys Kidz, Johnston and Murphy, Shi by Journeys and some Underground Stations stores may have had their information gathered during a criminal intrusion of Genesco’s computer network. It is possible that credit and debit card numbers, expiration dates and card verification codes were accessed.

UPDATE (01/17/2013): Genesco has spent $2.1 million on consulting and legal fees related to the breach.

UPDATE (03/08/2013): Genesco also owns Lids. Genesco sued VISA for $13 million in unnecessary fines associated with the data breach. VISA fined banks for their role in failing to comply with industry-wide credit card security standards. The banks then took money from Genesco to address fines and breach recovery.

Information Source: Databreaches.net

Some records of people affiliated with UW Madison were hacked into. The University discovered the breach on October 26 and sent notification to many former students, faculty and staff on November 30. One of the files had the photo ID of former students with their Social Security numbers embedded in the ID numbers and cardholder names. Only students enrolled prior to 2008 would have had their Social Security numbers exposed. It is unclear how far back the records date.
December 10, 2010  Southwestern Indiana Regional Council on Aging (SWIRCA)  Evansville, Indiana

Client information was on a case manager's laptop that was stolen from the SWIRCA office. Files on the laptop contained patient names, Social Security numbers, dates of birth, addresses, phone numbers, demographic information, medical condition information and case information. The laptop was stolen sometime between November 4 and 8.

December 10, 2010  Walgreens  Deerfield, Illinois

A hacker managed to obtain Walgreens' email marketing list. People on the list were sent realistic-looking phishing emails that directed them to a web page under hacker control. The only information that was stolen during the hack was the email list. People who fell victim to the phishing scam may have entered other personal information into the phony web page.

December 9, 2010  Methodist Theological School in Ohio  Delaware, Ohio

The October 13 theft of a laptop resulted in the exposure of personal information of some people with a connection to MTSO. Names, Social Security numbers, dates of birth, financial payments received and letter grades for completed courses may have been stored on the laptop. The laptop was stolen from a locked off-campus site.

December 8, 2010  Illinois Secretary of State Drivers License Division  Libertyville, Illinois

An executive turned himself into authorities after being accused of selling Libertyville customer database information to identity thieves in exchange for sports tickets and gift cards. The executive faces three counts of conspiracy to commit identity theft.

December 6, 2010  Dartmouth College  Hanover, New Hampshire

A stolen storage device contained the credit information of 147 parents and freshmen. The device was stolen from a secure room on November 8. Phone numbers, credit card numbers and credit card expiration dates for participants in the Dartmouth Outdoor Club First Year Program were on the device.

December 5, 2010  American Check Cashers of Oklahoma, LLC  Tulsa, Oklahoma

Hundreds of blank checks, bank and telephone statements, Social Security card copies and ID copies were found in a dumpster by someone from a neighboring store. The documents date from 2004 to 2009. The owner of the business said that the mistake occurred when some sensitive documents were sorted in with non-sensitive documents and dumped rather than shredded. It is unclear whether the sorting error was made by the shredding company or the business. Ninety-six of the documents were kept by the neighboring store's owner. He agreed to return the documents to their owners and destroy the ones he cannot return.

December 4, 2010  Phoenix  Baltimore, Maryland

Phoenix was composed of tax businesses named Phoenix Tax World, 101 Taxes, 420 Income Tax Services and 1 One 1 Taxes.

Sometime between late 2005 and April of 2009 the owner of the business and a co-conspirator prepared more than 600 fraudulent individual federal income tax returns on behalf of clients. A book with the names, Social Security numbers and dates of birth of various children was found at the owner's home during a police search. The children's information was
used to claim false deductions for fictional dependents of her clients. The owner pleaded guilty to conspiracy to file false tax returns and aggravated identity theft.

**Information**
**Source:** Databreaches.net

**December 3, 2010**
**Manor Care of Indy (South), LLC**
**Indianapolis, Indiana**

The protected health information of 845 individuals may have been viewed or obtained by an unauthorized person or persons.

**Information**
**Source:** HHS via PHIPrivacy.net

**December 3, 2010**
**Prime Home Care, LLC**
**Omaha, Nebraska**

The September 13 theft of a desktop may have left patient information exposed.

**Information**
**Source:** HHS via PHIPrivacy.net

**December 3, 2010**
**Mesa County, Western Colorado Drug Task Force**
**Grand Junction, Colorado**

A former employee accidentally posted sensitive information in a place that was publicly accessible on the Internet. The home addresses of sheriff’s deputies, names of confidential drug informants, confidential emails between officers and other sensitive information were accessible from April until the discovery in November. The FBI is investigating which computer users may have accessed the information. The breach was discovered on November 24 when an individual searched the Internet and found one of the files mentioning his or her name.

**Information**
**Source:** Databreaches.net

**December 2, 2010**
**University of Arizona**
**Tucson, Arizona**

An external hard drive was discovered to be missing from a secure records room. It was lost sometime in October or earlier. The hard drive contained former student withdrawal and disciplinary action records. Some Social Security numbers may have also been exposed. The relocation of the records room is one possible cause of the loss.

**Information**
**Source:** Databreaches.net

**December 2, 2010**
**KMax Systems**
**Kissimmee, Florida**

A box of job applications was thrown out by a new manager. Someone found the applications and showed them to another person who then contacted some of the applicants. Addresses, Social Security numbers, driver’s license numbers, names, phone numbers and other information typical of an employment application were exposed. Some of the applications also had questionable interview comments that seemed irrelevant to the selection process.

**Information**
**Source:** Media

**December 1, 2010**
**State Department of Labor and Industries, Washington State Employees Credit Union, Court of Appeals**
**Tacoma, Washington**

Confidential paper files from at least three tenants of the state-owned Rhodes Building were found in an unsecured recycling bin. Some documents included names, Social Security numbers, checking account information, health information and dates of birth. A news report claimed the documents numbered in the dozens. Representatives for some of the organizations claimed that the files were supposed to be shredded.
Farber Enterprises is located in Kerrville, Texas.

Hundreds of documents were abandoned near a bridge in the Harlingen area. The documents contained receipts, invoices, canceled checks, Social Security numbers, addresses and phone and driver's license numbers. A man whose information was found said that he had applied for employment with Farber two or three years ago.

Information Source: Databreaches.net

An administrative report that should have been shredded was accidentally thrown in the trash. Reports are usually left in a storage location for 45 days and then discarded properly. The Hospital became aware of the breach on October 4. Anyone looking through the report would find names, Social Security numbers and other patient information.

Information Source: PHIPrivacy.net

A September 15 office burglary resulted in the theft of a desktop computer. The computer once held protected health information of people with state Medicaid claims. Some files included encoded names and diagnostic codes. Medicaid account numbers, financial information and Social Security numbers were not exposed.

Information Source: HHS via PHIPrivacy.net

Approximately 398,000 members in the North and Metro-North districts of Puerto Rico's government health insurance plan (HIP) were affected. The information of an additional 5,500 HIP beneficiaries, 2,500 Medicare beneficiaries and IPA from three HIP districts serviced by TSS was accessed.

An internet database managed by TCI containing information of some people insured by Triple-S Salud, Inc. was accessed by employees of a competitor. People insured by TSS under the Puerto Rican government’s health insurance plan and independent practice associations (IPA) that provided services to those may have had their information accessed. The breach was the result of the unauthorized use of one or more active user IDs and passwords for the TCI IPA database. TCI believes that financial information related to IPAs was the target of the attack and not the information of individuals. Multiple intrusions happened in September. A TCI competitor notified the organization on September 21.

Information Source: PHIPrivacy.net

A former employee was able to enter a secured area and log onto a hospital computer while attending a social event. The former employee’s access code had been left active and patient records were viewed during the incident.

Information Source: PHIPrivacy.net

Some guests and employees were affected by a breach or breaches that occurred between June 2010 and October 2010. Credit and debit card information was stolen and misused. The method that criminals used to access the information was not disclosed.

UPDATE (11/30/10): Other hotels owned by Desert’s parent company Shell Vacation Resorts may have been affected.

UPDATE (12/22/10): A notice on Shell’s website states that the breach occurred because of a malicious software
infection. It was determined that the management system software program of Shell Vacation properties was infected with the malware.

**Information**  
**Source:** Security Breach Letter  
**November 19, 2010**  
**Private Dental Practice**  
**Florissant, Missouri**  
MED PORT  
1,400 (No SSNs or financial information reported)

A dentist’s laptop was stolen from his car in October. It contained the clinical information for patients who saw him at a St. Charles office. The dentist notified police immediately, but waited about a month to notify patients.

**Information**  
**Source:** PHIPrivacy.net  
**November 19, 2010**  
**1st Source Bank**  
**South Bend, Indiana**  
BSF UNKN Unknown

The Bank’s third-party payment service provider had a breach incident. Customer account numbers and expiration dates may have been exposed. The Bank sent affected customers a new pin and debit card.

**Information**  
**Source:** Databreaches.net  
**November 19, 2010**  
**American Association of Retired Persons, AARP Insurance**  
**Washington, District Of Columbia**  
BSF DISC Unknown

Any customers who receive another customer’s information should call 800-784-5789.

A client received another client’s information in an insurance policy letter. He attempted to trace the mistake and notified the organization that underwrites AARP’s life insurance program, New York Life Insurance. It is unknown how this error occurred and client names, phone numbers, policy numbers, check account information and dates of birth could have been exposed.

**Information**  
**Source:** Databreaches.net  
**November 19, 2010**  
**Kern Medical Center**  
**Bakersfield, California**  
MED PHYS  
596

Six other health facilities were fined. Each of the other six incidents involved fewer than 10 records and only the Kern incidents are included in the total.

The California Department of Public Health fined Kern Medical Center in Bakersfield, CA, $250,000 for allegedly keeping patient records in an outside, unlocked locker, allowing for the theft of 596 patient records in 2009. For several months in 2009 a Kern Medical Center employee placed the daily lab reports in the broken locker outside the hospital until they were stolen one night. Six additional health facilities were also fined: Biggs Gridley Memorial Hospital, Gridley, Butte County; Children’s Hospital of Orange, Orange, Orange County; Delano Regional Medical Center, Delano, Kern County; Kaweah Manor Convalescent Hospital, Visalia, Tulare County; Oroville Hospital, Oroville, Butte County; Pacific Hospital of Long Beach, Long Beach, Los Angeles County. The total amount of fines for the seven health facilities was $792,000.

**Information**  
**Source:** Media  
**November 18, 2010**  
**Hanger Prosthetics and Orthotics Group**  
**Austin, Texas**  
MED PORT  
4,486

A laptop was stolen from a human resources employee on November 4. The laptop contained employee names, Social Security numbers, health information and addresses.

**UPDATE** (2/15/11): HHS shows that the breach affected 4,486 people.

**Information**  
**Source:** Databreaches.net  
**November 18, 2010**  
**EOD Technology (EODT)**  
**Knoxville, Tennessee**  
BSO HACK Unknown

One or more unauthorized individuals definitely accessed employee names and Social Security numbers in 2008. The breach was not reported until 2010 because EODT did not have evidence that personal information had been accessed during the breach. The firm claims that the breach did not lead to any fraudulent activity during those two years.
November 18, 2010
Federal Reserve Bank of Cleveland, FedComp
Cleveland, Ohio
GOV HACK Unknown
FedComp system held the data of the Firemen's Association of the State of New York Federal Credit Union and the Mercer County New Jersey Teachers' Federal Credit Union, and other federal credit unions.

A foreign national responsible for fraudulently obtaining or holding 400,000 credit card numbers was caught in the U.S. while attempting to meet hackers and utilize stolen financial information. The man is also accused of hacking into the Cleveland Federal Reserve Bank in June, though the amount of information he was able to obtain is unknown and separate from the 400,000 card numbers found on his computer.

UPDATE (4/13/2011): The foreign national pleaded guilty to hacking into a Federal Reserve Bank computer server belonging to the Federal Reserve Bank, and installing a malicious code onto that server. The man had compromised many other computer servers that belonged to large corporations, financial institutions, defense contractors and other groups, and selling or trading the information. Because FedComp, a data processor for federal credit unions was affected, financial information from federal credit unions in various states may have been inappropriately accessed.

November 17, 2010
Oklahoma Veterans Affairs Medical Center
Oklahoma City, Oklahoma
GOV PHYS 1,950
An employee noticed that some pages were missing from a laboratory log book on October 15. The pages may have contained the names, last four digits of Social Security numbers, appointment information and tests of 1,950 VAMC visitors. Veterans who visited between January 1 and October 8 may have been affected. The military believes the most likely cause of the loss is that the pages were shredded.

UPDATE (12/2/10): An VA investigation determined that the information was most likely accidentally shredded.

November 16, 2010
Education Department, Department of Veterans Affairs
Bronx, New York
GOV PHYS 146
A box was left unsecured during an October 25 relocation. Employee names and Social Security numbers may have been accessed by volunteers and employees during that time. The information was from employees who took the Cardiopulmonary Resuscitation (CPR) test.

November 16, 2010
All Star Lanes
Salina, Kansas
BSF PHYS Unknown
A laptop and money bag were stolen during a burglary that occurred between November 14 and November 15. The bag had thousands of dollar in cash, checks and credit card transactions.

November 16, 2010
Chili's
Dallas, Texas
BSR HACK Unknown
Chili's email club service provider InterMundo Media experienced a server breach. No financial information or Social Security numbers were collected for club membership, but full names, email addresses and dates of birth could have been accessed.

November 16, 2010
Messiah College
Grantham, Pennsylvania
EDU PORT 43,000
An external hard drive was lost or stolen. Current, former and prospective students and their parents may have had their names, Social Security numbers, dates of birth and transcripts exposed. The information was from the financial aid department and spans from 1994 to 2010. Social Security numbers were not collected for all individuals involved, but exact number of individuals who had their Social Security or financial information exposed was not given.

UPDATE (11/21/10): The drive was found by the employee responsible for it. The likelihood that someone was able to access the information on the drive for a malicious purpose is very low or nonexistent.
At least 13 New Hampshire residents and an unknown number of other U.S. customers were affected by a breach of Monadnock’s card processor. Customer debit card numbers, expiration dates, CVC and PIN offsets may have been exposed. The Bank believes there is no evidence that the incident is related to a previous incident that occurred in September of 2010.

Information
Source: Databreaches.net

November 15, 2010
ECS Learning Systems
Bulverde, Texas
BSR HACK 1,300

On October 15, ECS learned that a hacker had accessed their database of online customer order information. Names, addresses, telephone numbers, email addresses, and credit or debit card information may have been accessed. Customers were notified of the breach, but were not offered credit monitoring services or encouraged to cancel their credit and debit cards.

Information
Source: Databreaches.net

November 15, 2010
Kayser-Roth Corporation
Greensboro, North Carolina
BSR PORT Unknown

A laptop with employee information was stolen from the Corporate Payroll Department sometime between the end of the day on October 14 and the beginning of the day on October 15. Names, addresses, bank account information and Social Security numbers of current and former employees may have been exposed.

Information
Source: Databreaches.net

November 15, 2010
University of Nebraska
Lincoln, Nebraska
GOV DISC Unknown

Thousands of students had their financial aid and loan information posted on the state treasurer's website. The office is refusing to remove the information for the time being because of limited staff resources. The treasurer's office also claims that the University was given ample time to edit the data so that student names and financial information were not included. Students who received loans, scholarships and other aid for the 2008-2009 school year had their information posted on the website. Some people are concerned that con artists could contact the students on the list and pretend to be a lender who holds their student loan information. Information for 2009-2010 school year spending was also submitted with detailed student information and is scheduled to be uploaded sometime in November.

Information
Source: Databreaches.net

November 15, 2010
Henry Ford Health System
Detroit, Michigan
MED PORT 3,700 (No SSNs or financial information reported)

Those with questions may call (888) 313-1027.

An employee’s laptop was stolen on September 24. It contained the information of patients who received prostate services between 1997 and 2008. The laptop was stolen from an unlocked urology medical office. No Social Security numbers, full medical records or health insurance identification numbers were on the stolen laptop. Patient names, medical record numbers, dates of birth and treatment information were on the laptop.

UPDATE (11/23/10): The breach affected 3,700 patients.

Information
Source: PHIPrivacy.net

November 14, 2010
Northridge Hospital Medical Center
Northridge, California
MED PHYS 837

Patients who used services between September of 2004 and June of 2006, but did not receive a notification letter may call (877) 906-1590.

A package sent through a national courier was damaged during transit. Because of this damage, patient names, Social Security numbers, addresses, phone numbers, dates of birth, dates of death, physician, financial account number, insurance ID, Medicare and Medicaid charges billed and paid, hospital room and board charges and guarantor Social Security number may have been exposed. People who were patients between September of 2004 and June of 2006 were affected.

Information
Source: Databreaches.net

November 14, Aetna of Connecticut
MED UNKN 2,345 (No SSNs or financial information reported)
A number of insured customers were affected by an unauthorized access or accidental disclosure of personal information in September.

Information Source: HHS via PHIPrivacy.net

November 14, 2010  Private Dental Practice
Flower Mound, Texas

The August 5 theft of a laptop resulted in the exposure of patient information.

Information Source: HHS via PHIPrivacy.net

November 12, 2010  Visiting Nurse Association of Southeastern Connecticut
Waterford, Connecticut

Patients in the area may call (860) 444-1111. The toll free number is (855) 732-3107.

Current and former patients received notification letters stating that their personal information was on a stolen laptop. The laptop was stolen from a nurse's car while it was parked at her home on September 30. The laptop was used to store patient addresses, medical information and names.

Information Source: Databreaches.net

November 10, 2010  Holy Cross Hospital, Office of Dr. Elliot Stein
Fort Lauderdale, Florida

Dr. Elliot Stein is located in Aventura, Florida.

A criminal investigation uncovered 38 patient files. The files contained names, addresses, Social Security numbers, dates of birth and descriptions of initial diagnosis from Emergency Room visits. An investigation that began in June showed that an employee was responsible; that employee was fired. The employee may have inappropriately accessed 1,500 patient files between April 2009 and September of 2010. The Hospital now limits the amount of key personal data included in the type of documents involved in the incident.

UPDATE (2/17/2011): Five other suspects have been arrested within the past month. Authorities learned of the fraud ring in May of 2010.

UPDATE (4/15/2011): A former Holy Cross Hospital employee was sentenced to prison for disclosing patient information. The woman was sentenced to 24 months in prison with 12 months of home confinement, followed by three years of supervised release. After being caught selling patient information from her employer, she pleaded guilty to disclosing individually identifiable health information.

UPDATE (6/21/2011): It was revealed that one of the other suspects is being charged with selling information from the office of Dr. Elliot Stein in Aventura. A criminal investigation uncovered lists of patient information from Dr. Stein that included names, Social Security numbers, addresses, dates of birth, and health information.

Information Source: Databreaches.net

November 9, 2010  New Hanover County
Wilmington, North Carolina

A list of 9,845 property owner accounts was published online. Social Security numbers were attached to 163 of the accounts, though some people had multiple accounts. The list of delinquent accounts was mistakenly published before the Social Security numbers were removed. It is unclear how long the information was available online.

Information Source: Databreaches.net

November 8, 2010  Arista OB-GYN Clinic
Woodstock, Georgia
Private medical records were dumped outside a closed office. A news team found several hundred documents that appeared to mostly be patient records with names, addresses, sonograms, copies of checks and detailed medical information. The dumpster was confiscated and searched by police. Files were also found under the dumpster. The doctor could face felony charges.

**Information**

**Source:** PHIPrivacy.net

**November 7, 2010**  
**Richmond Public Schools**  
**Richmond, Virginia**  
**EDU**  
**DISC**  
**110**

An employee accidentally sent an email with the names, Social Security numbers and other personal information of 110 employees to 3,300 employees. Administrators began limiting access to the document and the entire email system after the mistake was discovered half an hour later. The email contained personnel changes, but was supposed to be emailed without the personal information of those employees who were moving within the organization.

**Information**

**Source:** Databreaches.net

**November 6, 2010**  
**General Services Administration**  
**Washington, District Of Columbia**  
**GOV**  
**INSD**  
**12,000**

An employee sent an email with the names and Social Security numbers of the entire staff to a private, outside address. Though notification emails were sent at the end of September, many employees learned of the incident in November.

**Information**

**Source:** Databreaches.net

**November 6, 2010**  
**Murphy USA**  
**Shelbyville, Indiana**  
**BSR**  
**PHYS**  
**Unknown**

A file cabinet with personal information was found in a dumpster near Murphy USA gas station. Most of the files belonged to former employees of the gas station. Dozens of copies of Social Security cards, driver’s licenses, contact information and other personnel information were retrieved. A representative from the gas station said that the files should have been shredded and that they are searching for the employee responsible.

**Information**

**Source:** Databreaches.net

**November 4, 2010**  
**Bare Escentuals**  
**San Francisco, California**  
**BSR**  
**PORT**  
**Unknown**

Sensitive employee data was on an employee’s stolen laptop. The employee information on the laptop included name, Social Security number, postal address and historic salary data.

**Information**

**Source:** Databreaches.net

**November 4, 2010**  
**American Federation of Television and Radio Artists (AFTRA)**  
**Los Angeles, California**  
**BSO**  
**HACK**  
**2,811**

Hackers were able to access the Join Online portion of AFTRA’s website. Hackers may have obtained the names, Social Security numbers, credit card numbers and contact information of people who joined AFTRA online. People who attempted to join online between September 14 and 29 may have also been affected by the breach. AFTRA has disabled the Join Online website. AFTRA’s internal membership database and the “members only” section of the website were not affected.

**Information**

**Source:** Databreaches.net

**November 2, 2010**  
**Seton Hall University**  
**South Orange, New Jersey**  
**EDU**  
**DISC**  
**1,500 (No SSNs or financial information reported)**

An Excel spreadsheet with academic information was accidentally emailed to 400 students. Fifteen hundred students had their names, addresses, emails, student ID numbers, majors, credit hours and GPAs exposed. Students who received the attachment were instructed not to view or distribute it. Students were also informed to meet with the associate dean for Undergraduate Student Services and Enrollment Management if they had already opened the attachment.

**Information**

**Source:** Databreaches.net

**November 1, 2010**  
**Thai Cafe**  
**Indianapolis, Indiana**  
**BSR**  
**PHYS**  
**Unknown**
An Indianapolis school noticed that their dumpster was being used by someone else. A box of personal information from the Thai Cafe was found to have been illegally dumped. School officials discovered complete payroll stubs from 2000 inside the box and contacted the restaurant owner. The ex-spouse of the restaurant owner apologized for the illegal dumping and claimed that the disposal was handled by a third party.

Information
Source: Databreaches.net

October 31, 2010 Robins Airforce Base
Warner Robins, Georgia

GOV HACK 50

Around 50 employees noticed fraudulent charges on their credit or debit cards after using them on base in August of 2010. Officials became aware of the problem and notified employees within two weeks of the incidents.

Information
Source: Databreaches.net

October 29, 2010 Southwest Seattle Orthopaedic and Sports Medicine
Burien, Washington

MED HACK 9,493 (No SSNs or financial information reported)

A hacking incident may have exposed the personal information of patients on September 4.

Information
Source: HHS via PHIprivacy.net

October 29, 2010 University of Hawai’i West O’ahu (UHWO)
Pearl City, Hawaii

EDU DISC 40,101

Students from the University of Mānoa were also affected.

Unencrypted files that were placed on the faculty web server exposed student information. Student names, Social Security numbers, birth dates, addresses and academic information were placed on the server in December of 2009. Students who attended UHWO in Fall of 1994 or graduated between 1988 and 1993 were affected. A much larger number of students who attended the University of Hawai’i Mānoa between 1990 and 1998 were also affected. The files were removed on October 18 after a privacy group notified the University. The server was quickly removed from the network. The faculty member who accidentally placed the file on the server retired before the breach was discovered.

UPDATE (11/19/10): A former student is filing a class-action lawsuit on behalf of students affected by the University of Hawai’i’s multiple breaches. The man attended the Mānoa campus between 1990 and 1998 and claims that he was affected by the this breach and one that occurred in June of 2009. The names of four other people are attached to his Social Security number and his credit has been used in Georgia. Around 259,000 private records have been exposed by the University of Hawai’i since 2005.

UPDATE (1/27/2012): The University of Hawaii will provide two years of credit protection services and credit restoration services to settle a class-action lawsuit involving data breaches that affected nearly 100,000 students, faculty, alumni, and staff between 2009 and 2011. The settlement is still subject to court approval.

Information
Source: Databreaches.net

October 29, 2010 Japanese Foundation of Los Angeles
Los Angeles, California

BSR HACK Unknown

An unnamed third-party vendor that hosted the organization’s jflac.org website experienced a security incident. Customers who made purchases related to Japanese Language Proficiency Testing for 2009 and 2010 may have had their names, dates of birth and credit card information accessed. The servers containing customer data were shut down and taken offline after the incident was discovered. The incident occurred on or around September 18, 2010 and the organization aimed to notify all affected customers by October 25.

Information
Source: Databreaches.net

October 28, 2010 Minor Family Clinic
Phoenix, Arizona

MED UNKN 128 (No SSNs or financial information reported)

An insurance fraud scheme used medical information from the Clinic. Fraudulent charges to patients’ insurance companies totaled $108,000. Two people have been indicted, but their method for accessing patient information has not been reported.
PHIPrivacy.net

October 28, 2010

**Emergency Medical Services Bureau**

*Baton Rouge, Louisiana*

**GOV**  **HACK**  **56,000**

The Louisiana Department of Health and Hospitals notified emergency medical technicians that a hacker may have had
access to their names, Social Security numbers and other personal information. The incident occurred on September 17
and a lack of funding for letters and postage caused a delay in notification.

*Information Source:*
Databreaches.net

---

October 28, 2010

**Individual Tax Preparer**

*Laurinburg, North Carolina*

**BSF**  **PHYS**  **Unknown**

Eight cabinets full of tax records were stolen from a residence. The records belonged to a deceased tax preparer
named Ester Gaino and go back to at least five years ago. It seems that the thief or thieves were looking for information
that could be used to commit identity theft.

*Information Source:*
Databreaches.net

---

October 28, 2010

**University of Connecticut Storrs**

*Storrs Mansfield, Connecticut*

**EDU**  **DISC**  **23**

Student information from a class held in 2000 was discovered online. A faculty member had saved a list of one-time
students in the class. The list exposed names and Social Security numbers and was removed from the Internet shortly
after the discovery on October 4.

*Information Source:*
Databreaches.net

---

October 27, 2010

**Mount Sinai School of Medicine**

*New York, New York*

**MED**  **STAT**  **1,500 (No reports of SSNs or financial information)**

A hard drive from the World Trade Center Medical Monitoring and Treatment Program at Mt. Sinai Hospital was lost or
taken from a computer in the Mental Health Center. The information included emails with protected health information,
patients’ names, and possibly treatment and contact information.

*Information Source:*
PHIPrivacy.net

---

October 27, 2010

**Houston Independent School District (HISD)**

*Houston, Texas*

**EDU**  **HACK**  **232,000 (30,000 employees)**

The HISD may have experienced a hacking incident over the weekend of October 24. Employees and students were
unable to access the Internet, online classes and email until late Tuesday afternoon. Payroll information of workers and
academic information of students may have been compromised along with other personal information.

**UPDATE** (12/2/10): HISD announced an overhaul of the computer system following the breach. Private employee, vendor
and student data dating back 10 years could have been accessed by the hacker. Investigators have determined that the
private data of one HISD student was viewed by the hacker. The investigation is ongoing.

*Information Source:*
Databreaches.net

---

October 22, 2010

**Johns Hopkins University**

*Baltimore, Maryland*

**MED**  **DISC**  **692**

Approximately 85 staff members received an email from the Applied Physics Laboratory on June 15. The email had an
attachment with personal benefits information of APL staff dependents. The information included names, Social Security
numbers, parent names, dates of birth, marital and disability status and medical and dental coverage. The emails were
deleted by the IT department and staff members were asked to reply that they had not made copies or disclosed the
information.

*Information Source:*
PHIPrivacy.net

---

October 21, 2010

**Keystone Mercy Health Plan and AmeriHealth Mercy Health Plan**

*Philadelphia, Pennsylvania*

**MED**  **PORT**  **808 (7 full SSNs)**

AmeriHealth Mercy Health Plan is located in Harrisburg, PA.
A flash drive with patient information was lost or stolen on or around September 20. Patient names, addresses, and personal health information were on the drive. Seven patients had their full Social Security numbers exposed and 801 had the last four digits of their Social Security numbers exposed. As of October 21, the two companies had released very little information about the breach.

**UPDATE** (1/29/11): The final total of patients affected appears to be 808 rather than 280,000.

<table>
<thead>
<tr>
<th>Information</th>
<th>Source: PHIPrivacy.net</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 21, 2010 LoneStar Audiology Group</td>
<td>585 (No SSNs or financial information reported)</td>
</tr>
<tr>
<td>Houston, Texas</td>
<td>MED PORT</td>
</tr>
</tbody>
</table>

The August 11 theft of a laptop resulted in the exposure of patient health information.

<table>
<thead>
<tr>
<th>Information</th>
<th>Source: HHS via PHIPrivacy.net</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 21, 2010 Norman Pediatric Associates and Norman Urology</td>
<td>MED PHYS Unknown</td>
</tr>
<tr>
<td>Norman, Oklahoma</td>
<td></td>
</tr>
</tbody>
</table>

Hundreds of intact medical records and Social Security numbers of oncology patients were found at the Norman Recycling Center. Both organizations believe a common paper shredding company is at fault. The files were returned to the organizations and affected patients will be contacted.

<table>
<thead>
<tr>
<th>Information</th>
<th>Source: PHIPrivacy.net</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 21, 2010 California Men's Colony (CMC)</td>
<td>MED PHYS 8</td>
</tr>
<tr>
<td>San Luis Obispo, California</td>
<td></td>
</tr>
</tbody>
</table>

An attorney mishandled the records of eight inmates who had been found guilty of murder. The names, criminal history, psychological evaluations, Social Security numbers and observations about their family relationships and behavior in prison were found in a public dumpster.

<table>
<thead>
<tr>
<th>Information</th>
<th>Source: PHIPrivacy.net</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 20, 2010 University of Arkansas for Medical Sciences</td>
<td>MED PORT Unknown</td>
</tr>
<tr>
<td>Little Rock, Arkansas</td>
<td></td>
</tr>
</tbody>
</table>

A digital camera used for recording newborn information was stolen from an employee at the hospital. The information included newborn photos, mother names and contact information, dates of birth, insurance status and medical record numbers. The photos are taken as a security measure in case an infant is abducted. Infants born at the hospital between July and October were affected.

<table>
<thead>
<tr>
<th>Information</th>
<th>Source: PHIPrivacy.net</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 19, 2010 Chen Financial, KC Realty, and SBC Financial</td>
<td>MED PORT Unknown</td>
</tr>
<tr>
<td>Westminster, California</td>
<td>BSF INSD</td>
</tr>
</tbody>
</table>

Kathy Chen and co-conspirators took advantage of real estate clients at Chen's three businesses. Chen primarily obtained personal data from unsuspecting borrowers who new immigrants or senior citizens. The personal and credit information was then used to obtain 47 fraudulent loans amounting to $17,500,000. Clients in Kern, Orange and San Bernardino counties were affected between 2005 and 2007. Chen was sentenced to 68 years in prison for identity theft, grand theft, forgery and conspiracy charges. Her two co-conspirators have not been arrested.

<table>
<thead>
<tr>
<th>Information</th>
<th>Source: Databreaches.net</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 19, 2010 Carolina West Wireless</td>
<td>BSO UNKN Unknown</td>
</tr>
<tr>
<td>Beaumont, Texas</td>
<td></td>
</tr>
</tbody>
</table>

The Carolina West Wireless headquarters is located in Wilkesboro, North Carolina.

Authorities found customer information in the car of two men. It is not known if the information was obtained through hacking, from an insider, by collecting documents from the company or by other methods.

<table>
<thead>
<tr>
<th>Information</th>
<th>Source: Databreaches.net</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 19, 2010 Carolina West Wireless</td>
<td></td>
</tr>
</tbody>
</table>
October 19, 2010  Cumberland Gastroenterology P.S.C.  
Somerset, Kentucky  

MED  PHYS  
2,207 (No SSNs or financial information reported)

Paper records were stolen on September 18. The records contained protected health information.

Information
Source: HHS via PHIPrivacy.net

October 19, 2010  WESTMED Medical Group  
Purchase, New York  

MED  PORT  
578 (No reports of SSNs or financial information)

A laptop with patient information was stolen in August.

Information
Source: HHS via PHIPrivacy.net

October 18, 2010  Jackson Hewitt  
Jacksonville, Florida  

BSF  PHYS  Unknown

Clients and employees of the Jackson Hewitt at the Southside office plaza were affected.

An employee discovered old customer and employee documents in the dumpster behind the office. The documents included employees’ W-2 forms, personal bank statements and some tax information from customers. The former owner admitted to being responsible and eventually had the documents shredded.

Information
Source: Databreaches.net

October 18, 2010  Milwaukee County  
Milwaukee, Wisconsin  

GOV  INSD  30

A temporary employee who was hired through the staffing agency Adecco was convicted of identity theft. Over thirty county employees had their identities stolen. The temporary employee began working in the human resources department in December of 2009.

Information
Source: Databreaches.net

October 17, 2010  New Mexico Tech Community College  
Socorro, New Mexico  

EDU  DISC  3,000

It appears that anyone with a Tech computer account could have accessed more than 3,000 Social Security numbers over the past four or five years. Copies of an accounting file were mistakenly stored in two public locations on the TCC server.

Information
Source: Databreaches.net

October 16, 2010  University of California Davis (UCD) Medical Center  
West Sacramento, California  

MED  PHYS  900

UCD patient documents were stolen from an UltraEx courier service in West Sacramento in August. The information consisted of copies of checks and remittance records between the University and insurance companies. Six patients had their full Social Security numbers exposed and 40 patients had some part of their Social Security number exposed. The University now prohibits the courier service from storing documents overnight.

Information
Source: PHIPrivacy.net

October 15, 2010  University of North Florida  
Jacksonville, Florida  

EDU  HACK  106,884 (52,853 SSNs reported)

A hacker from outside of the country may have accessed applicant information sometime between September 24 and September 29. The information was mostly recruiting information and may have involved names, ACT and SAT scores, dates of birth and Social Security numbers.

Information
Source: Databreaches.net
Three women have been charged for their roles in defrauding clients of a Citibank in Florence, KY. At least two of the women were employees of Citibanks in other states. One woman stole customer credit card account numbers and changed their addresses, while another used the information to make purchases in another state. The third woman assisted in collecting the purchased goods. The fraud began at the end of 2006 and two of the women were arrested in March of 2007.

Information Source: Databreaches.net

Some veteran benefit information was mailed to the wrong addresses on August 25. Of the 6,299 letters sent to incorrect addresses, 3,913 had full Social Security numbers and 2,386 had Veterans Benefits Administration claim numbers. A program error caused some of the letters to be mailed to the incorrect addresses.

Information Source: Databreaches.net

The theft occurred in Las Vegas, NV and affects residents of Accomack County. Citizens are advised to call one of the three credit bureaus at 888-397-3742, 888-766-0008 or 800-680-7289 for a credit report fraud alert.

A stolen laptop contained the names and Social Security numbers of Accomack County, Virginia residents. Full addresses of some residents were also exposed. The laptop was county property and was stolen from an employee’s car during a vacation to Las Vegas. The incident happened on October 7; as of October 14, residents had not been notified.

Information Source: Databreaches.net

A person or persons broke into the building during the weekend of October 10. Personal information of clients may have been viewed or recorded, but does not appear to have been stolen. Police believe their suspect entered the building to retrieve a car title document.

Information Source: Databreaches.net

A bank employee used customer credit card information to open fraudulent loans in their names. The deceased and elderly were targeted. The employee has not yet been arrested and appears to have been using the money to pay for the legal defense of her son.

Information Source: Databreaches.net

Call 1-888-865-5940 for more information about this incident.

A back-up tape created for the purpose of disaster recovery testing and training was lost during shipping to the California Department of Developmental Services by UPS. Consumers’ first and last names, Social Security numbers, contact, diagnostic and medical information may have been exposed. Extracting information from the tape requires sophisticated technology, according to the breach notice letter.

Information Source:
A portable point of care device was stolen from an employee. Client names, addresses, Social Security numbers, medical record numbers, diagnoses and treatment information were on the unencrypted device.

Information Source: PHIPrivacy.net

A laptop containing client information was stolen from an employee’s car on May 3. Client names, addresses, Social Security numbers and diagnoses may have been exposed. The incident was reported on May 10.

Information Source: PHIPrivacy.net

An isolated administration error caused an encrypted file with the personnel information of one client’s employees to be made available to the HR department of another client. A password-based registration system was already in place to prevent the wrong addressee from opening encrypted email, however, the email was addressed to the wrong client. The total number of employees who may have had their names and Social Security numbers exposed is unknown, but 473 residents of Maryland were notified of the incident. On June 3, the other HR department notified ING that they had been sent the wrong information.

Information Source: Databreaches.net

An June theft at the facility exposed employee information. Employee names, Social Security numbers and some employee fingerprints were on the stolen equipment. It is unknown how many people were affected, but 284 Maryland residents were notified.

Information Source: Databreaches.net

A dishonest Florida State Farm agent was caught selling customer information to a third party. The former employee was terminated and arrested. The agent’s buyer and purpose for wanting the information was not reported.

Information Source: Databreaches.net

The March 16 theft of office computers may have exposed policyholder information. Names, addresses, Social Security numbers, telephone numbers and driver’s license numbers were on the computers. Clients were notified on July 26.

Information Source: Databreaches.net

Paper records were improperly disposed of on July 29. The incident affected 2,123 patients.

Information Source: HHS via
October 11, 2010  University of Oklahoma-Tulsa Neurology Clinic, Neurology Services of Oklahoma, LLC
Oklahoma City, Oklahoma

Neurology Services of Oklahoma, LLC is located in Tulsa, OK.

Malware was discovered on a clinic computer on or around July 28. Patients who saw Dr. John Cattaneo at the clinic and at his former employer Neurology, LLC were notified of the breach. Patient names, Social Security numbers, phone numbers, addresses, dates of birth, medical record numbers, lab reports and dates of service were in documents that may have been accessed by the virus.

Information
Source: PHIPrivacy.net

Records from this breach used in our total: 19,264

October 11, 2010  Private Counseling and Psychotherapy Practice
Bronx, New York

The September 6 theft of a desktop computer resulted in the exposure of patient information.

Information
Source: HHS via PHIPrivacy.net

Records from this breach used in our total: 0

October 11, 2010  Alliance HealthCare Services, Inc.
Newport Beach, California

Patients from Oroville hospital in Oroville, CA and Eden Medical Center in Castro Valley, CA were affected.

One or more portable devices were lost or stolen between July 31 and August 5.

Information
Source: HHS via PHIPrivacy.net

Records from this breach used in our total: 0

October 11, 2010  UnitedHealth Group
Minneapolis, Minnesota

A breach involving UnitedHealth Group and its business associate CareCore National was posted on the Health and Human Services (HHS) website. Unauthorized persons were able to access paper records on or around July 8.

Information
Source: HHS via PHIPrivacy.net

Records from this breach used in our total: 0

October 11, 2010  Private Medical Practice
Wichita, Kansas

Paper records and at least one laptop with patient information were stolen during an August 20 theft.

Information
Source: HHS via PHIPrivacy.net

Records from this breach used in our total: 0

October 11, 2010  St. James Hospital and Health Centers
Chicago, Illinois

The improper disposal of paper documents may have left the health information of patients of Saint James Hospital and Health Centers exposed. The incident occurred on or around August 10.

Information
Source: HHS via PHIPrivacy.net

Records from this breach used in our total: 0
A desktop computer was stolen on or around August 17.

Information
Source: HHS via PHIPrivacy.net

October 8, 2010 Mississippi National Guard
Jackson, Mississippi

It was discovered that personnel records had been posted online for several weeks. Administrative information collected from the 155th Brigade Combat Team between 2006 and 2008 was accessible online. Names, Social Security numbers, rank, pay grade, dates of birth and phone numbers were exposed.

Information
Source: Databreaches.net

October 8, 2010 AmeriCorps
Washington, District Of Columbia

A website flaw dating back to 2006 may have allowed people to view applicant and participant personal information. Individuals who manipulated the website URL and guessed or knew user log-in names could have accessed participant and applicant contact information, names, and partial or full Social Security numbers.

Information
Source: Databreaches.net

October 6, 2010 Gastroenterology Consultants
Omaha, Nebraska

A local news station responded to a report about patient files being left in a recycling dumpster outside of the clinic. Hundreds of documents with patient names, Social Security numbers, addresses and detailed medical information were found and secured by KMTV Action 3 News. The files appear to be from 2002 and 2003.

Information
Source: PHIPrivacy.net

October 4, 2010 Gulf Pines Hospital
Port St. Joe, Florida

Former employees are concerned that the hospital was not properly cleared before being sold. People reported abandoned files in the middle of the hospital. An emergency room log, driver’s license information, Social Security numbers and other personal files were left in the hospital. Patient medical records were removed. The buyer of the property was contacted, but did not return phone calls.

Information
Source: PHIPrivacy.net

October 2, 2010 Romeus Cuban Restaurant
Southwest Ranches, Florida

More than two dozen customers had their credit card numbers stolen by a waiter with a skimming device. Authorities believe the former waiter collected information over several months and sold it to a group of identity thieves operating outside of Florida.

Information
Source: Databreaches.net

October 2, 2010 Has-Camino Travel Agency
South Pasadena, California

A former employee and her husband were arrested on suspicion of stealing computers from her former employer. The computers contained the personal information of clients and were stolen during an office burglary.

Information
Source: Databreaches.net

October 1, 2010 Central Florida Regional Transportation Authority, LYNX
Orlando, Florida

A former bus driver pleaded guilty to stealing the identities of some of her disabled passengers. The driver pleaded guilty to 27 counts of wire fraud, aggravated identity theft and trafficking in a counterfeit device. The information was
stolen between October and November of 2009 and used to open fraudulent credit accounts.

**UPDATE (12/16/10):** The former bus driver was sentenced to three and a half years in prison and ordered to pay $3,667 in restitution.

**Information**
Source: Databreaches.net

**September 29, 2010**  
**Morgan Keegan & Company**  
**Memphis, Tennessee**  
**BSF**  
**PORT**  
**18,500**

An attorney was able to collect a disk with client names and detailed financial information during an investigation. Clients were notified and their accounts are being monitored for unauthorized use. The breach was discovered on September 15 and the disk was later returned by the attorney.

**Information**
Source: Media

**September 29, 2010**  
**University of Florida**  
**Gainesville, Florida**  
**EDU**  
**DISC**  
**239**

People who believe they may have been affected may read the information provided on the University's privacy website at [http://privacy.ufl.edu/](http://privacy.ufl.edu/). The University also has a toll-free privacy line 1-866-876-HIPA.

The University notified former students who took certain computer science classes in 2003 that their information was available online. Names, Social Security numbers and addresses were included in a web-accessible archive created by a faculty member. The University corrected the problem in August of 2010. Notification letters were sent to most students who may have been affected, but the University was unable to contact 54 former students.

**Information**
Source: Databreaches.net

**September 29, 2010**  
**Cheesecake Factory, PGA Tour Grill, Outback Steakhouse**  
**Washington, District Of Columbia**  
**BSR**  
**INSD**  
**Unknown**

Two people have been charged with conspiring to commit bank fraud and aggravated identity theft. They paid servers at multiple restaurants in the Washington D.C. area to use skimming devices to collect customer credit card information. The stolen information was used to fraudulently make purchases.

**Information**
Source: Databreaches.net

**September 28, 2010**  
**Maine Department of Education**  
**Augusta, Maine**  
**EDU**  
**DISC**  
**Unknown**

A technology director from the school district was able to access Social Security numbers of staff members in other districts. The Maine Department of Education has asked school districts to delay submitting student Social Security numbers until the problem has been addressed. According to reports, "For the first time, Maine school districts are collecting students’ SSNs for a statewide database intended to help policy makers track students’ progress throughout school and college and into the workplace." This practice has been controversial.

**Information**
Source: Databreaches.net

**September 28, 2010**  
**US Bank**  
**Eau Claire, Wisconsin**  
**BSF**  
**CARD**  
**Unknown**

A scanner was found at an ATM. It was left undetected between 12:30pm and 4:20pm on Friday, September 17. A customer reported the device the next day when it was placed at the same location again. It appears that one customer was directly affected by unauthorized charges. The bank is in the process of canceling cards that were used on September 17 and 18 of 2010.

**Information**
Source: Databreaches.net

**September 27, 2010**  
**Kern Medical Center**  
**Bakersfield, California**  
**MED**  
**HACK**  
**Unknown**

An employee opened an email that subsequently affected the entire hospital system in late July. The Kern Medical Center temporarily removed itself from the county computer network to prevent the spread of the attack. Patient records were eventually secured, but it is unknown if any were affected by the 16-day malware attack.

**Information**
Source: PHIPrivacy.net

**September 27, 2010**  
**Columbia University Medical Center**  
**MED**  
**DISC**  
**6,800 (10 SSNs)**
Those with questions may call 1-866-523-6760.

Patients treated in the Intensive Care Unit at New York-Presbyterian Hospital and Columbia University Medical Center may have had their information accessed on the Internet during July. The personal information may have included name, age, surgical status, medications and lab results. It appears that a hospital employee's computer files were Internet accessible.

**UPDATE** (5/17/2014): "Two health care organizations have agreed to settle charges that they potentially violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules by failing to secure thousands of patients' electronic protected health information (ePHI) held on their network. The monetary payments of $4,800,000 include the largest HIPAA settlement to date".

**Information**

**Source:** PHIPrivacy.net

- **September 25, 2010**
  - **St. Vincent Hospital (Saint Vincent)**
  - **Indianapolis, Indiana**
  - **MED PORT**
  - **1,200**

Patients who received notification letters and have questions may call CSIdentity at (800)-805-7004.

A computer was stolen from an employee's home on July 25. The computer had patient Social Security numbers and other personal health information. Patients were notified in late September.

**Information**

**Source:** PHIPrivacy.net

- **September 24, 2010**
  - **Wilderness Ridge, Hidden Valley Golf**
  - **Lincoln, Nebraska**
  - **BSR HACK**
  - **225**

At least 225 reports of credit and debit card fraud have been linked to a security breach that exposed the information of customers of the two golf courses. The affected systems were shutdown. The time of the security breach is unknown.

**Information**

**Source:** Databreaches.net

- **September 24, 2010**
  - **Comprehensive Accounting**
  - **Farmington Hills, Michigan**
  - **BSF PHYS**
  - **Unknown**

An employee error reportedly caused thousands of intact client files to be left in an easily accessible dumpster. The files contained client information and employee Social Security numbers, names, addresses, W2s, bank statements and profit reports from 1990 and after. The files were removed from the dumpster and are scheduled to be shredded.

**Information**

**Source:** Databreaches.net

- **September 23, 2010**
  - **Alaskan AIDS Assistance Association (Four A's)**
  - **Anchorage, Alaska**
  - **NGO PORT**
  - **2,000 (Unknown number of SSNs reported)**

The Four A's is a business associate of the State of Alaska Department of Health and Human Services.

A data storage device containing client names and contact information was stolen from Four A's executive director's car. Some clients had their Social Security numbers on the device.

**Information**

**Source:** PHIPrivacy.net

- **September 22, 2010**
  - **Ault Chiropractic Center**
  - **Batesville, Indiana**
  - **MED STAT**
  - **2,000 (No SSNs or financial information reported)**

The September 15 theft of a computer may have resulted in the exposure of the protected health information of patients.

**Information**

**Source:** HHS via PHIPrivacy.net

- **September 22, 2010**
  - **Hana Japanese Sushi Bar and Grill**
  - **Natchitoches, Louisiana**
  - **BSR HACK**
  - **30**
Over 30 cases of credit card fraud were linked to the restaurant. The computer server is believed to have been hacked in February of 2010. It appears that the $50,000 in fraudulent credit charges originated from a hacker in Romania.

**Information**
**Source:** Databreaches.net

**September 22, 2010**
**Private Legal Practice**
Hudson, New Hampshire

Mr. LaRocque's home was burglarized on the evening of July 25, 2010. A laptop with names, Social Security numbers, tax identification numbers and other personal information from his family law clients was stolen.

**Information**
**Source:** Databreaches.net

**September 22, 2010**
**The Kent Center**
Warwick, Rhode Island

A briefcase with patient records was stolen from a clinician's car on July 13. The lost documents included client names, dates of birth and some clinical information. The patient records do not appear to have been the target of the theft since other cars were broken into during that night.

**Information**
**Source:** HHS via PHIPrivacy.net

**September 22, 2010**
**Private Medical Practice**
Chesapeake, Virginia

The doctor’s patients in Norfolk, Portsmouth, Virginia Beach and Chesapeake may have been affected.

A laptop was stolen from a doctor’s office on July 12. It is unknown if patient files were accessible on the laptop. The files would have contained names, dates of birth, diagnoses, treatments, and other personal information.

**Information**
**Source:** HHS via PHIPrivacy.net

**September 22, 2010**
**Pediatric and Adult Allergy, PC**
Des Moines, Iowa

Patients of Dr. George Caudill (retired), Dr. Veljko Zivkovich (retired) Dr. Robert Colman and Dr. Whitney Molis were notified that a backup tape with their personal information was lost on or around July 11. The patient information included name, address, phone number, date of birth, Social Security number, dates of service, services and diagnoses. Medical records and financial information were not on the backup tape. It appears that all patients with accounts created before July 10, 2010 were affected.

**Information**
**Source:** HHS via PHIPrivacy.net

**September 20, 2010**
**Julie’s Place**
Tallahassee, Florida

Around a hundred people reported fraudulent charges to their financial accounts after making purchases at the restaurant. A hacker exploited knowledge of vulnerabilities in the Aloha POS software used by the restaurant and obtained customer information. The restaurant changed and upgraded their computer system.

**Information**
**Source:** Databreaches.net

**September 19, 2010**
**Albrecht Discount (ALDI)**
Chicago, Illinois

Several ATMs inside or near grocery stores in the Chicago area were outfitted with skimming devices. ALDI checked machines nationwide and removed a number of debit card terminals after discovering the problem.

**UPDATE** (10/1/10): A notice on the ALDI Inc. website reveals that customers in Hartford, Atlanta, Chicago, Indianapolis, Maryland, New Jersey, New York state, North Carolina, Pennsylvania, Charlotte (South Carolina), and Washington D.C. were affected by the breach. The terminals were in stores between June 1 and August 31 of 2010.
UPDATE (12/2/10): Eight thousand Maryland residents and 17,000 New York residents were affected.

Information
Source: Databreaches.net

September 18, 2010
University of Pittsburgh Medical Center Shadyside Hospital
Pittsburgh, Pennsylvania

MED INSD 19

In February of 2008, an employee disclosed the names, dates of birth and Social Security numbers of patients in exchange for personal gains. The patient information was eventually used to file false tax returns. The former employee was indicted on 14 counts.

UPDATE (7/05/2011): A former employee has pleaded guilty to taking the names, Social Security numbers and dates of birth of 19 Shadyside patients. The employee gave the patient information to other people who then filed fraudulent 2008 tax returns.

UPDATE (10/21/2011): The former employee was sentenced to one year of probation for disclosing the information of 19 UPMC patients. He claims he was intimidated into giving away the information and that the people who collected $84,190 in fraudulent tax returns returned to Zambia.

Information
Source: PHIPrivacy.net

September 18, 2010
New York City Human Resources Administration and New York City Department of Health and Mental Hygiene
New York, New York

GOV INSD Unknown

Two New York City employees from different agencies were involved in an identity fraud ring. One employee worked for the New York City Human Resources Administration and sold copies of welfare recipients’ birth certificates and Social Security numbers. The second employee worked for the New York City Department of Health and Mental Hygiene and sold parental identification information from birth certificates. The employees were sentenced to eight months to two years of prison time and one to two years of probation for identification fraud. These crimes happened between 2005 and 2008.

Information
Source: Databreaches.net

September 16, 2010
Saint Anselm College
Manchester, New Hampshire

EDU DISC Unknown

A number of alumni who received a University newsletter were notified that their Social Security numbers were printed on mailing labels. The error occurred on the spring 2010 and fall 2009 newsletters. It seems that no one complained about the fall accidental disclosure.

Information
Source: Databreaches.net

September 16, 2010
Martin Luther King Jr. Multi-Service Ambulatory Care Center
Los Angeles, California

GOV INSD 33,000 (No reports of SSNs or financial information)

A janitor removed 14 boxes of patient records and sold them to a recycling center. The records had names, genders, dates of birth, addresses, medical record numbers and financial batch numbers. Patients who received services from the outpatient facility between January and October of 2008 were affected. The files were discovered missing on July 29 of 2010 and the custodial worker admitted to selling them. The custodian is being charged with one count of felony commercial burglary. Those affected will be mailed notifications during the week of September 20 of 2010.

Information
Source: Databreaches.net

September 16, 2010
Benefit Concepts Inc
East Providence, Rhode Island

BSF PORT Unknown

A package containing payroll checks and a CD copy of payroll checks was lost during shipment between July 19 and July 20. Benefit Concepts’ vendor CompuPay will encrypt CDs and mask paper records in the future, but this CD was not encrypted. Employee names, Social Security numbers and bank account numbers were in the package.

Information
Source: Databreaches.net

September 16, 2010
SanDiegoFit.com
San Diego, California

BSR STAT Unknown

On August 30, a computer with customer information was stolen from the building. The password-protected computer had customer names, addresses, phone numbers and credit card numbers.
September 16, 2010  Cardinal Health  
Dublin, Ohio  
MED PORT Unknown

After an investigation into the status of decommissioned computers, it was determined that the locations of 11 were unknown. One laptop contained HR data. Current and former employee identification numbers, Social Security numbers and dates of birth may have been exposed. The investigation began in June when an employee was caught selling a laptop with sensitive information on eBay. Cardinal gave notice of the breach on September 7.

September 15, 2010  Paul Martin's American Bistro  
Roseville, California  
BSR HACK Unknown

Hundreds of customers who used their credit cards at Paul Martin's were put at risk for credit card fraud. Hackers accessed the restaurant’s credit-card processing system. Customer credit card information was then sold to other criminals and used to make purchases. According to a police news release, the hack did not involve the external financial services network or any third-party data processing service. It appears that the first customers were affected in March of 2010.

September 14, 2010  Rice University  
Houston, Texas  
EDU PORT 7,250 (4,003 Social Security numbers)

A portable device with personal information of current and former employees and some students was stolen. The device had a payroll file which contained the information of students, faculty, and staff on payroll as of January 2010. Social Security numbers, addresses, names, dates of birth and other employment information may have been exposed.

UPDATE (9/18/10): Additionally details reveal that the information was not encrypted. Approximately 2,270 students were affected. Four thousand of the Social Security numbers on the device were from faculty or staff, while three were from students. The banking information of two employees was also on the device.

September 13, 2010  Saint Barnabas Health Care Systems and Newark Beth Israel Medical Center  
West Orange, New Jersey  
MED PORT 4,586 (No SSNs or financial information reported)

KPMG LLP is the accounting firm responsible for the loss of the flash drive.

An employee of Saint Barnabas’ accounting partner KPMG lost an unencrypted flash drive. The flash drive had patient names and information about their health, but did not have Social Security numbers or financial information. The incident occurred in June and patients were notified in September.

September 13, 2010  SunBridge Healthcare Corporation  
Albuquerque, New Mexico  
MED PORT 1,000 (No SSNs or financial information reported)

A BlackBerry mobile device was stolen from an employee’s desk. The device had unencrypted current and former resident and patient information from eight different nursing and rehabilitation facilities in Georgia. No Social Security numbers
or financial information were stored on the device, but it did contain patient names, medical record numbers, medical information, dates of birth, and dates of service.

Information
Source: HHS via PHIPrivacy.net

September 13, 2010
New York University School of Medicine Aging and Dementia Clinical Research Center
New York, New York
MED PORT 1,200 (No reports of SSNs or financial information)

A portable electronic device was lost or stolen on April 3. The health information of 1,200 patients was lost. The incident was reported to the Department of Health and Human Services in September.

Information
Source: HHS via PHIPrivacy.net

September 13, 2010
City of Shreveport
Shreveport, Louisiana
GOV PHYS Unknown

Personal city government documents were easily accessible during a public auction. Buyers looking for city furniture were able to search through city payroll information, law enforcement reports and a variety of other documents which contained people’s names, contact information and Social Security numbers. City employees admit the exposure was a mistake and removed the documents within an hour of notification. It is believed that the documents escaped from a stack that was scheduled to be burned.

Information
Source: Databreaches.net

September 13, 2010
Florida Department of Children and Families, Department of Juvenile Justice
Tallahassee, Florida
GOV INSD 550

Seven people worked together to collect 880 fraudulent tax refunds between 2006 and 2008. It is believed that people served through the Florida Department of Children and Families and people connected to the Department of Juvenile Justice were affected. The conspirators somehow gained access to names, Social Security numbers and other information on the state databases.

UPDATE (9/15/2011): The source of the breach was found to be two dishonest employees. On October 28, 2010 a call center supervisor was fired for negotiating to sell the Medicare numbers of disabled and elderly Floridians to an informant. A second Department of Children and Families (DCF) employee was also caught selling sensitive information. Each employee repeatedly misused access to a DCF computer system to obtain the information of people who applied to DCF for food stamps, cash benefits, and Medicaid. One dishonest employee was sentenced to 36 months in prison and three years of supervised release on June 30, 2011. The other is scheduled to be sentenced on November 21, 2011 and faces a maximum of ten years in prison for health care fraud charges, five years for authentication feature fraud, and two years for each aggravated identity theft charge.

Information
Source: Databreaches.net

September 11, 2010
Cheesecake Factory
White Plains, New York
BSR INSD Unknown

A waiter used a skimming device to make $100,000 worth of fraudulent charges to customer credit cards. The waiter committed these crimes in late 2008 and was arrested in September of 2010.

Information
Source: Databreaches.net

September 11, 2010
Corona-Norco Unified School District
Norco, California
EDU DISC 82

An information privacy watchdog notified administrators that teacher and administrator personal information was available online. Most of the information was immediately removed, but a Google document with Social Security numbers was not removed. It is unknown how long the information was online, but it was discovered on August 31.

Information
Source: Dataloss DB

September 9, 2010
Mayo Clinic
Phoenix, Arizona
MED INSD 1,700 (No reports of SSNs or financial information)
Those who received notification and have further questions may call 1-877-309-9839. Locations include New England, Florida, Minnesota and Arizona.

An employee was fired after it was learned that the employee accessed patient records without authorization. The employee repeatedly accessed information at a location in Arizona between 2006 and 2010, but the Mayo Clinic system allows employees to access patient records from across the country.

Information
Source: PHIPrivacy.net

September 9, 2010
Lucile Packard Children's Hospital at Stanford University
Palo Alto, California
MED STAT 532

http://hfcis.cdph.ca.gov/LongTermCare/details/stateEnforcementAction.aspx?fac=070001349

A former employee took a hospital desktop computer with patient records home around January 11 of 2010. In February it was determined that the computer could not be recovered and patients were notified of the incident. The hospital was fined $250,000 by the California Department of Public Health for the delay in reporting the incident. As of September 9 2010, the hospital was in the process of appealing the fine.

UPDATE (9/10/10): The desktop did contain patient Social Security numbers, medical record numbers, names, insurance information, diagnoses and treatment information.

Information
Source: PHIPrivacy.net

September 9, 2010
California Department of Health Care Services
Sacramento, California
GOV DISC 5,000 (No reports of SSNs or financial information)

The California Department of Health Care Services released confidential and identifying information about HIV positive Medi-Cal recipients to a third party service provider. A network of organizations have deemed this action illegal and unauthorized. A letter was sent by the network asking for an explanation of how this happened and reassurance that it will not happen again.

Information
Source: PHIPrivacy.net

September 8, 2010
HEI Hospitality (HEI Hotels and Resorts)
Norwalk, Connecticut
BSR HACK 3,400

A vulnerability was discovered in the information systems of multiple hotels. Customers who used credit cards between March 25 and April 17 of 2010 may have had their credit card information exposed.

Information
Source: Databreaches.net

September 8, 2010
SeaChange International
Anton, Massachusetts
BSR INSD Unknown

A temporary administrative assistant admitted to stealing the identity of one employee in July. It is unclear how many employees had their information accessed by the temp, but SeaChange sent notification of the incident to employees in 26 states shortly after discovering the breach.

Information
Source: Databreaches.net

September 7, 2010
City University of New York
New York, New York
EDU PORT 7,000

Those with questions may call (212) 650-5426.

A computer with student information was stolen. The information included Social Security numbers and names.

Information
Source: Dataloss DB

September 6, 2010
Humana
Louisville, Kentucky
MED INSD 4 (No SSNs or financial information reported)

A former employee pleaded guilty to illegally accessing and using patient information in order to support his drug habit. The employee worked in Humana's information technology department. He also agreed to help address internal security
flaws.

Information Source: PHIPrivacy.net

September 5, 2010  Eastern Michigan University
Ypsilanti, Michigan  EDU  HACK   Unknown

Online banking information may have been exposed because of a computer server hacking incident. The information included log-ins and personal identification numbers for some employees.

Information Source: Dataloss DB

September 4, 2010  Essex Youth Commision Summer Program
Essex, Massachusetts  GOV  PHYS   Unknown

Paper records and digital files with personal health and personally identifiable information from youth participants, parents and staff were reported missing.

Information Source: PHIPrivacy.net

September 3, 2010  University of Rochester Medical Center (URMC)
Rochester, New York  MED  PORT   837 (0 reports of SSNs or financial information)

The loss of a USB device may have exposed current and former patient health information and dates of birth. Patients of a single surgeon were affected.

Information Source: PHIPrivacy.net

September 2, 2010  Chattanooga Family Practice Associates
Chattanooga, Tennessee  MED  PORT   1,711 (No SSNs or financial information reported)

A missing portable device had the names, dates of birth and purposes of visits for a limited number of patients.

Information Source: HHS via PHIPrivacy.net

September 2, 2010  Kinetic Concepts Inc. (KCI)
San Antonio, Texas  BSR  DISC   4,000

An attachment with sensitive employee information was accidentally emailed to company employees. The information included names, Social Security numbers, addresses, dates of birth and salary information.

Information Source: Dataloss DB

September 2, 2010  Arkansas State University
Jonesboro, Arkansas  EDU  DISC   2,484

The full names, driver's license numbers and Social Security numbers of 2,484 full and part-time employees of the University were accidentally emailed to 144 University emails.

Information Source: Databreaches.net

September 2, 2010  Sprint  Overland Park, Kansas  BSR  INSD  Unknown

The location listed is Sprint Nextel's headquarters. The former employees worked in New York, New Jersey and Florida.

Between January 2010 and June 2010 nine former employees inappropriately accessed confidential customer account information and used it to make unauthorized calls. Defrauded customers were credited by the company. Around $15 million dollars in authorized calls resulted from the cellphone cloning scheme.
Social Security numbers were printed on the outside of envelopes mailed to beneficiaries of the pension fund. It is unclear how many of the 24,000 members had their information mailed before the error was discovered.

Information Source: Databreaches.net

September 1, 2010 Jason’s Deli Memphis, Tennessee BSR HACK Unknown

Hundreds of customers may have been affected after using their credit or debit cards at the restaurant. The computer server was infected with a new virus.

Information Source: Databreaches.net

August 31, 2010 P.K. Yonge Gainesville, Florida EDU PORT 8,300

The July 23 theft of a laptop in California resulted in the exposure of current and former student and employee personal information. The information included Social Security numbers and some driver’s license numbers. The information dates back to 2000.

Information Source: Databreaches.net

August 31, 2010 Armed Forces Recruiting Center Cape Girardeau, Missouri GOV PHYS Unknown (8 SSNs reported)

Dozens of records with high school diplomas were found in a dumpster outside of the recruiting center on William Street. In eight cases, copies of people’s birth certificates, Social Security cards, or both were also with their diplomas.

Information Source: Media

August 30, 2010 Aon Consulting Chicago, Illinois BSF DISC 22,000

The Social Security numbers, genders and dates of birth of retirees in Delaware were accidentally posted online for four days as part of a Request for Proposal for the State of Delaware. Names were not included.

UPDATE (9/2/10): A woman affected by Aon’s failure to remove personal information from the request has filed a class action lawsuit against Aon Consulting.

Information Source: Dataloss DB

August 29, 2010 Rolling Meadows Townhomes Saline, Michigan BSO HACK Unknown

Dozens of residents of the Rolling Meadows Townhomes community became identity theft victims. Thieves somehow obtained banking information from checks that residents sent to pay for their co-op properties.

Information Source: Databreaches.net

August 26, 2010 HMS Host Cleveland, Ohio BSR INSD Unknown

This appears to affect people seeking employment with the Starbucks in Cleveland Hopkins International Airport prior to 2009.

A woman was charged with misusing applicant information to open more than 65 credit cards under different names. The woman made over $115,000 in fraudulent charges between February of 2006 and November of 2008.

Information Source: Databreaches.net

August 24, 2010 Eastmoreland Surgical Clinic and Vein Center Portland, Oregon MED STAT 4,328

Desktop computers were stolen from the office around July 5. The computers had patient names, addresses, Social Security numbers.
Desktop computers were stolen from the office around July 5. The computers had patient names, addresses, Social Security numbers, phone numbers, reason for visit and insurance carrier information.

**Information**
**Source:** PHIPrivacy.net  
**records from this breach used in our total:** 4,328

**August 24, 2010**  
**Mahaska County Hospital**  
**Oskaloosa, Iowa**  
MED INSID Unknown

Two patient-orders coordinators were fired for separate incidents of snooping. One inappropriately accessed at least two patients' data. The other employee inappropriately accessed the data of multiple family members.

**Information**
**Source:** PHIPrivacy.net  
**records from this breach used in our total:** 0

**August 24, 2010**  
**Oak Ridge National Laboratory**  
**Columbus, Ohio**  
GOV STAT Unknown

About 1,500 unused hard drives were mismanaged, abandoned, and unsecured in the offices. The hard drives had sensitive information such as names, medical information, dates of birth and salary information. Auditors found hard drives in hallways, unused offices and docks. Only 55 unused hard drives were being stored properly; computer security officers destroyed the others.

**Information**
**Source:** Databreaches.net  
**records from this breach used in our total:** 0

**August 24, 2010**  
**Riverview Gardens School District**  
**St. Louis, Missouri**  
EDU PHYS Unknown

Hundreds of documents with student Social Security numbers, pictures, phone numbers and ages were left near a dumpster.

**Information**
**Source:** Databreaches.net  
**records from this breach used in our total:** 0

**August 23, 2010**  
**Wachovia Bank**  
**Atlanta, Georgia**  
BSF INSID Unknown

A former employee was sentenced to prison after being convicted of identity theft and bank fraud. While working at Wachovia’s bank fraud detection department in 2007, the employee sold credit card and bank account numbers to an outside accomplice. The former employee was ordered to pay $91,104 in restitution and serve a four and a half years federal prison sentence.

**Information**
**Source:** Databreaches.net  
**records from this breach used in our total:** 0

**August 20, 2010**  
**Cook County Health and Hospital Systems (CCHHS)**  
**Chicago, Illinois**  
GOV PORT 7,000

On June 1, a laptop with patient information was stolen from a locked office in an administration building. The password protected-computer included names, dates of birth and Social Security numbers.

**Information**
**Source:** PHIPrivacy.net  
**records from this breach used in our total:** 7,000

**August 20, 2010**  
**University of Kentucky Newborn Screening Program**  
**Lexington, Kentucky**  
EDU PORT 2,027

A laptop with information from the Department of Pediatrics Newborn Screening Program was stolen from a locked private office. Patient dates of birth, names and medical record numbers were on the password-protected laptop. Some patients also had Social Security numbers on the laptop.

**Information**
**Source:** PHIPrivacy.net  
**records from this breach used in our total:** 2,027

**August 20, 2010**  
**Turley’s Restaurant**  
**Boulder, Colorado**  
BSR PHYS Unknown

The owner of Turley’s Restaurant went to recycle old employee files. After seeing that the dumpster was full, the owner then left boxes of intact files from former employees near the dumpster. The files included Social Security numbers, birth dates and phone numbers.

**Information**
**Source:** NAID  
**records from this breach used in our total:** 0

**August 19, 2010**  
**Yale School of Medicine**  
MED PORT 1,000

496
<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Type</th>
<th>Affected Individuals</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 19, 2010</td>
<td>New Haven, Connecticut</td>
<td>MED</td>
<td>1,000</td>
</tr>
<tr>
<td>August 19, 2010</td>
<td>University of Connecticut West Hartford, Connecticut</td>
<td>EDU</td>
<td>10,174</td>
</tr>
<tr>
<td>August 18, 2010</td>
<td>Baton Rouge Police Department Baton Rouge, Louisiana</td>
<td>GOV</td>
<td>30</td>
</tr>
<tr>
<td>August 18, 2010</td>
<td>Beauty Dental, Inc. Chicago, Illinois</td>
<td>MED</td>
<td>657</td>
</tr>
<tr>
<td>August 18, 2010</td>
<td>Humana Inc, Matrix Imaging Louisville, Kentucky</td>
<td>BSF</td>
<td>2,631</td>
</tr>
<tr>
<td>August 18, 2010</td>
<td>Payday Loan Stores of Illinois, PLS Financial Chicago, Illinois</td>
<td>BSF</td>
<td>369</td>
</tr>
<tr>
<td>August 18, 2010</td>
<td>Wright State Physicians Dayton, Ohio</td>
<td>MED</td>
<td>1,309</td>
</tr>
</tbody>
</table>

Affected individuals who received a notification letter may contact 877-751-3361.

A stolen laptop resulted in the exposure of patient clinical health information.

Information Source: PHIPrivacy.net  
records from this breach used in our total: 1,000

The August 3 office theft of a laptop resulted in the exposure of 10,174 applicants’ names, contact information and Social Security numbers. Undergraduate application information from 2004 to July of 2010 could have been accessed through the laptop.

Information Source: Databreaches.net  
records from this breach used in our total: 10,174

A man pled guilty to using a printout with the information of around 30 current and retired Baton Rouge officers to commit credit fraud. An insider sold him the computer printout.

UPDATE (2/18/11): The man was sentenced to seven years in prison. He did not reveal the name of the person who sold him the printout.

Information Source: Databreaches.net  
records from this breach used in our total: 30

The paper records of some individuals were lost or stolen on June 5.

Information Source: HHS via PHIPrivacy.net  
records from this breach used in our total: 0

The location is listed as Humana’s headquarters.

Paper records involving information from business associate Matrix Imaging were lost or stolen on June 25.

Information Source: HHS via PHIPrivacy.net  
records from this breach used in our total: 0

Payday Loan Stores (PLS) was fined $1,107,000 for failing to protect consumer information. In April of 2010, three boxes of documents were found by police at a dumpster near a Payday Loan Store. According to the Illinois Department of Financial and Professional Regulation, "the discarded documents contained personal customer information, including Social Security numbers and copies of driver’s licenses."

UPDATE (11/08/2012): The Federal Trade Commission (FTC) settled charges with PLS Financial Services and The Payday Loan Store of Illinois regarding their violation of FTC’s Disposal Rule and the Gramm-Leach-Bliley Act’s Privacy Rule and Safeguards Rule. The two companies agreed to pay $101,500. The companies must also implement a comprehensive information security program that will be assessed for compliance for the next 20 years.

Information Source: NAID  
records from this breach used in our total: 369

Payday Loan Stores (PLS) was fined $1,107,000 for failing to protect consumer information. In April of 2010, three boxes of documents were found by police at a dumpster near a Payday Loan Store. According to the Illinois Department of Financial and Professional Regulation, "the discarded documents contained personal customer information, including Social Security numbers and copies of driver’s licenses."

UPDATE (11/08/2012): The Federal Trade Commission (FTC) settled charges with PLS Financial Services and The Payday Loan Store of Illinois regarding their violation of FTC’s Disposal Rule and the Gramm-Leach-Bliley Act’s Privacy Rule and Safeguards Rule. The two companies agreed to pay $101,500. The companies must also implement a comprehensive information security program that will be assessed for compliance for the next 20 years.

Information Source: NAID  
records from this breach used in our total: 369
A password-protected laptop with patient information was accidentally thrown in the trash and lost for five days. Names, dates of service, and sometimes treatment description of patients treated for vascular conditions within the last four years were on the laptop. The laptop was thrown out on June 11 and found in a landfill on June 16.

Information Source: 
HHS via PHIPrivacy.net

August 17, 2010 Spring Mill Partners
Conshohocken, Pennsylvania
BSF PORT Unknown

Laptops with client information were stolen during a February office burglary.

Information Source: 
Databreaches.net

August 17, 2010 American Fidelity Assurance Company
Edmond, Oklahoma
BSF PHYS Unknown

The boxes were found in Edmond, Oklahoma and had the information of some Tulsa, Oklahoma residents as well.

Storage containers with Social Security numbers, names, dates of birth and other information were left on a curb in Edmond, Oklahoma. A couple went to the local news after having stored the hundreds of documents for a few years. The insurance papers are from 2003 and 2004 and have information on employees of multiple companies.

Information Source: 
Databreaches.net

August 16, 2010 Aultman Health Foundation
Canton, Ohio
MED PORT 13,800

On June 7, a laptop was stolen. Patient information from the Aultman Healthcare in Your Home program may have been exposed. This information included names, insurance identification numbers, health information, telephone numbers, addresses, dates of birth and Social Security numbers.

Information Source: 
Databreaches.net

August 16, 2010 Private Dental Practice
Tacoma, Washington
MED STAT Unknown

Around July 16, an office break in resulted in the loss of a computer with patient names, addresses, internal account numbers, telephone numbers, Social Security numbers and dates of birth.

Information Source: 
PHIPrivacy.net

August 16, 2010 Centric Software
Campbell, California
BSR PORT Unknown

A laptop theft resulted in the exposure of employee names, Social Security numbers and possibly contact information and dates of birth. The laptop was stolen from an employee’s car on July 23.

Information Source: 
Databreaches.net

August 13, 2010 Holyoke Medical Center, Caritas Carney Hospital, Milton Hospital, Milford Hospital
Georgetown, Massachusetts
MED PHYS 45,600

At least 32,750 files were found at the Georgetown Transfer Station in Georgetown, MA. Holyoke Medical Center is located in Holyoke, MA. Carney Hospital is located in Dorchester, MA. Milton Hospital is located in Milton, MA. Milford Hospital is located in Milford, MA.

A large pile of medical records was found at Georgetown Transfer Station public dump. The reports contained names, addresses, diagnosis, Social Security numbers, and insurance information. A medical billing company known as Goldthwait Associates is believed to be responsible. The medical records are mostly from pathology patients served at the hospitals between 2007 and March of 2010.

UPDATE (9/2/10): Holyoke reported that 24,750 patients were affected. The exact number of patients affected from other medical centers is still unknown. Between 8,000 and 12,000 patients of Milton Hospital were affected.

UPDATE (10/11/10): Milton Pathology Associates, P.C. reported that a prior owner of Goldthwait Associates improperly disposed of patient information. Eleven thousand patients were affected. Milford Regional Medical Center reports that the incident affected 19,750 patients.
UPDATE (01/07/2013): People associated with Goldthwait Associates, Chestnust Pathology Services, Milford Pathology Associates, Milton Pathology Associates, and Pioneer Valley Pathology Associates agreed to collectively pay $140,000 to settle allegations related to the breach.

Information Source: PHIprivacy.net

August 13, 2010 Doherty Hotel and Convention Center
Clare, Michigan

BSR HACK

Over 150 credit cards used at the Hotel's restaurant were later fraudulently charged. It is believed that the Hotel's database was illegally accessed.

Information Source: Dataloss DB

August 13, 2010 Montana Mikes
Clinton, Oklahoma

BSR HACK Unknown

Software that gathers credit card information was remotely installed on the Restaurant's computer system. The problem was fixed.

Information Source: Databreaches.net

August 13, 2010 Metro Nashville
Nashville, Tennessee

GOV PORT

In February of 2009, an auditor lost a USB device. The bank account information of victims of juvenile crime was on the unencrypted device.

Information Source: Media

August 13, 2010 Nashville Career Advancement Center
Nashville, Tennessee

GOV DISC

Outdated software is believed to have caused the Social Security numbers of clients of the Center to be exposed online.

Information Source: Media

August 12, 2010 Walsh Pharmacy
Fall River, Massachusetts

MED PORT

A DVD with patient information was lost in transit. Information included patient names as well as some Social Security numbers, health insurance information, driver's license numbers and prescription information. The DVD was not in the envelope when the recipient opened it.

UPDATE (8/18/10): The incident involved 11,440 patients.

Information Source: PHIprivacy.net

August 12, 2010 Tino's Greek Cafe
Austin, Texas

BSR CARD Unknown

Thieves collected debit and credit card information from customers of Tino's.

Information Source: Databreaches.net

August 12, 2010 Loma Linda University School of Dentistry
Loma Linda, California

EDU STAT

On the weekend of June 12, thieves stole three desktop computers with password protection. The computers did not contain patient treatment records, but did have Social Security numbers, dates of birth and other health information.

Information Source: PHIprivacy.net

August 11, 2010 Ambrosia Asian Bistro
Greeley, Colorado

BSR INSD

A waitress admitted to using a skimming device to collect the credit card information of between 50 and 60 customers.
Thomson Reuters
New York, New York

Police found Thomson CompuMark customer information in the home of a former employee. The information included names, addresses and credit card information. The employee processed customer payments between May and December of 2009.

NBC Universal
New York, New York

A laptop containing names, Social Security numbers and other personal information of current and former employees was stolen on February 4, and recovered on February 24.

LPL Financial
Boston, Massachusetts

An advisor accidentally sent an email attachment to clients that contained the names and account information of 38 other clients.

ProAssurance Mid-Continent Underwriters
Houston, Texas

Customer names, Social Security numbers, dates of birth, and addresses were exposed on the Per Diem Insurance web page.

College Center for Library Automation (CCLA)
Tallahassee, Florida

Personal data from students, faculty and staff from six colleges was accessible through an Internet search for five days. The information may have included full names, Social Security numbers, driver’s license numbers, and Florida identification card numbers. The institutions were Broward College, Florida State College at Jacksonville, Northwest Florida State College, Pensacola State College, South Florida Community College, and Tallahassee Community College.

Jewish Hospital Catheterization Lab
Louisville, Kentucky

Two stolen laptops contained personal information on patients who were treated between June 2, 2009 and July 16, 2010. Patient names, Social Security numbers, dates of birth, medical record numbers, addresses, phone numbers, patient account numbers, and insurance carriers.

Metropolitan Life Insurance Company (MetLife)
New York, New York

MetLife wrote "On January 5, 2010, we learned that one of our employees was sharing individual disability insurance applications with an unauthorized individual. We believe that the shared documents contained sensitive information including name, address, Social Security number, driver’s license number, checking account information, and date of birth."

Baltimore Chesapeake Bay Outward Bound Center
Baltimore, Maryland
After the theft of two office computers it was discovered that a file cabinet with employment documents was unlocked. The documents included names, Social Security numbers, addresses and bank account numbers. The robbery occurred sometime around February 1.

### August 10, 2010

**Select Portfolio Servicing (SPS)**  
**Salt Lake City, Utah**  
BSF DISC Unknown

Unencrypted SPS client data was sent to a server. Files of client 1099A and 1099C forms were exposed from January to February.

### August 10, 2010

**DC Chartered Health Plan**  
**Washington, District Of Columbia**  
MED PORT 540 (No SSNs or financial information reported)

The May 26 theft of a laptop resulted in the exposure of private health information of 540 people.

### August 10, 2010

**Nationwide Bank**  
**Columbus, Ohio**  
BSF PHYS 62

Customers were mailed the cards of other customers. The cards had Social Security numbers and names.

### August 9, 2010

**University of North Carolina at Greensboro**  
**Greensboro, North Carolina**  
EDU HACK 2,300

In June, it was discovered that a University computer from the Speech and Hearing Center was infected with malware. Around 2,300 people who received services as far back as 1997 may have had their Social Security numbers, addresses, dates of birth, telephone numbers, insurance companies, and insurance ID numbers exposed. Another computer from the Psychology Clinic was discovered to have a similar problem. Around 240 people were affected; though no Social Security numbers or financial accounts were involved.

### August 9, 2010

**Cathedral Square Corporation**  
**South Burlington, Vermont**  
NGO HACK Unknown

Residents of CSC may have had their names, bank account numbers and routing numbers exposed if they paid their rent electronically. Staff Health Savings Account information may have also been accessed.

### August 9, 2010

**Ameritas Investment Corp.**  
**Madison, Wisconsin**  
BSF PORT Unknown

On January 27, a backup tape was stolen when the office was burglarized. The backup tape contained names, addresses, Social Security numbers, dates of birth and policy numbers of clients.

### August 9, 2010

**Paraco Gas**  
**Rye Brook, New York**  
BSR STAT Unknown

On March 16, a computer containing personal information was stolen. The information included names, Social Security numbers, addresses, dates of birth and bank account numbers.

Information Source: Databreaches.net
A CD with employee W-2 statement information was lost in transit during December of 2009. Employee names, addresses and Social Security numbers were in the W-2 files. Around 143 employees from Maryland alone were affected.

Information Source: Databreaches.net

---

August 9, 2010  HSBC Bank Nevada
Buffalo, New York

The location listed is the headquarters; not the location of the incident.

A caller claiming to be an employee managed to get an employee to change the information on 14 customer accounts.

Information Source: Databreaches.net

---

August 9, 2010  Jones Lang LaSalle
Chicago, Illinois

Some employee information was on a stolen laptop. The laptop was stolen from an employee's car on December 17 of 2009 and contained bank account information, names, and addresses.

Information Source: Databreaches.net

---

August 7, 2010  Fort Worth Allergy and Asthma Associates
Fort Worth, Texas

The June 29th theft of four computers resulted in patient records being exposed. The patient records contained addresses, Social Security numbers and dates of birth.

Information Source: PHIPrivacy.net

---

August 6, 2010  United HealthGroup
Minneapolis, Minnesota

It appears that a breach involving paper records and categorized by the Health and Human Services (HHS) website as "theft, unauthorized access" occurred when patient documents were stolen on March 2. The incident was reported to HHS on August 4. Little more is known about the incident.

Information Source: HHS via PHIPrivacy.net

---

August 6, 2010  United HealthGroup
Minneapolis, Minnesota

United HealthGroup reported a breach of paper records to Health and Human Services in June. The breach occurred on January 26.

Information Source: HHS via PHIPrivacy.net

---

August 6, 2010  WellPoint, Inc.
Indianapolis, Indiana

It is unclear if this incident is related to a June 2010 incident which was determined to have affected 470,000 people.

A hacking or IT incident that occurred or was discovered around November 3, 2009 resulted in the possible exposure of protected health information on a network server. The incident was reported by HHS on August 6, 2010.

Information Source:
August 5, 2010  
**Ross**  
Houston, Texas  

Someone reported a public dumpster full of Ross applications and resumes. Employees from the Ross were then sent to recover the applications. The applications dated back to 2002 and contained Social Security numbers and contact information.

**Information Source:**  
NAID  

---

August 5, 2010  
**Blue Cross Blue Shield of Alabama**  
Birmingham, Alabama  

A dishonest employee was charged with identity theft. The employee fraudulently obtained credit by using the health insurance information of at least 15 clients.

**Information Source:**  
PHIPrivacy.net  

---

August 4, 2010  
**Rockland town government**  
Rockland, Massachusetts  

On July 23, canceled payroll checks with Social Security numbers and bank account numbers were lost when wind knocked them off of a recycling truck. Current and former employees of Rockland’s government between 1992 and 2002 were affected.

**Information Source:**  
Databreaches.net  

---

August 4, 2010  
**Hingham city government**  
Hingham, Massachusetts  

An email with the Social Security numbers, names, and employee identification numbers of Hingham city employees was accidentally emailed to about 30 department heads. Some of the emails were automatically forwarded to personal accounts and personal devices.

**Information Source:**  
Databreaches.net  

---

August 3, 2010  
**Metro Assessor of Property**  
Nashville, Tennessee  

Flood victims who were applying for property tax cuts had their personal information exposed online. The online application involved uploading canceled checks; these checks, tax returns, and other sensitive information were all available online because the system’s password requirements had been removed. According to the Organization: “The staff were trying to make it easier for people to enter information online.”

**Information Source:**  
Databreaches.net  

---

August 1, 2010  
**Guttenberg Housing Authority**  
Guttenberg, New Jersey  

An unauthorized individual may have accessed sensitive information on housing applicants and residents in late December 2009. The information may have included Social Security numbers, names and other personal identifying information.

**Information Source:**  
Databreaches.net  

---

July 31, 2010  
**The Center for Neurosciences**  
Tucson, Arizona  

A visitor stole a laptop from an electromyogram and nerve conduction studies exam room on December 15, 2009. The computer contained names, dates of birth, referring physicians and reasons for neurophysiological tests.
Two computers were stolen during the weekend of May 22nd. Names, medical record numbers, Social Security numbers, dates of birth, insurers, and hospital admission dates for an unknown number of patients were on the computers.

**UPDATE** (8/3/10): One computer was from the Finance Department and had the information of 16,000 patients; the second computer theft affected the records of 23,000 students from the School Health Program and their families.

**First Advantage Tax Consulting Services (TCS)**
Indianapolis, Indiana

A laptop that contained personal information was lost or stolen during an airport layover. The Social Security numbers of people who were employed by companies that used TCS for tax help were on the laptop. The laptop did have a password and after it was lost its access to TCS’s network was blocked.

**Texas Children's Hospital and Baylor College of Medicine**
Houston, Texas

A physician’s laptop was stolen from an office on May 13th. The laptop contained personal information on cardiology patients. Affected persons were notified that their names, dates of service, medical record numbers, diagnoses and dates of birth were on the password-protected laptop.

**UPDATE** (9/2/10): Only 694 patients were affected. The original notice on the website stated that 1600 patients were at risk.

**New York Urology Associates**
Cheektowaga, New York

Someone reported that medical papers were blowing around a parking lot. The documents had Social Security numbers, addresses, and names.

**University of Virginia**
Charlottesville, Virginia

A transient was ordered to spend time in a men’s diversion program after pleading guilty to stealing credit cards and electronics. One of the laptops he stole was a University-owned laptop. The man served 12 months in jail before being sentenced and slept in his car and in the University library during the time of the thefts.

**DebtStoppers USA, Robert J. Semrad and Associates**
Chicago, Illinois

Documents from the Joilet office were involved

A tipster led to the discovery of hundreds of personal and financial documents in a trash bin outside the attorney’s office. The documents included Social Security numbers, names, addresses, driver’s license numbers, and signed debit card authorizations from clients.

**Rowland Equipment Co.**
Smithfield, Virginia

Linda Rowland pleaded guilty to wire fraud and identity theft. She used the names and information of over 30 customers to falsify loan agreements for over 10 years.
July 28, 2010  Wendy's
Tukwila, Washington  BSR  INSD  135

A dishonest employee used a skimmer between September 14, 2009 and July 21, 2010 to commit identity theft and make fraudulent charges to customer credit accounts. At least 135 accounts were fraudulently charged.

July 28, 2010  Time Warner Cable
New York, New York  BSR  INSD  Unknown

A former employee was convicted of installing spyware on three company computers. The employee intended to capture the passwords of users who had access to a customer database and a billing system.

July 27, 2010  Rite Aid Corporation
Camp Hill, Pennsylvania  BSR  PHYS  Unknown

Etters, PA is also mentioned as Rite Aid’s headquarters

Rite Aid paid one million dollars to settle HIPAA privacy violations. Rite Aid also agreed to update corporate policies and procedures so that patient medical information would be properly disposed, employees would be properly trained in disposal of patient information, and employees would be held accountable if they did not dispose of patient information properly.

July 27, 2010  Private Legal Practice
San Antonio, Texas  BSO  PHYS  75

An attorney left legal files in a public dumpster. The attorney thought it was appropriate to dispose of the files in this way since the accounts were old and closed. The documents contained names, addresses, bank account information, Social Security numbers, driver’s license numbers, and dates of birth.

July 27, 2010  Cooper University Hospital
Camden, New Jersey  MED  PORT  Unknown

A flash drive with the personal information of graduate medical residents and fellows was reported missing on July 23. The personal information included Social Security numbers, dates of birth, race, gender, addresses, phone numbers, marital status, emergency contacts and more. Students enrolled between 2008 and 2010 and current members of staff were affected.

July 27, 2010  Citigroup Inc.
New York, New York  BSR  DISC  117,600 (No incidents reported)

Citigroup’s mobile banking application for Apple’s iPhone has a security flaw that saves user account numbers, bill payments and security access codes into a hidden file on the iPhone and the user’s computer. An upgrade that will fix the problem is available.

July 26, 2010  Natchez Police Department
Natchez, Mississippi  GOV  INSD  Unknown

A police officer with the Natchez department fraudulently used and encouraged others to use stolen credit and debit cards.
Student records dating from 2000 to June 21, 2010 were compromised on a University file server on four separate occasions within the last two years. The server contained student health center prescription records.

Information Source: Databreaches.net

July 23, 2010  Thomas Jefferson University Hospitals Philadelphia, Pennsylvania  
A password-protected laptop was stolen from the office of an employee on June 14. The computer should not have contained protected health information, but did. It also contained the name, birth date, gender, ethnicity, diagnosis, Social Security number, insurance information, and hospital account number of approximately 24,000 patients.

Information Source: Databreaches.net

July 23, 2010  University of California San Francisco (UCSF) Medical Center San Francisco, California  
A former employee used the Social Security numbers of his colleagues to obtain vouchers for Amazon.com purchases. He secretly used the Social Security numbers to create hundreds of accounts and complete 382 online StayWell health surveys in exchange for $100 online vouchers.

UPDATE (10/28/10): The former employee pled guilty to wire fraud and improper use of Social Security numbers. He was sentenced to 12 one year and one day in prison.

Information Source: Databreaches.net

July 22, 2010  The Loft and Comedy Club Columbus, Georgia  
Names, addresses, phone numbers, and credit card information from customers of The Loft and Comedy Club were discovered through a Google search. Customer data from 2004 to 2008 was posted. The Loft fixed the problem and is working on having the site removed.

Information Source: Databreaches.net

July 22, 2010  Colorado Department of Health Care Policy and Financing Denver, Colorado  
A hard drive containing personal information for clients enrolled in state-provided health insurance was stolen from the Colorado Office of Information Technology. The information included names, state ID number and the name of the client’s program. The Agency is certain that contact information, financial information and Social Security numbers were not involved.

Information Source: Databreaches.net

July 22, 2010  Iowa Department of Agriculture and Land Stewardship Des Moines, Iowa  
A laptop containing personal information from Iowa residents was stolen from a locked state vehicle. The computer was encryption protected and contained names, addresses, phone numbers and Social Security numbers. Iowa residents who participate in the Iowa Horse and Dog Breeding Program were notified.

Information Source: Databreaches.net

July 21, 2010  Lincoln National Life Insurance Radnor, Pennsylvania  
A vendor printed a user name and password for agents and authorized brokers in a brochure. The brochure was also posted on an agent’s public website. The login information enable access to a website containing medical records and other personal information from individuals seeking life insurance. Applicant name, Social Security number, address, policy number, driver’s license number and credit information is also on the website.
July 20, 2010  Long Island Consultation Center (LICC)  
Rego Park, New York  

A computer device containing doctor reports was reported missing from a secured area at LICC on May 24th. Names, dates of birth, diagnostic information and treatment information of some patients may have been included on the device.

July 20, 2010  South Shore Hospital, Active Data Solutions  
South Weymouth, Massachusetts  


Computer files containing personal, health and financial information of volunteers, patients, vendors, business partners and employees from January 1996 through January 2010 may have been lost by a professional data management company. Depending on the person's association with the hospital, the information exposed could be full name, address, phone number, date of birth, Social Security number, driver's license number, medical record number, patient number, bank account information, credit card number, diagnoses and treatment.

**UPDATE (9/10/10):** Archive Data Solutions (formerly Iron Mountain Data Products) was revealed to be the company responsible for disposing of South Shore Hospital's records. Archive Data Solutions subcontracted the process to Graham Magnetics, who then lost the tapes in shipping. The tapes may have also had patient information from Harbor Medical Associates and patient and vendor information from South Shore Physician Hospital Organization.

After investigating the incident the hospital decided not to mail notices or offer credit monitoring and identity theft services to those who may have been affected by the loss. It was determined that the risk of the data being accessed was extremely low and that notifications inside the hospital, on websites, via email and in newspapers would be enough. In addition, the Attorney General's office of Massachusetts has spoken out against the hospital's decision to skip precautions.

**UPDATE (5/24/2012):** South Shore Hospital will pay $750,000 to settle HIPAA violation and state law charges. The breach involved the loss of two of three boxes containing 473 unencrypted back-up computer tapes with sensitive information sometime between February 2010 and June of 2010. A total of $250,000 in civil penalty fines and a payment of $225,000 for an education fund to be used by the Attorney General's Office to promote education concerning the protection of personal information and protected health information was determined. South Shore Hospital was given a credit of $275,000 to reflect the cost of security measures it had already taken subsequent to the breach.

July 20, 2010  Maryland Department of Human Resources  
Baltimore, Maryland  

An employee posted Social Security numbers and other personal information of around 3,000 clients on an outside website. The organization provides food stamps and other benefits and aid to clients. The employee was placed on administrative leave.

July 19, 2010  LV Financial Services  
Orlando, Florida  

Dozens of boxes of files from medical offices that hired LV to collect unpaid bills were found in an Orlando public dumpster. The files contained names, addresses, Social Security numbers, driver's license copies and credit reports. The collection agency went out of business in 2005 and the location of the files prior to this incident is unknown.

July 16, 2010  United Healthcare (UnitedHealthcare), Deere and Company  
Minneapolis, Minnesota  

Deere and Company is headquartered in Moline, Illinois.
United Healthcare notified members of a Deere and Company employee benefits plan of a mistake that led to claims summary statements being sent to the wrong addresses. Dates of services, categories of service, cost of service, and physician names were included.

**Information Source:** PHIprivacy.net

**July 16, 2010**

**Buena Vista University**

**Storm Lake, Iowa**

EDU HACK 93,000

Someone gained unauthorized access to a BVU database. The database contained records of names, Social Security numbers, and driver’s license numbers of BVU applicants, current and former students, parents, current and former faculty and staff, alumni and donors. These records go back as far as 1987.

**Information Source:** Databreaches.net

**July 16, 2010**

**Connecticut Department of Labor**

**Bridgeport, Connecticut**

GOV PORT 5,000

A highly encrypted laptop was stolen from the office of the Connecticut Department of Labor. The laptop contained confidential information about unemployment insurance claims, wage discrepancy complaints and some Bridgeport area employers.

**Information Source:** Databreaches.net

**July 15, 2010**

**Private Dental Practice**

**Barstow, California**

MED PHYS Unknown

An anonymous tipster called the Sheriff’s Department and reported unattended boxes of personal records outside the dental office. The boxes contained patient records from the early 1990’s to the present. These records numbered in the hundreds and had personal information such as Social Security numbers, names, birth dates, credit card numbers, and addresses. The Sheriff’s Department destroyed the records and warned patients of dentists Lee, Sang H. Yoon and Patricia Patterson.

**Information Source:** Databreaches.net

**July 15, 2010**

**Prince William County Intellectual Disabilities Case Management**

**Woodbridge, Virginia**

GOV PORT 669

On June 18th or 19th, a government-issued Blackberry was stolen from an employee’s car. The Blackberry had personal information on patients enrolled in the program. The County notified residents that their Social Security numbers, names, addresses, dates of birth, phone numbers, and Medicaid numbers may have been accessed.

**Information Source:** PHIprivacy.net

**July 15, 2010**

**Utah Department of Workforce Services**

**Salt Lake City, Utah**

GOV INSD 1,300 (Unknown number of SSNs)

A leak that allowed anti-immigration activists to post and circulate the names, Social Security numbers, medical information, addresses, workplaces, and phone numbers of alleged illegal immigrants in Utah has been linked to Utah’s Department of Workforce Services. A large number of employees had access to this information.

**Information Source:** Databreaches.net

**July 15, 2010**

**Nix Check Cashing**

**Manhattan Beach, California**

BSF STAT Unknown

The May 17th theft of a computer resulted in the exposure of customer names, addresses, phone numbers, Social Security numbers and driver’s license numbers. Affected customers were notified on June 30th. Over one hundred customers from New Hampshire were affected; though the total number of customers affected is unknown.

**Information Source:** Databreaches.net

**July 15, 2010**

**NBTY**

**Bohemia, New York**

BSR DISC Unknown

An email containing current and former employees' and plan participants' personal information was sent to the wrong recipient on June 15th. The information in the email included names, dates of birth, and Social Security numbers.
July 15, 2010  Alcoa Global Mobility Group  
New York, New York  
BSO DISC Unknown

An electronic folder containing personal information on current and former expatriates and others who received assistance from Alcoa’s Global Mobility Group was shared as a public folder within its network. The personal information included names, dates of birth, family members’ names and dates of birth, salary compensation, Social Security numbers, and some people’s medical information.

July 14, 2010  SunBridge Healthcare  
Albuquerque, New Mexico  
MED PORT 3,830

Residents of Arizona, Colorado, Montana, California, New Mexico, Oklahoma, Idaho, Washington, Wyoming and Utah affected

A laptop containing Social Security numbers, medical record numbers, dates of service, health insurance numbers and names was stolen in May. The laptop was password-protected.

July 14, 2010  Oregon State University  
Corvallis, Oregon  
EDU HACK 34,000 (unknown number of SSNs)

A University computer containing personal information of current and former employees was found to be infected by a virus. Employee records from 1999 to 2005 contained Social Security numbers.

July 14, 2010  Carle Clinic Association  
Urbana, Illinois  
MED PHYS 1,300 (no SSNs or financial information reported)

An impostor posing as a representative of the organization’s recycling service removed several barrels of purged x-ray films and film jackets. The health information included approximately 1,300 patient names, dates of birth, gender, clinic medical numbers, internal accession numbers, site locations, physician or provider names, and internal provider numbers.

July 14, 2010  Blue Island Radiology  
Blue Island, Illinois  
MED PORT 2,000 (number and type of financial account numbers and SSNs unknown)

A backup data tape and compact disc containing protected health information were never received. Individuals demographic, financial and clinical information were on the CD.

July 14, 2010  Blue Cross Blue Shield Association  
Chicago, Illinois  
MED PHYS 15,000 (0 SSNs and financial information reported)

An error in the quarterly address update process resulted in the mailing of approximately 15,000 individuals’ protected health information to incorrect addresses. The information in the letters included demographic information, explanation of benefits, clinical information, and diagnoses. The returned mail was collected and the organization verified whether or not it had been delivered.
<table>
<thead>
<tr>
<th>Date</th>
<th>Organization</th>
<th>Industry</th>
<th>Location</th>
<th>Financial Information Involved</th>
<th>Records from this Breach Used in Our Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 14, 2010</td>
<td>VHS Genesis Lab</td>
<td>MED</td>
<td>Berwyn, Illinois</td>
<td>No SSNs or financial information involved</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Over 500 client invoices went missing. It does not appear that the month's worth of invoices were mailed. They contained health information such as names, dates of birth, and medical testing information.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Information Source:</strong> PHIPrivacy.net</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>July 14, 2010</td>
<td>University of Pittsburgh Student Health Services</td>
<td>EDU</td>
<td>Pittsburgh, Pennsylvania</td>
<td>Not included because no specific type of financial information stated</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>An employee dishonestly took documents containing names and financial information. The employee was fired.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Information Source:</strong> PHIPrivacy.net</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>July 14, 2010</td>
<td>Tomah Memorial Hospital</td>
<td>MED</td>
<td>Tomah, Wisconsin</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>A nurse used patient names and account numbers to illegally obtain narcotics. The nurse was fired.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Information Source:</strong> PHIPrivacy.net</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>July 13, 2010</td>
<td>Carolina Center for Development and Rehabilitation</td>
<td>MED</td>
<td>Charlotte, North Carolina</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>After a doctor left office cleaning to his sons, they mistakenly threw out hundreds of medical records. The medical records were left in a public recycling bin and included medical histories, pictures of patients and Social Security numbers.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>UPDATE (7/31/10):</strong> The psychologist has contacted 1,590 of his patients.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>UPDATE (9/7/2011):</strong> The psychologist has paid $40,000 for violating state regulations by illegally dumping files containing patients’ financial and medical information. This information included names, Social Security numbers, addresses, dates of birth, drivers’ license numbers, insurance account numbers, and health information.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Information Source:</strong> NAID</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>July 12, 2010</td>
<td>Connecticut Department of Education, State Teachers' Retirement Board</td>
<td>GOV</td>
<td>Hartford, Connecticut</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>An encrypted flash drive containing 2007-2008 Connecticut Teachers’ Retirement Board member annual statement data has been lost or stolen. It is unlikely that outside parties could read the pension and employment credit.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>UPDATE (8/5/10):</strong> The total number of retirees exposed to ID theft is reported as 58,000.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Information Source:</strong> Databreaches.net</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>July 12, 2010</td>
<td>Marsh and Mercer</td>
<td>BSF</td>
<td>Washington, District Of Columbia</td>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Marsh and Mercer’s Seaby and Smith, Inc. and Mercer Health and Benefits LLC operations were involved. The list of known organizations with affected employees includes Idaho Power, Saint Luke’s health System and Saint Alphonsus Regional Medical Center.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The location is listed as Seaby and Smith’s office.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The insurance broker and benefits consulting firm reported the loss of a backup tape during transport. The tape contained employee benefits information for companies that used Marsh and Mercer for consultation. Names, addresses, Social Security numbers, dates of birth, account information and driver’s license numbers were on the tape.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>UPDATE (8/9/10):</strong> Three hundred current and former Boise, Idaho city employees were also affected.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>UPDATE (8/26/10):</strong> The Idaho Power website revealed that around 5,000 employees were affected, and a total of 375,000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
individuals from other organizations were affected.

**Information**  
**Source:** Databreaches.net  
**Records from this breach used in our total:** 378,000

**July 10, 2010**  
**Ohio Department of Developmental Disabilities**  
**Columbus, Ohio**  
**MED DISC 200**

Within a two week period personal information of 200 people using the Department's services was accidentally posted online. The Social Security numbers, names, addresses, medical records, and treatment information were only available for viewing through the state computer network.

**Information**  
**Source:** PHIPrivacy.net  
**Records from this breach used in our total:** 200

**July 10, 2010**  
**Village of Big Bend**  
**Big Bend, Wisconsin**  
**BSO PORT Unknown**

A laptop containing payroll information for the village’s employees was stolen from the car of the village’s payroll provider in Milwaukee. Police have not recovered the laptop. The provider reported the theft and sent letters to employees to inform them their personal information was not secure. The provider recommended that employees contact a credit bureau that would place a 90-day alert on their information to prevent identity theft.

**Information**  
**Source:** Dataloss DB  
**Records from this breach used in our total:** 0

**July 10, 2010**  
**Cisco Live 2010**  
**Las Vegas, Nevada**  
**BSO HACK Unknown**

Someone hacked the list of attendees for the recent Cisco Live 2010 users' conference, a security breach that led Cisco to notify the customers as well as a broader group who have dealings with the company. A vendor told Cisco that someone had made “an unexpected attempt to access attendee information through ciscolive2010.com,” the event Web site. That lead to the general notification that Cisco sent to attendees and others who had been invited but did not attend. According to Cisco, details about less than 20% of those on the list were compromised. The breach was closed quickly, "but not before some conference listings were accessed." The compromised information consisted of Cisco Live badge numbers, names, titles, company addresses and e-mail addresses. "No other information was available or accessed," according to the warning Cisco Live's event team sent via e-mail.

**Information**  
**Source:** Dataloss DB  
**Records from this breach used in our total:** 0

**July 9, 2010**  
**Emily Morgan Hotel**  
**San Antonio, Texas**  
**BSO PHYS 17,000**

Identity thieves obtained stacks of credit card receipts from one of the hotel’s storage rooms in 2006. Hundreds of thousands of dollars in fraudulent charges were then made in three different states. Investigators first became aware of a large identity theft issue in the area during the beginning of 2009.

**UPDATE** (12/4/2010): The ringleader pleaded guilty to ID theft fraud conspiracy, access device fraud and conspiracy to launder money. Seven other co-conspirators have been identified.

**UPDATE** (4/7/2011): A former hotel worker faces up to 22 years in prison for stealing customer information and using it to go on a shopping spree. In 2006, the former employee used credit card receipts from the Emily Morgan hotel in downtown San Antonio to make fraudulent charges totaling $300,000. This appears to be the one of the largest cases in Alamo City’s history. The accused former employee pleaded guilty to three charges and is scheduled to be sentenced in July.

**Information**  
**Source:** Databreaches.net  
**Records from this breach used in our total:** 17,000

**July 8, 2010**  
**Waukesha County**  
**Big Bend, Wisconsin**  
**GOV PORT Unknown**

A laptop was stolen from a payroll services provider of the county. It is unknown what types of Big Bend employee payroll information were contained on the laptop.

**Information**  
**Source:** Dataloss DB  
**Records from this breach used in our total:** 0

**July 7, 2010**  
**University of Hawai'i**  
**Honolulu, Hawaii**  
**EDU STAT 53,000**

53,000 people may have had their personal information exposed after a breach to the University of Hawai'i computer system was discovered. The university released statement that more than 40,000 Social Security numbers and 200 credit card numbers were part of the exposed information that was housed on a computer server used by the Mānoa campus parking office.
July 7, 2010

Massachusetts Secretary of State, Securities Division
Boston, Massachusetts

The Massachusetts Secretary of State’s office accidentally released confidential personal information earlier this year on 139,000 investment advisers registered with the state. The data, including the advisers’ Social Security numbers, were on a CD-ROM sent to IA Week, an investment industry publication that had requested public information from the Securities Division. Secretary of State IA Week had asked for a list of registered investment companies. The Securities Division responded by sending a list of individual investment professionals. In addition to their names and Social Security numbers, this list included their dates and locations of birth, height, weight, hair color, and eye color.

Information Source: Dataloss DB

July 6, 2010

Massachusetts Secretary of State Office
Boston, Massachusetts

In an attempt to release public information from the Securities Division, the Massachusetts Secretary of State’s office released the Social Security and driver’s license information of 139,000 investment advisers registered with the state. The information was sent on a CD-ROM sent to IA Week, an investment industry publication.

Information Source: Dataloss DB

July 6, 2010

University of Florida
Gainesville, Florida

Social Security numbers or Medicaid identification numbers were shared with a telephone survey company and included on address labels sent out to request research participation. The letters were sent through the U.S. Postal Service on May 24th and the issue was discovered on June 6th.

Information Source: Databreaches.net

July 6, 2010

DentaQuest
Chicago, Illinois

In a statement datelined out of Nashville, DentaQuest reported the laptop theft occurred March 20 in Chicago and was informed of the incident April. DentaQuest reported the laptop contained a database which held the personal information of approximately 76,000 clients. The contractor advised most of the data is not considered sensitive, but the device did contain the first names, last names and Social Security Numbers of about 21,000 individuals. Some 10,500 are Tennessee residents.

Information Source: Dataloss DB

July 4, 2010

AMR Corporation
Fort Worth, Texas

American Airlines parent company said Friday the personal information of about 79,000 retirees, former and current employees has been compromised after a hard drive was stolen from its Fort Worth headquarters. No customer data was affected. The data was held by the company’s pension department. The drive contained images of microfilm files, which included names, addresses, dates of birth, Social Security numbers and a “limited amount” of bank account information. Some health insurance information may have also been included -- mostly enrollment forms, but also details about coverage, treatment, and other administrative information. The data spans a period from 1960 to 1995. AMR also believes some of the employee files also contained information on beneficiaries, dependents and other employees from 1960 to 1995.

Information Source: Dataloss DB

July 4, 2010

Beautiful Brands International
West Lafayette, Indiana

Computer hackers have infiltrated the credit card processing system.

Information Source: Dataloss DB

July 2, 2010

AMR Corporation
Fort Worth, Texas

Retirees, current, and former employees who participated in AMR’s pension plan may have had their names, Social Security numbers, addresses, dates of birth, and other personal information stolen by the theft of a hard drive containing microfilm files. Employees and beneficiaries of employees who were enrolled between 1960 and 1995 are at risk.
According to Cornerstone: “During the weekend of April 30th, 2010, flood waters broke windows of our administrative office for School-Based Services... As a result of the unprecedented flooding that occurred, some clinical record information, along with name, Centerstone ID#, Social Security number, and date of birth, may have been removed from the building by flood waters.”

An unencrypted portable USB was lost or stolen sometime around May 12th. It contained patient names, medical record numbers, sex, age, procedure, attending physician, time of arrival in recovery room and time of discharge from recovery room.

Multiple CDs containing patient personal information were lost in transit by FedEx. Information included dates of birth, driver’s license numbers, descriptions of medical procedures, addresses, and Social Security numbers. Siemens Medical Solutions USA, the Hospital’s billing contractor, shipped the CDs around March 16th. They were never received.

The university’s Information Technology department noticed unusual Internet activity on a laptop computer associated with its network. It determined the computer belonged to an employee and was infected with a virus known as Zeus or Z-Bod. The employee’s laptop had access to computer files that contain student names and Social Security numbers.

Hackers compromised the personal information of 4,585 students who received services from the school’s counseling center. The center provides students with support and mental health services. The information on the servers included names, Social Security numbers and clinical information on every student who sought counseling services from the center between August 8, 2002 and June 21 of this year.

Hackers have broken into the payment processing system of Destination Hotels & Resorts, a high-end chain best known for its resort hotels in destinations such as Vail, Colorado; Lake Tahoe, California; and Maui, Hawaii. Destination has uncovered a malicious software program inserted into its credit card processing system from a remote source. Destination Hotels is in the process of notifying victims but will not say how many people have had their credit card numbers stolen. The attackers appear to have hit only point-of-sale processing systems, where credit cards are swiped for purchases. Personal information such as guests’ home addresses was not compromised.

UPDATE (7/2/10): Around 700 customers were affected nationwide by the hack; including dozens of customers of the Driskill Hotel of Austin, Texas.
Information such as names and Social Security numbers was exposed to the public through a web server. The students affected were on the class roster for a computer science and engineering course. The files were discovered and removed on June 10th.

Information Source: Databreaches.net

<table>
<thead>
<tr>
<th>Date</th>
<th>Organization</th>
<th>Location</th>
<th>Sector</th>
<th>Impact</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 29, 2010</td>
<td><strong>Sparta Board of Education</strong></td>
<td>Sparta Township, New Jersey</td>
<td>GOV</td>
<td>DISC</td>
<td>Several vendor Social Security numbers and tax identification numbers were accidentally sent out via email to a local activist requesting information on Sparta Board of Education vendors. UPDATE (7/8/10): The activist mentioned is Jesse Wolosky and he has not returned the information because &quot;they could get lost in cyberspace or go to the wrong inbox.&quot; Wolosky also claims that state agencies are looking into the matter. The number of Social Security numbers is still unknown since Wolosky claims 600-800 and the district claims 200-300.</td>
</tr>
<tr>
<td>June 29, 2010</td>
<td><strong>Brooklyn Tech High School</strong></td>
<td>Brooklyn, New York</td>
<td>EDU</td>
<td>HACK</td>
<td>Hackers accessed PSAT information from the school and posted the names, home addresses, citizenship status, and Social Security numbers of students. The information was discovered on the school’s website.</td>
</tr>
<tr>
<td>June 29, 2010</td>
<td><strong>Merrimack Mortgage</strong></td>
<td>Greer, South Carolina</td>
<td>BSF</td>
<td>PHYS</td>
<td>Personal documents from Merrimack Mortgage were found in an unsecured public dumpster. The documents were not shredded and contained Social Security numbers, credit scores, bank information, and other personal information.</td>
</tr>
<tr>
<td>June 29, 2010</td>
<td><strong>A Woman's Place</strong></td>
<td>Ketchikan, Alaska</td>
<td>MED</td>
<td>DISC</td>
<td>An ACLU lawsuit claims that police acted inappropriately during a raid of A Woman’s Place clinic. The lawsuit claims that police not only confiscated around 400 medical records, but read them and revealed sensitive medical information about patients to outside parties. UPDATE (12/28/2012): ACLU is asking that the records be returned. The police were investigating the clinic because it’s owner is accused of billing state Medicaid program for services to 37 patients after having her license suspended. Seven pharmacies billed Medicaid for prescriptions she had written after the owner’s prescription authority was also suspended.</td>
</tr>
<tr>
<td>June 29, 2010</td>
<td><strong>Ridgefield High School</strong></td>
<td>Ridgefield, Connecticut</td>
<td>EDU</td>
<td>HACK</td>
<td>Two students were arrested for hacking into their school’s computer system. Their goal appears to be changing their own grades; but they had access to the grades and personal information of other students.</td>
</tr>
<tr>
<td>June 28, 2010</td>
<td><strong>Children's Hospital of Orange County</strong></td>
<td>Orange, California</td>
<td>MED</td>
<td>PHYS</td>
<td>The Hospital is checking its database for accuracy after discovering that patient files have been faxed to the wrong location at least twice. Patient records were faxed to an auto shop in 2009, and the wrong doctor on a separate occasion.</td>
</tr>
</tbody>
</table>

Information Source: Databreaches.net
Mercer, the firm’s consulting group, provided a subcontractor with a file containing Pension Plan participant addresses and Social Security numbers. The Social Security numbers were exposed on the mailing label.

**Information Source:** PHIPrivacy.net

**June 26, 2010**  
**Federal Aviation Administration**  
**Washington, District Of Columbia**

This is an update to the February 9, 2009 breach entry.

An investigation that was launched in response to the 2009 breach of the Federal Aviation Administration’s computer system (see Feb. 9, 2009, entry) was released June 26, 2010. The findings reveal that the names addresses, Social Security numbers, medical data and other personal information of airmen are still vulnerable and that “serious security lapses” exist.

**NOTE (12/2/2010):** This entry has been updated to correct an error. Prior to December 2, 2010, this entry erroneously implied that a new breach had occurred involving 3 million records. We apologize for our mistake.


**June 26, 2010**  
**New York Life Insurance Company**  
**Sacramento, California**

A woman was sentenced to 30 months in federal prison for access device fraud. Stephanie Fahlgren was arrested in July of 2009 after it was determined that she had obtained and misused the personal and financial information of more than 114 people. She obtained access to the New York Life Insurance Company’s computer database by using the login information of a Sacramento insurance agent. The database contained personal and medical information of prospective life insurance purchasers. Fahlgren used the information between June and November of 2008, to open lines of credit and obtain credit cards in the names of those people. The amount of restitution owed to the fraud victims will be determined in July of 2010.

**Information Source:** Databreaches.net

**June 25, 2010**  
**University Hospital**  
**Augusta, Georgia**

Two backup tapes containing personal information have gone missing. The hospital does not suspect theft and does believe that there is a very low probability that the personal information on the tapes can be misused. However, credit monitoring services are being offered to those who were affected. The hospital gave up looking for the tapes on May 7th and began notifying patients in late June.

Per phone interview with University Hospital, Social Security number were involved but they are unaware of any financial data involved in this breach.

**Information Source:** Dataloss DB

**June 25, 2010**  
**Sacramento Department of Parks and Recreation**  
**Sacramento, California**

A local news team investigated a pile of materials in a dumpster outside of a parks building. Unused, unopened books and learning materials were thrown out along with sensitive personal information. Names, Social Security numbers, phone numbers, dates of birth, addresses, monthly incomes, and copies of driver’s licenses dating back to 2005 were found in several abandoned folders.

**Information Source:** Databreaches.net

**June 24, 2010**  
**University of Oklahoma**  
**Norman, Oklahoma**

The University of Oklahoma began warning students of a security breach after its IT department noticed unusual internet activity on a laptop associated with its network. The laptop was infected with a virus and it contained student names and Social Security numbers. Students were advised to check bills and credit card transactions to make sure that no fraud had occurred.

**Information Source:** Media
More than 200,000 Anthem Blue Cross customers this week received letters informing them that their personal information might have been accessed during a security breach of the company's website. Only customers who had pending insurance applications in the system are being contacted because information was viewed through an online tool that allows users to track the status of their application. Social Security and credit card numbers were potentially viewed. Anthem Blue Cross merged with WellPoint in 2004.

**UPDATE (6/29/2010):** Around 470,000 customers in 10 states were notified of the breach. The original story states that only applicants were affected, but existing customers also received notification of a possible breach of their information.

**UPDATE (7/12/2010):** 20,000 Louisville, Kentucky residents received notification that a security mistake online resulted in the exposure of their Social Security numbers and financial information. It is unclear whether these residents are included in the original 470,000 customers. Only customers who were self insured were affected. WellPoint is claiming that this and other recent breaches were committed by an attorney or attorneys attempting to gain information for a lawsuit against WellPoint.

**UPDATE (9/17/2010):** An Anthem applicant whose information was exposed by the breach filed a lawsuit against Anthem at the Los Angeles County Superior Court. The lawsuit claims that the breach exposed applicants and clients to identity theft. An applicant behind the lawsuit is seeking class action status.

**UPDATE (10/29/2010):** The office of the Attorney General of Indiana is suing WellPoint Inc. because of the company's delay in notifying customers of the breach. WellPoint is accused of violating an Indiana law that requires businesses to provide notification of breaches in a timely manner and faces $300,000 in fines. State officials believe WellPoint was aware of the exposure in late February, but waited until June to notify customers.

**UPDATE (7/5/2011):** WellPoint Inc. will pay Indiana a $100,000 settlement for violating a 2009 data breach notification law. Customer data was accessible between October 23, 2009 and March 8, 2010. One or more consumers informed WellPoint of the problem on February 22, 2010 and again on March 8, 2010. WellPoint began notifying consumers on June 18, 2010.

**UPDATE (07/13/2013):** About 612,000 individuals may have had their names, Social Security numbers, dates of birth, addresses, telephone numbers, health information, and other electronic protected health information exposed. WellPoint paid HHS $1.7 million in fines.

---

**Florida International University, Miami, Florida**

Florida International University is in the process of sending notification letters to 19,407 students and 88 faculty members after the university's IT Security Office discovered personal data may have been exposed over the internet via a database's external search function. An announcement posted on the FIU website lists the personal data as GPAs, test scores, and Social Security numbers that were stored on the College of Education's E-Folio software app. This database kept track of student data related to state mastery standards, grade tracking, assignments, and Social Security numbers for both students and faculty.

**Information Source:** Dataloss DB

**June 22, 2010**

**Oregon National Guard, Portland, Oregon**

A laptop belonging to an Oregon National Guard member was stolen and the military is contacting service members who might be affected by the theft. According to the Oregon National Guard, the laptop was stolen from a vehicle. The Guard member had been using the laptop to conduct work from home. Although this laptop is password protected, there is still potential for exposure of individual personal information.

**UPDATE (7/1/10):** The 3,500 National Guard members who were affected have been notified.

**Information Source:** Dataloss DB

**June 21, 2010**

**TeleTech, Sony Electronics, Englewood, Colorado**

Customers who placed orders through Sony Style Telesales Department between May 23rd and June 3rd 2010 may have had their credit card information illegitimately copied and sent to parties outside of the TeleTech network. TeleTech is a third party service provider of Sony.

**Information Source:** Databreaches.net

**June 20, 2010**

**Mercy Willard Hospital, Willard, Ohio**
A former employee kept patient photographs, videos, memos, schedules, and forms. Some of the documents included patient Social Security numbers and other personal information. The employee is also being accused of voyeurism and possession of child pornography; though this is unrelated to these findings.

**Information Source:** PHIPrivacy.net

**June 18, 2010**  
**St. Francis Federal Credit Union**  
**Tulsa, Oklahoma**  
BSF  PORT  8,400

Saint Francis Federal Credit Union has notified 8,400 customers that a backup tape containing customer information was lost. SFFCU believes the tape was accidentally destroyed and that no member information has been misused as a result of the loss.

**Information Source:** Databreaches.net

**June 18, 2010**  
**University of Nevada**  
**Reno, Nevada**  
EDU  STAT  7,526

Some patient information from the University Health System may have been accessed after the theft of computer equipment at the Reno office on June 11th. Patient names, Social Security numbers, patient account numbers, medical information, birth dates and addresses may have been viewed.

**Information Source:** Databreaches.net

**June 18, 2010**  
**Family Care Center**  
**Clinton, Washington**  
MED  PORT  8,000 (0 SSNs reported)

Operations in Clinton, Freeland, and Oak Harbor were affected.

A thief or thieves entered the physical therapy office on June 12th. Cash, other items, and a laptop containing encrypted patient information such as names and account numbers were stolen. It appears that a door was left unlocked.

**Information Source:** PHIPrivacy.net

**June 18, 2010**  
**Ebony Medical Equipment and Supplies, Inc.**  
**Tyler, Texas**  
MED  INSD  Unknown

The owner used patient medical information to fraudulently obtain over $70,000 from Medicare and Medicaid. The owner is also charged with buying patient information.

**Information Source:** PHIPrivacy.net

**June 17, 2010**  
**Ocean Lakes High School**  
**Virginia Beach, Virginia**  
EDU  HACK  11,388

Schools that may have been accessed: Advanced Technology Center, Corporate Landing Middle School, Creeds Elementary School, Fairfield Elementary School, Indian Lakes Elementary School, Kellam High School, Kingston Elementary School, Landstown Middle School, Linkhorn Park Elementary School, Lynnhaven Middle School, New Castle Elementary School, Ocean Lakes Elementary School, Ocean Lakes High School, Red Mill Elementary School, Renaissance Academy, Rosemont Elementary School, Salem Elementary School, Technical & Career Education Center, Thalia Elementary School, Three Oaks Elementary School, Windsor Oaks Elementary School.

Over 11,388 students from schools listed on the Virginia Beach City County Public Schools page of publicschoolreview.com

Because of an incorrect security setting, an Ocean Lakes High School student was able to access a temporary file on a server that contained the names, addresses and Social Security numbers of students at 22 schools. The breach was discovered when the student tried to print some of the information in the school library. In addition to names, addresses and Social Security numbers, the student files also contain parent names, phone numbers, class schedules, birth dates and student ID numbers.

**Information Source:** Dataloss DB

**June 17, 2010**  
**Quantum Corporation**  
**Bellevue, Washington**  
BSR  PORT  Unknown

Laptops were stolen on June 13th. One of the laptops was password protected and contained sensitive employee information such as Social Security numbers, addresses, and names.
June 16, 2010  **AT&T**  
Dallas, Texas  
BSR  DISC  Unknown  

AT&T customers who were using their own usernames and passwords to log into their accounts reported being sent to the accounts of other AT&T customers. The account information did not include Social Security numbers or credit card information.

June 14, 2010  **Franklin County Treasurer’s Office**  
Columbus, Ohio  
GOV  DISC  0  

Although it has a newer and better protected website for paying property taxes, the Franklin County Treasurer’s Office continues to allow taxpayers to use an older URL which was recently discovered to be vulnerable to hackers. This may expose taxpayer credit card and checking account numbers.

June 13, 2010  **Butler County Department of Job and Family Services**  
Middle, Ohio  
GOV  PHYS  10,600  

The Agency learned in 2008 that confidential records were being left in public dumpsters without being shredded. Documents from Medicaid, Food Stamps, Ohio Works First, and child care programs included information such as Social Security number, name, address, phone number and pay stub. The agency failed to notify those who were affected.

June 12, 2010  **JP Morgan Chase**  
Hackettstown, New Jersey  
BSF  INSD  12  

A Chase bank teller sold twelve customer account profiles to outside parties between 2008 and 2009. These customer accounts were then fraudulently charged over $60,000. The former employee and the outside parties were all caught.

June 12, 2010  **Middle Township Municipal Hall**  
Middle Township, New Jersey  
GOV  PHYS  Unknown  

Personal information from Municipal Hall was found in a public dumpster. The information was not shredded and included police reports, Social Security numbers, home addresses, telephone numbers, names, and tax records. The improper disposal of information continued after the first dumpster discovery.

June 11, 2010  **Payless Shoe Store**  
Bellmore, New York  
BSR  INSD  11  

An employee used a skimming device to obtain customer credit card information. He made fraudulent purchases totaling nearly $11,000 and was charged with grand larceny, possession of a forged device, and identity theft.

June 10, 2010  **Durham County Government**  
Durham, North Carolina  
GOV  PHYS  8,700  

A group of people obtained a list of Durham employees which included Social Security numbers, birth dates, and employment information. They then used their personal information to commit credit card fraud and identity theft. Police report that more than 200 employees were victims.

June 10, 2010  **City of Springfield**  
Springfield, Illinois  
GOV  DISC  Unknown  

The city of Springfield put documents online that contained sensitive information such as Social Security numbers, driver’s license numbers, home and work telephone numbers, bank account numbers and the name of someone who called
the state anonymously to report suspected child abuse. The documents were posted on the city's website in response to Freedom of Information Act requests as part of an initiative to make public information available to anyone with a computer. But personal information such as home phone numbers, Social Security numbers and driver’s license numbers are exempt from disclosure under state law.

Information Source: Dataloss DB

June 9, 2010 Apple Inc., AT&T Cupertino, California BSR HACK

120,000 (No SSNs or financial information involved)

A security breach has exposed iPad owner information. Dozens of CEOs, military officials, and top politicians may have been affected. They—and every other buyer of the cellular-enabled tablet—could be vulnerable to spam marketing and malicious hacking. The breach exposed the most exclusive email list on the planet, a collection of early-adopter iPad 3G subscribers. It includes thousands of A-listers in finance, politics and media, from New York Times Co. CEO Janet Robinson to Diane Sawyer of ABC News to film mogul Harvey Weinstein to Mayor Michael Bloomberg. It even appears that White House Chief of Staff Rahm Emanuel’s information was compromised. It doesn’t stop there. According to the data given by the web security group that exploited vulnerabilities on the AT&T network, 114,000 user accounts have been compromised, although it’s possible that confidential information about every iPad 3G owner in the U.S. has been exposed.

UPDATE (01/18/2011): Chat logs of the accused iPad hackers were turned over to investigators. It appears that two men used an “account slurper” to conduct a “brute force” attack that lasted five days and extracted data from iPad users who accessed the Internet through AT&T’s 3G network. Each of the two men were charged with one count of conspiracy to access a computer without authorization and one count of fraud.

UPDATE (06/23/2011): One of the people responsible for writing the malicious code used to breach AT&T’s computer servers pleaded guilty to his part in the attack.

UPDATE (11/20/2012): The second person responsible for discovering and exploiting a security weakness was found guilty. AT&T iPad subscribers had their emails exposed because of the security issue.

UPDATE (03/19/2013): One of the conspirators was sentenced to 41 months in prison for identity theft and conspiracy to gain unauthorized access to computers.

Information Source: Dataloss DB

June 9, 2010 TennCare, New Mexico Human Services Department Chicago, Illinois MED PORT

76,000 (21,000 cases involving SSNs)

This theft affects people in Tennessee and New Mexico. Around 9,600 people from New Mexico and over 10,000 from Tennessee were affected.

An employee from a subcontractor company called West Monroe Partners was robbed of a laptop containing information for a Medicaid billing company named DentaQuest. DentaQuest was responsible for dental benefits of the New Mexico Human Services Department and TennCare. Around 21,000 people had their full names and Social Security numbers on the stolen laptop. Approximately 55,000 others had some form of personal information on the laptop.

Information Source: Databreaches.net

June 9, 2010 St. John’s Mercy Medical Group St. John, Missouri MED DISC

1,907

Patient files were found outside a doctor’s office. The doctor admitted to failing to shred the old papers and claimed that he ran out of space for the files.

UPDATE (8/25/10): Reports state that 1,907 patients were notified. The patient files included contact and credit card information, Social Security numbers and dates of birth.

Information Source: NAID

June 8, 2010 Bank of America Sun City, Florida BSF INSD

An employee in one of Bank of America’s customer call centers has admitted he stole sensitive account information and tried to sell it for cash. The man met with two individuals whom he later learned were undercover FBI agents and offered to sell them names, dates of birth, telephonic passwords, and other details for Bank of America customers, according to court records. He was looking for accomplices who knew how to milk the accounts by establishing phony credit cards in the customers’ names or through other means.
Employees shared patient information on Facebook. Differing reports leave it unclear if these employees were nurses, and whether or not they were fired.

A dishonest employee used welfare beneficiary information to file for two million dollars worth of tax refunds. The employee was caught and charged with 11 counts of identity theft and 11 counts of making false claims to the United States.

UPDATE (2/13/11): The former employee pleaded guilty to two counts of filing false claims against the United States.

Sam's Club and Wal-Mart stores in Connecticut, New Jersey, Massachusetts, Rhode Island, New Hampshire, New York, Pennsylvania, Maryland, Delaware, and Puerto Rico were affected.

During a credit card fraud scheme, a man obtained and misused customer information. His scheme involved using customer information to impersonate customers and open new lines of store credit in their names. Total loses amounted to $781,571.80.

The New York City's Special Commissioner Office revealed a hacker stole more than $640,000 from the Department of Education's petty cash account at JP Morgan Chase and distributed the codes to others to use to pay for student loans, gas bills and other purchases. The hacker allowed individuals to pay personal bills through EFTs and, in turn, he was given cash. The scam was discovered when an unidentified woman informed Chase someone was trying to pay bills using the account.

Over two thousand patient records, surgery information, Social Security numbers and bank information were found dumped behind Nashville Center Point Church of the Nazarene. The documents came from the now defunct and bankrupt Nursing Visioned Medical Services group. Maryland-based Impulse Monitoring, Inc. bought the assets to NVMS last year when they filed bankruptcy. They said they are not responsible for the patient information because the services NVMS provided were one-time services. The old owners had shredded a bunch of old documents and the more recent ones had been passed on to the company (Impulse) that bought NVMS back in January. It is unclear where the documents came from.

Confidential medical files were found in a dumpster near the medical office of the two doctors. The doctors were in the process of moving to a new location.
A limited search of NHTSA’s public complaint database uncovered Social Security numbers, names, birth dates, addresses, VINs, and drivers’ license numbers. Public access to the database of 792,000 complaint cases was temporarily ended.

**Information**  
**Source:** Databreaches.net  
**Date:** June 5, 2010  
**Company:** Marco’s Restaurant  
**Location:** Indianapolis, Indiana  
**Method:** BSR HACK  
**Count:** 500

The encrypted Internet connection of a restaurant was breached by hackers outside of the organization. Customer credit and debit card information was lost and fraudulently used.

**Information**  
**Source:** Databreaches.net  
**Date:** June 4, 2010  
**Company:** Digital River Inc.  
**Location:** Eden Prairie, Minnesota  
**Method:** BSF HACK  
**Count:** 200,000

A massive data theft from the e-commerce company Digital River Inc. has led investigators to hackers in India and a 19-year-old in New York who allegedly tried to sell the information to a Colorado marketing firm for half a million dollars. The Eden Prairie company obtained a secret court order last month to block Eric Porat of Brooklyn from selling, destroying, altering or distributing purloined data on nearly 200,000 individuals. Digital River suspects that the information was stolen by hackers in New Delhi, India, possibly with help from a contractor working for Digital River.

**Information**  
**Source:** Dataloss DB  
**Date:** June 3, 2010  
**Company:** Penn State  
**Location:** University Park, Pennsylvania  
**Method:** EDU DISC  
**Count:** 15,806, 25,000 more later discovered

The Pennsylvania State University sent data breach notification letters to 15,806 individuals who at one time had their personal information, including Social Security numbers, stored in a university database. Penn State issued a press release statement on Wednesday informing the university community that a computer in its Outreach Market Research and Data office was found to be actively communicating with a botnet CNC. According to the statement, the database used by the office had previously contained Social Security numbers on individuals. The university, which discontinued use of SSNs for identification purposes in 2005, nevertheless found that an archived copy of the information went undetected in the computer’s cache.

**UPDATE** (6/8/10): An additional 25,000 individuals may have been affected.

**Information**  
**Source:** Dataloss DB  
**Date:** June 3, 2010  
**Company:** Safe Harbor Med  
**Location:** Santa Cruz, California  
**Method:** MED PORT  
**Count:** Unknown

Burglars stole client records, a suitcase and two bags of cookies from a medicinal marijuana referral office. Burglars also stole a computer hard drive that contained a client database, including Social Security numbers, ID numbers and other sensitive information. The burglars apparently cut power to the building — so the alarm didn't go off — and shattered a window to get into the office.

**Information**  
**Source:** Dataloss DB  
**Date:** June 2, 2010  
**Company:** Avalon Center  
**Location:** Cheektowaga, New York  
**Method:** MED DISC  
**Count:** Unknown

Sensitive medical information was dumped outside of a DMV office. The medical information came from a eating disorder clinic that had recently closed. Patient information such as medical treatment and Social Security number was exposed. It is unknown how the information ended up in the dumpster.

**Information**  
**Source:** Databreaches.net  
**Date:** June 2, 2010  
**Company:** Rainbow Hospice and Palliative Care  
**Location:** Park Ridge, Illinois  
**Method:** MED PORT  
**Count:** Unknown

According to their website: "On April 12, 2010, one of our laptop computers, which contained personal information, was stolen during a patient visit. The laptop had security measures in place, but there is a very small chance that protected information such as name, address, date of birth, Social Security number, insurance information, medications, treatment, and diagnoses may have been inappropriately accessed."
June 2, 2010  Roanoke City Public Schools  Roanoke, Virginia  EDU  PORT  2000

Personal information of more than 2,000 Roanoke City Public Schools employees may be at risk. School officials said the hard drives of eight computers were not removed before the units were sold as surplus. “We believe that we have recovered all of the hard drives,” said Superintendent Rita Bishop. The drives contained the names, school locations and Social Security numbers of the division’s employees as of November 2006. The division will be setting up a hotline for employees to call with questions and concerns. Free credit monitoring service will be offered to affected employees.

June 2, 2010  University of Louisville  Louisville, Kentucky  EDU  DISC  709

A University of Louisville database of 708 names that included Social Security numbers and dialysis details was available on the Internet without password protection for nearly a year and a half. The Web site was disabled on May 17 when the university discovered the flaw. University officials said in a statement that accessing the database would not have been easy, and no direct links to the database were discovered. The information was available so long because the U of L doctor who set up the Web site thought the information was protected by a password and other precautions. U of L was finally notified when someone outside the university sent an e-mail about open access to the information. The Web site was shut down an hour later.

June 1, 2010  Brew HaHa!  Wilmington, Delaware  BSR  HACK  30

Outdated and improperly managed software caused customer debit and credit cards to be exposed to fraudulent charges. Between 20 and 30 customers of one bank had fraudulent charges from overseas added to their statements. It is not known how many other customers were affected.

May 28, 2010  Aetna  South Windsor, Connecticut  BSO  PHYS  6,372

The number of clients from New Jersey and Pennsylvania affected totals 6,372.

A cabinet full of documents with sensitive information was found sitting on the side of the road. A woman made the discovery about a month ago and gave the documents to investigators with Aetna Insurance Co. The woman said she saw a bureau on the side of the road in front of Admiral Storage in South Windsor with a sign that said “free.” She brought it home and discovered the documents. There were eight bags of nothing but Social Security numbers, names, and death benefits. Information also included patient records and medications. Aetna responded by saying, “Aetna is committed to protecting the privacy of our members and we take this situation seriously. We have policies for properly safeguarding our members’ information, and we are investigating how this incident occurred, but it appears to be human error. The woman contacted us via e-mail on the evening of May 5, and we immediately responded the next morning. She has consistently declined to give us her name or phone number, or to make arrangements to allow us to retrieve the documents at a place convenient for her, or to return them to us. As of today, we now have the files, and will go through each of them to determine the contents and whether any member information has been breached. If it has been, we will notify those members and take steps to mitigate any potential harm.”

The woman attempted to arrange the hand-off, however, a short time after she got off the phone with the company, three men from Aetna showed up at her workplace, unannounced, and asked for the documents immediately. The woman said, “But when they sent the three guys to my work yesterday, it was an intimidation tactic and I didn’t appreciate it. So that told me what I was going to do. That they were going to try and hide it.”

Aetna said someone from the company made a “serious human error,” and it will now go through the files to make sure no sensitive information was lost. What’s more troubling, the woman said, is that the bureau wasn’t the only piece of furniture offered for free that day. “Out of the pieces that were up for grabs, whose to say that I’ve got the only piece that was full of Aetna papers.” The woman has also contacted the state to investigate the situation. Aetna has clients across the country.

UPDATE (8/2/10): Aetna notified 7,250 clients of the breach and reported that 6,372 were affected.

May 28, 2010  Cincinnati Children’s Hospital Medical Center  MED  PORT  61,000 (0 SSNs and financial
A laptop containing the names, medical record numbers, and medical services provided of patients was stolen from an employee's car while it was parked at his or her home. As a precaution, no additional laptops will be allowed outside the hospital unless they are encrypted.

**Information Source:**
Databreaches.net

**May 28, 2010**
**Interior National Business Center**
**Denver, Colorado**
**GOV**  **PORT**  7,500 (0 SSNs reported)

A disc containing employee information was lost or stolen. The Interior Department reported that it was encrypted and password-protected personally identifiable federal employee information.

**Information Source:**
Databreaches.net

**May 26, 2010**
**Inovis**
**Alpharetta, Georgia**
**BSO**  **PORT**  Unknown

On May 4th a laptop containing employee information was stolen from an employee of GXS who was helping with their merger. A letter notified an unknown number of Inovis employees that their addresses, Social Security numbers, names and salary information were on the laptop.

**Information Source:**
Databreaches.net

**May 26, 2010**
**Children’s Hospital and Research Center at Oakland**
**Oakland, California**
**MED**  **DISC**  1,000 (0 SSNs reported)

http://www.childrenshospitaloakland.org/EnhancedPatientPrivacyProtection...

Approximately 1,000 patients received information about themselves and other patients in the mail. According to the Hospital’s website “equipment designed to generate, fold and stuff documents for mailing was programmed to fold and stuff two pages rather than one. This programming error caused guarantor billing statements prepared on May 25 and May 26 to be collated and mailed incorrectly."

**Information Source:**
PHIPrivacy.net

**May 25, 2010**
**Loma Linda University Medical Center**
**Loma Linda , California**
**MED**  **STAT**  584 (No SSNs or financial information reported)

(877) 558-6208

A thief has stolen personal information regarding more than 500 surgical patients of Loma Linda University Medical Center, according to hospital officials. A desktop computer containing the information disappeared April 5 from the department of surgery’s administrative office on Campus Street. The missing information includes each patient’s name, medical record number, diagnosis, surgery date, and the type of procedure.

**Information Source:**
Dataloss DB

**May 25, 2010**
**AT&T/Ferrell Communication**
**Jacksonville, Florida**
**BSO**  **DISC**  Unknown

A woman got quite a surprise when she looked in her recycle bin. Someone had dumped hundreds of files of people’s personal information. The manila folders that were found contained personal information of AT&T cell phone customers, including credit card numbers, driver’s licenses and Social Security numbers. It appears the information was collected by another company called Ferrell Communication, which was located in a strip mall. It’s no longer there, and the phone number listed isn’t valid. The information is contracts for AT&T wireless service customers dating back to 1999 or 2000. The information is old, but could still be valid.

**Information Source:**
Dataloss DB

**May 25, 2010**
**City of Charlotte**
**Charlotte, North Carolina**
**GOV**  **PHYS**  5,220
The city of Charlotte says the personal information of 5,220 current and former city employees and elected officials has been lost. The loss affects individuals who received health insurance from the city in early 2002. Two DVDs containing the Social Security numbers of the affected individuals failed to arrive at the offices of Towers Watson & Co., the city’s benefits consulting firm, in Atlanta. The discs also contained prescription-drug information for five individuals.

### Information Source: Dataloss DB

**May 25, 2010**  
**Local Coffee**  
**San Antonio, Texas**  
**BSR**  
**HACK**  
**Unknown**

Hackers may have gained access to credit and debit card information by exploiting Aloha software weaknesses. After a purchase at Local Coffee, a customer’s debit card was canceled. This prompted Local Coffee to temporarily stop using Aloha. Another San Antonio eating establishment, Aldaco, also encountered hacking problems while using Aloha software.

### Information Source: Databreaches.net

**May 25, 2010**  
**Lincoln Financial Group**  
**Radnor, Pennsylvania**  
**BSF**  
**DISC**  
**1,286 (0 SSNs reported)**

In 2002, 2008, and 2010 records of correspondence between agents and clients were misplaced. Technical errors caused the names, addresses, policies or contract numbers, account values, trade and transaction activities, and dates of birth of the clients to be accessible.

### Information Source: Databreaches.net

**May 25, 2010**  
**Wells Fargo**  
**San Francisco, California**  
**BSF**  
**INSD**  
**1,023**

A former stock broker left the firm with the personal information of 1,023 clients. Names, addresses, Social Security numbers and brokerage account numbers were taken.

### Information Source: Databreaches.net

**May 24, 2010**  
**Cheesecake Factory**  
**Washington, District Of Columbia**  
**BSR**  
**INSD**  
**Unknown**

Three servers from a Cheesecake Factory restaurant were charged with using skimming devices to make over $117,000 in fraudulent charges to customer credit card accounts.

### Information Source: Databreaches.net

**May 24, 2010**  
**Lake Ridge Middle School**  
**Woodbridge, Virginia**  
**EDU**  
**PORT**  
**1,200 (0 SSNs reported)**

A USB drive containing student names, identification numbers, phone numbers, and medical information was stolen from the unlocked car of a school administrator at the employee’s home. Over 1,200 students were affected.

### Information Source: Databreaches.net

**May 22, 2010**  
**Staff Jennings Boats**  
**Portland, Oregon**  
**BSR**  
**DISC**  
**Unknown**

Sales documents dating back 20 years were found in a dumpster. The personal financial information of customers included Social Security numbers and information on purchases. Staff Jennings went out of business in April of 2010.

### Information Source: Databreaches.net

**May 21, 2010**  
**Aldaco’s Mexican Cuisine**  
**San Antonio, Texas**  
**BSR**  
**HACK**  
**Unknown**

Aldaco’s Mexican Cuisine at Stone Oak had a data security breach. Customers were notified of fraudulent charges; some were from places outside of the U.S. Aldaco urged customers who had used their credit cards at the restaurant to cancel them.
May 21, 2010  
**Tufts University**  
*Medford, Massachusetts*  
EDU  
HACK  
2,000

Campus computers with former student files were exposed to a virus. Over two thousand alumni may have had their Social Security numbers and other information exposed.

May 20, 2010  
**Rockbridge Area Community Services**  
*Lexington, Virginia*  
MED  
STAT  
500

On March 3rd, at least one computer and one laptop containing personal information were stolen. Information such as names and Social Security numbers may have been compromised.

May 20, 2010  
**Strong Memorial Hospital**  
*Rochester, New York*  
MED  
DISC  
1250 (0 SSNs and credit cards involved)

Around half of all patient medical bills were sent to the wrong address. The billing statements included patient names, name and address of the person responsible for paying the bill, description of services received and the dates of services, dollar amount owed, health insurance plan and subscriber number. Around 1,250 patients were affected.

May 18, 2010  
**The Vine Tavern and Eatery**  
*Tempe, Arizona*  
BSR  
PHYS  
Unknown

Personal documents including applicant names, Social Security numbers, and dates of birth were found in a dumpster. Customer checks with banking information and credit card receipts were also found. Reports indicate that thousands of pages of information were located.

May 18, 2010  
**Capitol One**  
*McLean, Virginia*  
BSF  
UNKN  
Unknown

A fraud ring may have accessed customer information. The information included names, addresses, Social Security numbers, and other personal information. It is not known how the information was obtained or how many customers were affected. The information may have been accessed sometime between December of 2009 and February of 2010.

May 17, 2010  
**Edward Waters College**  
*Jacksonville, Florida*  
EDU  
DISC  
210

Over 210 staff and prospective student names, Social Security numbers, driver’s license numbers, and addresses were accessible to the public through a Google or Yahoo! search. The cause was a mistake in setting up software.

May 17, 2010  
**Silicon Valley Eyecare Optometry and Contact Lenses**  
*Santa Clara, California*  
MED  
STAT  
40,000

A computer and a plasma TV were stolen from the office on Friday April 2nd, 2010. The computer server contained patient names, addresses, phone numbers, email addresses, birth dates, family member names, medical insurance information, medical records, and in some cases, Social Security numbers. The data were password protected.

May 15, 2010  
**Los Angeles Firemen’s Credit Union**  
*Los Angeles, California*  
BSF  
DISC  
Unknown
An "extremely small percentage" of member files were not properly moved when the CU relocated from an old location. The data that could have been compromised included members' names, addresses, phone numbers, account numbers, Social Security numbers and other identifiers. The CU sought to reassure members that it did not believe any of their information had been compromised and that the CU had "state of the art protocols" available to validate member identifies. The CU also arranged for CU members who chose to do so to be able to enroll in a credit monitoring service for the next two years at no cost to them.

Information
Source: Dataloss DB
May 15, 2010 Mellow Mushroom
Warner Robins, Georgia
BSR HACK 2,000

Customers of the Mellow Mushroom eatery had their credit and debit card information hacked sometime around March 11th. Customers of other merchants have been affected, but a hack of Mellow Mushroom's processor is believed to be the source.

Information
Source: Databreaches.net
May 14, 2010 Department of Veterans Affairs
Washington, District Of Columbia
GOV PORT 616

The Department of Veterans Affairs has suffered another possible breach of private data as a thief recently stole an unencrypted laptop that had held the Social Security numbers and other information of 616 veterans. Theft of the laptop was owned by a contractor and not the VA.

Information
Source: Dataloss DB
May 14, 2010 Principal Financial Group
Des Moines, Iowa
BSF HACK Unknown

An unauthorized person using a valid employer password and user name accessed group contract number, member name, Social Security number, age and employment status of certain individuals with a connection to Principal Life Insurance.

Information
Source: Databreaches.net
May 13, 2010 Army Reserve/Serco Inc.
Morrow, Georgia
GOV PORT 207,000

A laptop containing the names, address and Social Security numbers of more than 207,000 Army reservists has been stolen from a government contractor in Georgia. A CD-Rom containing the personal identifiable information was in one of three laptops stolen from the Morrow, Ga., offices of Serco Inc., a government contractor based in Reston, Va. The other laptops did not contain sensitive personal information. Serco had a contract with the U.S. Army's Family and Morale, Welfare and Recreation Division, so some of the pilfered information also could belong to reservists' family members.

Information
Source: Dataloss DB
May 11, 2010 New Mexico Medicaid
Santa Fe, New Mexico
GOV PORT 9,500

(877) 453-8424

A employee of a subcontractor for the company that processes claims and provides dental benefits for the State's Medicaid program, filed a stolen car report for a vehicle whose trunk contained an "unencrypted" laptop loaded with patient information. The patient information in the laptop included name, health plan identification number, which in some cases is the individual's Social Security number, and a provider identification number but not the name of the provider. The agency sent out a message today saying that it was in the process of notifying 9,500 New Mexicans who use its Medicaid Salud plan of a possible security breach.

Information
Source: Dataloss DB
May 7, 2010 FHG Finance
Pleasant Hill, California
BSF DISC 300

The financial and personal details of about 300 property loan applicants were compromised when confidential documents were mistakenly tossed into an outdoor waste bin. The documents, which contained bank account and Social Security numbers, were found by employees at a neighboring store, who alerted FHG. The company padlocked the trash bin until the documents could be shredded.

Information
Source: Dataloss DB
May 7, 2010  Fast Cash  Knoxville, Tennessee

Hundreds, maybe thousands, of documents with personal information were dumped behind a shopping center. The documents scattered around a dumpster behind the business listing Social Security numbers, names, addresses, bank account numbers and signatures.

Information
Source: Dataloss DB

May 7, 2010  Bureau of Engraving and Printing  Washington, District Of Columbia

Hackers have caused the Bureau of Engraving and Printing (BEP), a part of the US Department of the Treasury, to shut down a number of websites. The BEP confirmed to IT PRO that the hosting company it uses experienced an intrusion and as a result of the breach numerous websites were affected, including non-BEP sites. Those URLs are: bep.gov; bep.treas.gov; moneyfactory.gov and moneyfactory.com. BEP has since suspended the website. The chief research officer at IT security company AVG, indicated that the BEP websites had a line of code injected into them. Upon accessing the US Treasury website (treas.gov, bep.gov, or moneyfactory.gov), the iframe silently redirects victims through statistic servers and exploit packs which will carry the victim onto the second stage of the attack. The exploit kit determined that Java was the “best method” for infecting his test machine. Once infected, users’ web browsers will start directing them to ads and “other nasty things” like rogueware.

Information
Source: Dataloss DB

May 4, 2010  Millennium Medical Management Resources  Westmont, Illinois

Health records belonging to patients were stolen in a break-in. The records were on a portable hard drive and stolen from the Westmont office of Millennium Medical Management Resources. Millenium believes the hard drive contained personally identifiable information about EHP patients including name, address, phone, date of birth, and Social Security number. In some cases other information such as diagnosis, procedure (and/or codes), medical record number, account number, drivers license number and health insurance info. It was NOT encrypted.

Information
Source: Dataloss DB

April 30, 2010  Our Lady of Peace  Louisville, Kentucky

A flash drive containing personal information on 24,600 patients is missing from Our Lady of Peace psychiatric hospital. The drive contained the following information on patients admitted since 2002: patient names, room numbers, insurance company names and admission and discharge dates. It didn’t include diagnoses or treatments, Social Security numbers, dates of birth, telephone numbers or addresses for these patients. The drive also included the following information on patients assessed since 2009 but never admitted: name, date of assessment, date of birth and the time they left the hospital. For these patients, the information on the drive didn’t include diagnoses or treatments, Social Security numbers, telephone numbers, addresses or insurance information.

Information
Source: Dataloss DB

April 30, 2010  North Country Health Services  Bemidji, Minnesota

The online bill payment website was hacked. The credit card and debit card account information of customers who paid online was exposed.

Information
Source: PHIPrivacy.net

April 29, 2010  St. Jude Heritage Medical Group  Orange, California

(800) 627-8106

20,000 patients may have had their personal information stolen after a break-in at the St. Jude Heritage Healthcare Clinical Management Services building in Fullerton. The thieves stole five computers. The stolen patient data included Social Security numbers, dates of birth and in some cases, health related information.

Information
Source: Dataloss DB

April 28, 2010  The Medical Center  Bowling Green, Kentucky

527
The Medical Center at Bowling Green is notifying 5,418 patients whose medical information may have been breached when a computer hard drive was stolen. The computer hard drive was taken from the hospital’s mammography suite and contained information from patients who underwent bone density testing between 1997 and 2009.

Information Source: Dataloss DB
April 28, 2010  Montana Tech  Butte, Montana

A Montana Tech employee mistakenly included the personal information of former students in an e-mail message sent to faculty, staff and students last week. The e-mail was an invitation to watch students present their research projects. But the file that this year’s information was taken from included the names, addresses, Social Security numbers and in some cases birth dates of students whose research projects were done from 1998 through 2005.

Information Source: Dataloss DB
April 28, 2010  Accretive Health  Roseville, Minnesota

An employee’s laptop was stolen from a rental car that was left unattended in a restaurant parking lot. The theft occurred on June 2, 2010. The laptop was rendered inoperable within two hours of the discovery of the theft. It contained data related to Fairview health system billing issues and was encrypted.

Information Source: PHIPrivacy.net
April 26, 2010  South Carolina Department of Health and Environmental Control  Columbia, South Carolina

Over 1,824 people’s information was found in a dumpster. It is not known what kind of personal information was included in the documents.

Information Source: NAID
April 26, 2010  Child Protective Services, Texas Department of Family and Protective Services  Austin, Texas

An administrative technician working for Child Protective Services under the Texas Department of Family and Protective Services misused the personal information of at least 70 adoptive and foster parent applicants. The dishonest employee would exchange the information for gifts and money and another person used the information to make fake drivers’ licenses. This allowed fraudulent credit card accounts to be opened in victims’ names. Both people were caught.

Information Source: Databreaches.net
April 23, 2010  ESB Financial  Ellwood City, Pennsylvania

ESB Financial officials announced that a data backup seven years ago had inadvertently been sent to an unauthorized storage source. Only checking and money-market account information was backed up to the incorrect outside data-storage company. A total of 3,097 customers could have been affected by the backup. Names, addresses, account numbers and, in some cases, Social Security numbers, would have been available to someone who found them on the Internet. However, the jumble of numbers would not have been easily recognizable and ESB was not identified as the source of the information.

Information Source: Dataloss DB
April 23, 2010  Blippy.com  Palo Alto, California

Blippy is a social Web service that lets users share with the world all their credit card transactions. One big problem though: Blippy appears to have inadvertently published some of its users’ credit card numbers. Google search resulted in viewing of some of the credit card numbers.

Information Source: Dataloss DB
April 23, 2010  Chattanooga State  Chattanooga, Tennessee
Nearly two thousand students records from Chattanooga State are missing. The company hired to scan the documents, mishandled them. The school took the records to a company, United Imaging in Walker County, where the papers would be converted to computer discs. The school was contacted by individuals who said there was something aawry going on at this scanning site. That's when the school found their records in disarray, and brought them back. The papers included students' names, Social Security numbers, addresses, phone numbers, some even contained high school transcripts. Chattanooga State went through each item, hand by hand, and found nearly 2000 missing documents from 2007.

Information
Source: Dataloss DB
April 23, 2010 DRC Physical Therapy Plus
Monticello, New York

Officials have seized hundreds, perhaps thousands, of files containing Social Security numbers and other private patient information found dumped outside the shuttered office of DRC Physical Therapy Plus. The manila folders, dating back to at least 1998, include information sheets showing the names, addresses and birth dates of patients and, in some cases, Social Security numbers. Deputies impounded a dump truck loaded with patient files and about a dozen or so boxes stacked inside the bucket of a front-loader.

Information
Source: Dataloss DB
April 23, 2010 Hutcheson Medical Center
Chattanooga, Tennessee

Anyone who peered inside the mixed paper bin at the Dupont Recycling Center in May of 2009 got an eyeful. Files, in plain sight, which contained sensitive medical and identity information. Authorities don't know how those thousands of files got there. Some of the records came from Hutcheson and a plastic surgery office in the area. The information inside those files included graphic photos, and Social Security numbers.

Information
Source: Dataloss DB
April 22, 2010 JE Systems Inc.
Fort Smith, Arkansas

The company in Arkansas lost more than $110,000 this month when hackers stole the firm's online banking credentials and drained its payroll account. On Wednesday, Apr. 7, Ft. Smith based JE Systems Inc. received a call from its bank stating that the company needed to move more money into its payroll account. Over the course of two days, someone had approved two batches of payroll payments — one for $45,000 and another for $67,000. A few days later, the First National Bank of Fort Smith sent JE Systems a letter saying the bank would not be responsible for the loss. It was their internet address that was used to process the payments, and their online banking user name and password.

Information
Source: Dataloss DB
April 21, 2010 Massachusetts Eye and Ear Infirmary
Boston, Massachusetts

On February 19, 2010, a laptop belonging to a physician affiliated with the Massachusetts Eye and Ear Infirmary was stolen while the physician was lecturing in South Korea. The laptop belonged to a neurologist with a particular focus on ringing in the ears, or tinnitus. The following types of information about affected individuals associated with Mass. Eye and Ear may have been present on laptop, names, addresses, telephone numbers, emails, date of birth and age, sex, medical record numbers, dates of service, medical information, including diagnoses, symptoms, test results, and prescriptions, name and contact information for patient pharmacies, and research participant status. In addition, four individuals' information also included their pharmacy insurance account number.

UPDATE (09/17/2012): Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates Inc. agreed to pay the U.S. Department of Health and Human Services (HHS) $1.5 million to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. An HHS Office for Civil Rights investigation indicated that Mass. Eye and Ear failed to take necessary steps to comply with certain requirements of the Security Rule. These steps include conducting a thorough analysis of the risk to the confidentiality of electronic protected health information (ePHI) maintained on portable devices, implementing security measures sufficient to ensure the confidentiality of ePHI that Mass. Eye and Eye created, maintained, and transmitted using portable devices, adopting and implementing policies and procedures to restrict access to ePHI to authorized users of portable devices, and adopting and implementing policies and procedures to address security incident identification, reporting, and response. Mass. Eye and Eye will also have to adhere to a corrective action plan to address these issues. The full HHS disclosure can be read here: http://www.hhs.gov/news/press/2012pres/09/20120917a.html

Information
Source: Dataloss DB
April 21, 2010 US Army Reserve
Fort Totten, New York

The Army is warning about 12,000 military and civilian personnel once associated with a reserve command based at Fort Totten that they should check their credit records, after discovering that it cannot locate files containing information
that could make them vulnerable to identity theft. The records cover reservists from Long Island, New York City and upstate who were assigned to the 77th Regional Readiness Command and its subordinate units from 2001 until the unit was absorbed by the 99th Regional Support Command in 2008. The files were discovered missing when the new command asked for an accounting of the old unit’s records. They could have been burned, shredded or stolen.

Information
Source: Dataloss DB

April 21, 2010 Affinity Health Plan
Bronx, New York MED PORT 409,262

Affinity Health Plan, a New York managed care service, is notifying more than 400,000 current and former customers employees that their personal data might have been leaked through the loss of an unerased digital copier hard drive. Some personal records were found on the hard drive of a copier found in a New Jersey warehouse. The copier had previously been leased by Affinity and was then returned to the leasing company. Affinity Health Plan says it has not had a chance to review the data found on the copier. The figure of 409,262 notifications includes former and current employees, providers, applicants for jobs, members, and applicants for coverage.

UPDATE (08/15/2013): Affinity Health Plan will pay more than $1.2 million in HIPAA violations as a result of the breach.

Information
Source: Dataloss DB

April 21, 2010 Brooke Army Medical Center
San Antonio, Texas MED PORT 1,272

An Army three-ring binder that may have included detailed information on soldiers and families being treated at Brooke Army Medical Center was stolen on Oct. 16 from a car belonging to a case manager. Names, phone numbers and health information of 1,272 patients being treated at hospitals may have been breached by the car break-in.

Information
Source: Dataloss DB

April 21, 2010 St. Mary and Elizabeth Hospital Women’s Center
Louisville, Kentucky MED STAT 77 (0 SSNs reported)

A hard drive was stolen from a locked area. Medical information such as biopsy images, patient names, and medical exams were on the stolen hard drive.

Information
Source: PHIPrivacy.net

April 18, 2010 Rapid Return Tax
San Antonio, Texas BSF PHYS Unknown

Dozens of legible tax documents were found among ashes in a dumpster outside of a tax return business. Social Security numbers may have been on the documents. This appears to be the result of a failure to burn all of the documents.

Information
Source: Databreaches.net

April 16, 2010 Blue Cross and Blue Shield of Rhode Island (BCBSRI)
Providence, Rhode Island MED PHYS 12,000

A filing cabinet containing survey information from approximately 12,000 BlueCHIP for Medicare members was donated to a local nonprofit organization. The surveys were from 2001 to early 2004 and contained information such as names, Social Security numbers, telephone numbers, addresses and Medicare Identification numbers.

Information
Source: Databreaches.net

April 16, 2010 Higher Education Services Corp.
Albany, New York BSR DISC 1,433

A “process error” may have lead to Social Security numbers and last names going through Internet servers outside of HESC’s control. Those who may have been affected received letters and free credit monitoring services.

Information
Source: Databreaches.net

April 16, 2010 General Motors
Detroit, Michigan BSR DISC Unknown

An electronic file containing Social Security numbers, names and email addresses was accidently sent.
A service provider lost an unencrypted DVD with employee names and Social Security numbers.

Customer information was sent to the wrong agent. The format of the information is unknown. The information included names and Medicare numbers.

An employee at the call center was inappropriately accessing customer names, billing addresses, credit card numbers and CVVs.

The location listed is DuPont’s headquarters. DuPont and BMI merged in 2005.

The Tatum division of SFN (Strategic Workforce Solutions) notified employees that a portable electronic device was stolen from the trunk of a car. The device contained unencrypted files with names, addresses and Social Security numbers.

A laptop containing the information of people regularly employed at Lam Research Corp. on or after January 1, 2009 was stolen from an employee’s car. Temporary employees and contractors from August 1, 2007 and beyond may have also been affected. The information included names and Social Security number; however, it was protected by passwords and fingerprints checks.

Up to 800 police files were left in an area where the general public could easily access them. Some of the files contained Social Security numbers, patient addresses, and treatment information.

At least eight human services employees, including supervisors, have been fired or disciplined in the past year for
wrongfully accessing confidential and personal information about former employees, family members and clients. The violations include a boss who forced her employees to gather information from a state database about her husband's child and a worker who checked on the status of a dead client's Medicaid benefits to help the client's family. Most of the cases stemmed from the agency's financial assistance department, which handles food stamps, Medicaid assistance, grants for the disabled and emergency relief for needy families. As part of their jobs, the 330 employees in the department who provide social services have varying degrees of access to secured databases. They need the information to determine whether a client qualifies for financial help.

Information Source: Dataloss DB
April 13, 2010 St. Peter's Hospital Albany, New York MED INSD Unknown

An East Greenbush man who worked as a medical records clerk at St. Peter’s Hospital is accused of stealing personal information from patient's files to open credit card accounts. The man allegedly stole Social Security numbers and other personal information from patient’s records, then used the data to open credit card accounts for making personal purchases online. The man was charged April 12 with five counts of felony second-degree forgery, three counts of felony second-degree identity theft and three counts of misdemeanor second-degree criminal impersonation.

Information Source: Dataloss DB
April 13, 2010 Lorillard Tobacco, General Agencies Welfare Benefits Program, National Gypsum, Towers Watson Greensboro, North Carolina BSR PORT 1,874

Two unencrypted DVDs containing employee information were lost in transit by a benefits consulting firm. Multiple organizations were involved. Benefits consulting firm Towers Watson notified Lorillard and the General Council on Finance and Administration, which administers the General Agencies Welfare Benefits Program, of the loss in February. The DVDs contained names, addresses, dates of birth, and Social Security numbers of current and former employees and their family members.


Information Source: Databreaches.net
April 13, 2010 Room Store Annapolis, Maryland BSR PHYS Unknown

A Maryland man found his own credit application lying on the ground near a dumpster. The dumpster contained thousands of old credit applications and some newer ones. The information included Social Security numbers, driver's licence numbers, names, addresses, and phone numbers. Room Store employees were doing a massive cleanup and unknowingly dumped the bag of documents without shredding them.

Information Source: Databreaches.net
April 13, 2010 Atlanta Firefighters Atlanta, Georgia GOV DISC 1000

While attending a seminar on security, Atlanta police officers were astonished to discover that personal information from city firefighters was being used as an example of what could be found on the Internet. The information included Social Security numbers, names and addresses. It is believed that the information was hacked and/or uploaded to a file sharing website from a city employee’s off-site laptop.

Information Source: Databreaches.net
April 12, 2010 Kern County Employee's Retirment Association Bakersfield, California GOV INSD 37,000

A former employee was convicted of using the Social Security number of a member to create a false identity. The county employee opened a line of credit and had committed felonies before being hired at KCERA in a position with access to retirees' personal information.

Information Source: Databreaches.net
April 9, 2010 Hollywood Video Sparks, Nevada BSR PHYS Unknown

This Hollywood Video like many others has closed. Hundreds, perhaps thousands of pieces of paper, receipts, records and worst of all membership forms, were exposed. It appears they were not even placed in the dumpster, but left out in the open and scattered everywhere by the wind. On these forms were names, addresses, birth dates, I-D numbers, credit card numbers and signatures.
Police have received about 80 complaints of victims' whose credit cards have been compromised. The police have connected the scam to cards used at the Mad Capper Saloon & Eatery. The owner of the Mad Capper Saloon & Eatery has been cooperating with police, he is frustrated that somehow his 30-year-old business is linked to identity theft. The restaurant’s owner, has taken steps to make sure his customers are protected. “We’ve looked into our credit card processing. We’ve looked into our software program -- our routers in the building, We’ve scanned everything -- combed it with a fine tooth comb and we can't find anything off of it, so its frustrating.”

**UPDATE (4/10/10):** The number of people affected is now nearing 200.

**Information**
**Source:** Dataloss DB  
**April 9, 2010**  
**Mad Capper Saloon & Eatery**  
**Stillwater, Minnesota**  
**BSR**  
**HACK**  
**200**

A Russian national was sentenced to 37 months in prison for hacking into victims' brokerage accounts at Charles Schwab, laundering more than $246,000 and sending a portion back to co-conspirators in Russia. The man also sold approximately 180 stolen credit card numbers to a cooperating witness and directed that they be fabricated into credit cards. According to the indictment, from approximately September 2006 through December 2007 two men participated in a scheme to steal funds from bank and brokerage accounts by hacking into those accounts through the Internet, using personal financial information obtained through a Trojan computer viruses and then laundering the stolen proceeds.

**Information**
**Source:** Dataloss DB  
**April 9, 2010**  
**Charles Schwab**  
**Albany, New York**  
**BSF**  
**HACK**  
**Unknown**

A USB containing client names, Social Security numbers, addresses, and dates of birth went missing. The data was unencrypted. Woodbury is a broker with The Hartford.

**Information**
**Source:** Databreaches.net  
**April 9, 2010**  
**Woodbury Financial Services**  
**Woodbury, Minnesota**  
**BSF**  
**PORT**  
**Unknown**

A Sand Springs woman has been indicted on allegations that she used personal identifying information she copied from her then-employer’s computer system as part of a scheme involving fraudulent credit cards and stolen mail. The indictment was released Wednesday in federal court in Tulsa and states that the 45 year old woman exceeded her computer-access authority at St. Francis Hospital to obtain information such as Social Security numbers and dates of birth of at least 60 people.

**UPDATE (11/24/10):** A second woman was sentenced for her role in the credit card fraud case. Both women had been employed at Saint Francis. Patient names, Social Security numbers and addresses obtained between August 6 and December 28 of 2009 were used to illegally obtain credit cards.

**Information**
**Source:** Dataloss DB  
**April 8, 2010**  
**St. Francis Hospital**  
**Tulsa, Oklahoma**  
**MED**  
**INSD**  
**60**

Police are investigating whether former H&R Block employees received fraudulent tax refunds by using customer information. At least customers 20 have come forward, but there could be many more customers who were affected.

**Information**
**Source:** Databreaches.net  
**April 8, 2010**  
**H&R Block**  
**Bronx, New York**  
**BSF**  
**INSD**  
**20**

A security breach resulted in the possibility that hackers accessed customer names, addresses, credit card information, email addresses and phone numbers. Customers who used the site between December 1, 2009 and February 10th, 2010 may have been affected.

**Information**
**Source:** Databreaches.net  
**April 8, 2010**  
**HBDirect.com**  
**Waterbury Center, Vermont**  
**BSO**  
**HACK**  
**Unknown**

A Sand Springs woman has been indicted on allegations that she used personal identifying information she copied from her then-employer’s computer system as part of a scheme involving fraudulent credit cards and stolen mail. The indictment was released Wednesday in federal court in Tulsa and states that the 45 year old woman exceeded her computer-access authority at St. Francis Hospital to obtain information such as Social Security numbers and dates of birth of at least 60 people.

**UPDATE (11/24/10):** A second woman was sentenced for her role in the credit card fraud case. Both women had been employed at Saint Francis. Patient names, Social Security numbers and addresses obtained between August 6 and December 28 of 2009 were used to illegally obtain credit cards.

**Information**
**Source:** Dataloss DB  
**April 8, 2010**  
**H&B Direct**  
**Waterbury Center, Vermont**  
**MED**  
**INSD**  
**60**

A Sand Springs woman has been indicted on allegations that she used personal identifying information she copied from her then-employer’s computer system as part of a scheme involving fraudulent credit cards and stolen mail. The indictment was released Wednesday in federal court in Tulsa and states that the 45 year old woman exceeded her computer-access authority at St. Francis Hospital to obtain information such as Social Security numbers and dates of birth of at least 60 people.

**UPDATE (11/24/10):** A second woman was sentenced for her role in the credit card fraud case. Both women had been employed at Saint Francis. Patient names, Social Security numbers and addresses obtained between August 6 and December 28 of 2009 were used to illegally obtain credit cards.

**Information**
**Source:** Databreaches.net  
**April 8, 2010**  
**H&B Direct**  
**Waterbury Center, Vermont**  
**MED**  
**INSD**  
**60**

A Sand Springs woman has been indicted on allegations that she used personal identifying information she copied from her then-employer’s computer system as part of a scheme involving fraudulent credit cards and stolen mail. The indictment was released Wednesday in federal court in Tulsa and states that the 45 year old woman exceeded her computer-access authority at St. Francis Hospital to obtain information such as Social Security numbers and dates of birth of at least 60 people.

**UPDATE (11/24/10):** A second woman was sentenced for her role in the credit card fraud case. Both women had been employed at Saint Francis. Patient names, Social Security numbers and addresses obtained between August 6 and December 28 of 2009 were used to illegally obtain credit cards.
Montgomery County’s Department of Health and Human Services is looking into how numerous Wheaton nursing home papers containing sensitive patient information have made their way into nearby neighbors’ yards over the past few months. The county sent a nursing home inspector to investigate complaints from residents in the Wheaton Regional Park Civic Association who said they have found internal documents from the nearby ManorCare Health Services that contain patient conditions, names and Social Security numbers. The inspector cited ManorCare for inappropriate conduct.

Information Source: Dataloss DB
April 8, 2010 Private Dental Practice San Clara, California
MED INSD 20

Dishonest employees who worked at an unnamed dental office and an unnamed law office in the Bay Area were part of an identity theft ring. A total of seven people are facing charges for their involvement in the ring. The charges include identity theft, conspiracy, possession of stolen property, and grand theft. Over $170,000 in cash and fraudulent purchases was taken through the use of sensitive patient and client information from the dental office and law office.

UPDATE (9/06/2011): The former employee of the dental office was sentenced. He will serve four years in prison for supplying patient information between June and December of 2009. The information was then used to create false driver’s licenses and to file illegal change-of-address forms.

Information Source: PHIPrivacy.net
April 7, 2010 Bank of America Charlotte, North Carolina
BSF INSD Unknown
An IT staff member of Bank of America pled guilty to installing illegal software on Bank of America ATMs. The software caused the ATMs to erroneously dispense money; some of it may have affected customer accounts.

Information Source: Databreaches.net
April 6, 2010 Pediatric Sports and Spine Associates Brentwood, Tennessee
MED PORT 955
A laptop was stolen from an employee on February 10. The theft occurred off-site. The laptop contained names, addresses, phone numbers, dates of birth, medical information and Social Security numbers.

Information Source: PHIPrivacy.net
April 6, 2010 Providence Hospital Southfield, Minnesota
MED PORT 12
The hospital has sent letters alerting patients that a hard drive used for backing up data has been “lost or stolen from a locked office suite. The hospital explained that the data included patient names, medical record numbers and/or clinical information, addresses and phone numbers of some employees, and what the hospital called proprietary businesses information. The hospital would not comment on how many patients may be affected, but said only 12 patients’ Social Security numbers were on the hard drive.

Information Source: Dataloss DB
April 5, 2010 John Muir Physician Network Walnut Creek, California
MED PORT 5,450
John Muir Health, the Walnut Creek-based hospital system, has begun notifying 5,450 patients by mail of a potential breach of their personal and health information. Two months ago two laptop computers at the John Muir Physician Network Perinatal office in Walnut Creek were stolen. The laptops were password protected and contained data in a format that would not be readily accessible. External vendors and internal experts discovered that the missing laptops contained personal and health information going back more than three years.

Information Source: Dataloss DB
April 3, 2010 Middletown City Government Building: Public Works, Utilities, Police, and Finance Departments Middletown, Ohio
GOV PHYS Unknown
Personal documents that originated from the city building were left in a dumpster. Most of the documents were from the public works and utilities departments. An unknown number of Middletown residents had their Social Security numbers, phone numbers, and carbon copies of checks exposed.

Information Source: Databreaches.net
More than 200 employees were notified that a non-government entity may have seen their personal information. The non-government entity were lawyers for two of three workers who fought a security access suspension against them. It took the Navy 17 months to inform employees at the Naval Facilities Engineering Service Center in Port Hueneme, California, that their Social Security numbers had been inadvertently released.

Information Source: Dataloss DB

March 30, 2010 Three Rivers Community College Norwalk, Connecticut

Three Rivers Community College may have suffered a security breach due to unauthorized access to its computer network. Data made vulnerable in the breach included names and Social Security numbers. Those affected would have been involved in the following programs during these years:
1997-2009: Participants in the Real Estate programs
2004-2009: Participants in the Life Long Learners programs
2003-2006: Participants in the Patient Care Technicians programs
2004-2006: Participants in the Certified Nursing Assistant programs
2004-2005: Participants in the Electric Boat academic programs
2007-2008: Participants in the Bridges to Health Care Careers programs
2006-2008: Participants in the Photons for Educators programs
2004-2009: Faculty or staff members of the Three Rivers Continuing Education office.

Information Source: Dataloss DB

March 30, 2010 Boulder Community Hospital, Family Medical Associates Lafayette, Colorado

Anonymous letters were sent to at least 14 patients of the Family Medical Associates clinic in Lafayette. The letters contained Social Security numbers, medical records, dates of birth and names. The sender claimed that the clinic was improperly disposing patient personal information.

Information Source: PHIPrivacy.net

March 30, 2010 Proxima Alfa Investments LLC New York, New York

In November the firm discovered that several backup tapes were missing from its office. The tapes contained customer information such as names, e-mail addresses, addresses, phone numbers, Social Security numbers, bank account information, passport numbers and sometimes scans of passports. The firm ceased operations in mid-2009.

Information Source: Databreaches.net

March 29, 2010 University MRI Diagnostic Center, Holy Cross Hospital, North Ridge Medical Center, and Oncology and Hematology Associates of West Broward, Florida

People in Fort Lauderdale, Aventura and Tamarac, Florida were affected. The hospital’s information hotline is (800) 388-4301.

The Holy Cross Hospital breach has its own post for November 10, 2010.

Two former employees of these organizations were involved in an identity theft scheme with at least three other partners. Thousands of victims have been confirmed. The employees had access to emergency room patient records such as names, dates of birth, Social Security numbers, Medicare numbers, and addresses. The stolen information was used by others to obtain Care Credit accounts and Chevron Visa credit cards. Victims lost a total of approximately $162,000.

Information Source: Databreaches.net

March 29, 2010 Griffin Hospital Derby, Connecticut

A former employee appears to have continued accessing patient names, medical information, dates of birth and medical record numbers. Patients received soliciting phone calls from a physician at another hospital.

UPDATE (06/212012): The physician and radiologist responsible for the breach has been fined $20,000 for downloading patient information and using it to promote radiology services at Advanced Mobile Imaging Radiology.
Thousands of medical documents fell out of a truck bed while in transit. The scattered documents contained billing information and possibly medical records from 1993 or later.

ECMC, a guarantor of federal student loans, said that a theft has occurred from its headquarters involving portable media with personally identifiable information. The data was in two stolen safes and contained information on approximately 3.3 million individuals and included names, addresses, dates of birth and Social Security numbers. No bank account or other financial account information was included in the data.

UPDATE (4/16/10): The information was recovered shortly after the theft and discovered weeks later in a police evidence room.

A 21-year-old former Evergreen Public Schools student has pleaded guilty to criminal charges in connection with a computerized payroll security breach that put more than 5,000 past and current Vancouver district school employees at risk of identity theft. The man had "shoulder-surfed" a password from an Evergreen school employee while still a student there.

The Cook County Sheriff's Department has uncovered an identity theft ring, a limited part of which may involve an employee of Millard Cleaning Service, the service contracted to clean the Foundation's offices. The suspect may have stolen information from paper records, including names, dates of birth, Social Security numbers, and addresses. NMFF has reviewed the Sheriff's Department's list of identity theft victims in Illinois and other states. It has identified approximately 65 people who were recent patients of NMFF, and it is contacting those who are known identity theft victims and offering assistance. While the Sheriff's Department has identified hundreds of other identity theft victims, the majority of them have no connection to NMFF and their personal information was not stolen from NMFF.

UPDATE (3/25/10): At least seven individuals linked to the Millard Cleaning Service janitor have been connected to the theft ring.

Two employees from the New York City office

Seven people, including two former New York State DMV employees from New York City, were indicted in a theft ring. The identify fraud ring involved New York State driver's licenses, learner's permits, and identification cards. The information was then sold to felons. Fifteen other people were charged with buying the stolen information.
A student gained access to the entire district of Hart’s system, but only went into his high school’s portion. The student claimed he changed some things and then returned them. The student most likely used a password, but it is not known whether he used a district computer or a personal one. The district is providing one year of free credit monitoring services.

Information
Source: Databreaches.net
March 25, 2010 Yuma Proving Ground
Yuma, Arizona
GOV HACK 700

A home computer that contained personnel data may have picked up a virus from the Internet. This breach puts employee names and Social Security numbers at risk.

Information
Source: Databreaches.net
March 25, 2010 Johns Hopkins University School of Education
Baltimore, Maryland
EDU DISC Unknown

A file containing student enrollment information was accessible online. Student names, races, genders, Social Security numbers, identification numbers and dates of birth were accessible for at least one month.

Information
Source: Databreaches.net
March 24, 2010 Wachovia
Alexandria, Washington
BSF CARD Unknown

A skimming device was spotted outside a Wachovia branch in Alexandria, Washington. It is estimated that over $60,000 in fraudulent charges was stolen from ATM customers of the Wachovia King Street branch.

Information
Source: Databreaches.net
March 23, 2010 H&R Block
Chicago, Illinois
BSF INSD 60

After Highland, Ind., police pulled over a driver for suspicion of driving under the influence. A search of the car uncovered a treasure-trove of evidence: a file box full of H&R Block client information, numerous blank W-2 forms, more than 100 debit cards and yellow legal pads with columns of Social Security numbers, PIN numbers, dates of tax filings and whether the returns had been accepted or rejected. The two women stole the identities of more than 60 H&R Block customers from the East Chicago branch. Fraudulent tax returns were then filed in their names since January, and refunds went to bank accounts set up by the two, the complaint alleged. IRS agents have found 17 bank accounts with deposits totaling almost $290,000.

Information
Source: Dataloss DB
March 23, 2010 Connecticut Office of Policy and Management
Hartford, Connecticut
GOV INSD 11,000

Police are investigating the theft of personal information — including Social Security numbers, names and addresses — from as many as 11,000 people who had applied for furnace rebate programs with the state. The investigation by Hartford and state police has led them to a woman who worked at the state Office of Policy and Management from May 2008 until May 2009. There have been no arrests. The state collected Social Security numbers because the refunds are federally taxable and the state was required to send a 1099 tax form to the recipients.

Information
Source: Dataloss DB
March 23, 2010 Montefiore Medical Center
Bronx, New York
MED PORT 625 (Unknown number of SSNs and financial accounts)

A laptop containing private health information was stolen on February 20th.

Information
Source: PHIPrivacy.net
March 22, 2010 Arkansas Crime Information Center
Little Rock, Arkansas
BSO INSD Unknown
It appears that the owner of a bail bonds business accessed criminal, family, and financial background information by misusing a police password. The Arkansas Crime Information Center database was fraudulently accessed 1,200 times in less than one year.

**Information Source:**
Databreaches.net

**March 22, 2010**
**Yuma Proving Ground**
**Yuma, Arizona**

The personal information of more than 700 Yuma Proving Ground employees may be at risk of identity theft because a home computer that contained their data may have been compromised. According to YPG spokesman, personnel information from 2005-2007, which included the names and Social Security numbers of the employees at that time, was being stored on the personal home computer of an employee of the installation's Resource Management Division. That information, which was being maintained by the Department of the Army, could have been compromised and possibly accessed during that time because the employee's computer may have picked up a virus from the Internet.

**Information Source:**
Dataloss DB

**March 19, 2010**
**PNC Financial Services Group Inc.**
**Dayton, Ohio**

PNC Financial Services Group is investigating a possible security breach involving some debit cards issued by the former National City Corp., which it acquired in December 2008. The problem surfaced when former National City customers began reporting unauthorized charges on their accounts. The breach involves a small number of cards in the Cincinnati area, and it appears to have been committed by someone outside PNC or National City prior to the merger. It doesn't involve any PNC-branded cards or longterm PNC customers. PNC has shut down National City debit cards in the Cincinnati area and asks that customers who have not yet done so activate their PNC debit cards. PNC is working one-on-one with customers to refund accounts, and has been returning funds within 24 hours.

**UPDATE (10/19/10):** Three men were charged with using skimming devices at PNCs in Pittsburgh in April and May.

**Information Source:**
Media

**March 19, 2010**
**National Realty and Investment Advisors, LLC**
**Hoboken, New Jersey**

Certain consumer information was accessed without proper authorization on March 9, 2010. Names and addresses were accessed, as well as additional information that may have included Social Security numbers, dates of birth and/or account numbers.

**Information Source:**
Dataloss DB

**March 19, 2010**
**MyPilotStore.com**
**Scottsdale, Arizona**

In February, it was discovered that a database containing customer names, addresses, e-mails, telephone numbers, and credit card information had been hacked. Some customers received phony charges to their accounts as a result of this hack.

**Information Source:**
Databreaches.net

**March 18, 2010**
**California State University, Los Angeles (Cal State Los Angeles)**
**Los Angeles, California**

Cal State Los Angeles has notified 232 former students that a computer stolen from the mathematics department office last month may have contained personal information such as their Social Security numbers and grades.

**Information Source:**
Dataloss DB

**March 18, 2010**
**Vanderbilt University**
**Nashville, Tennessee**

A professor's desktop computer, containing the names and Social Security numbers of 7,174 current and former students was stolen some time during the weekend of Feb. 6.

**Information Source:**
Dataloss DB

**March 18, 2010**
**Mary's Pizza Shack**
**Sonoma, California**

The Plaza location of Mary's Pizza Shack has been identified as the target of Internet hackers who penetrated the restaurant's computer system with a "logger" virus that captured credit card numbers at the transaction terminal. Only
credit card numbers were taken by the virus, Albano emphasized, no personal identification information, such as Social Security numbers or bank account records were exposed, although VISA and MasterCard debit accounts were apparently raided. Trustwave identified and removed the virus doing the damage.

Information
Source: Dataloss DB

March 17, 2010  Private Medical Practice
Lake Mary, Florida  MED  PHYS  Unknown

Police were looking for evidence of another crime when they found personal documents in the dumpster outside of a doctor’s office. The doctor specializes in treating the ear, nose, and throat and claims there was nothing about patients in the documents. The doctor agreed to shred the documents while the police investigated whether or not patient information was compromised.

Information
Source: NAID

March 16, 2010  Albany Police Department (ADP Georgia)
Albany, Georgia  GOV  DISC  Unknown

Sensitive city documents were found near a garbage can in an alley. The documents may have contained Social Security numbers. It is believed that officers failed to shred the documents and dispose of them properly.

Information
Source: Databreaches.net

March 13, 2010  St. Louis Metropolitan Police Department
St. Louis, Missouri  GOV  HACK  24

24 people may have had their personal information compromised following the cyber attack of one computer in the St. Louis Metropolitan Police Department. The attack came through an e-mail. The department’s website was not attacked. The names, addresses and Social Security numbers of the 24 people may have been viewed.

Information
Source: Dataloss DB

March 13, 2010  John Hancock Financial Services
Boston, Massachusetts  BSF  PORT  At least 1,085

A CD that contained customer names, Social Security numbers, and dates of birth went missing. The CD was password protected and encrypted and credit monitoring services were offered to customers who may have been affected.

Information
Source: Databreaches.net

March 13, 2010  Beer and Wine Hobby
Woburn, Massachusetts  BSR  HACK  35,000 (0 complete credit card numbers reported)

Personal information may have been accessed during a breach of Beer and Wine Hobby’s computer system. The personal information included partial credit card numbers.

Information
Source: Databreaches.net

March 13, 2010  TD Bank
Mount Laurel, New Jersey  BSF  INSD  Unknown

A former TD Bank employee provided information to outside accomplices who stole over $200,000 from customer accounts. The insider passed along driver’s license numbers and bank account numbers.

UPDATE (8/7/2011): A fraud ring involving insiders at multiple TD Banks in South Jersey was uncovered. A federal trial will begin in October. The members of the fraud group are accused of stealing more than $400,000 from customers and banks between November 2005 and May 2010. Six members are part of the 148-count indictment. The scheme involved obtaining customer ID data, creating false ID photos with customer data and using the phony IDs to access customer accounts. Investigators were able to raid the ring leader’s home on June 7 after catching a few of the ring members posing as customers.

Information
Source: Databreaches.net

March 13, 2010  California Pizza Kitchen
Plymouth Meeting, Pennsylvania  BSR  CARD  Unknown
A credit card thief and his partner used skimming devices to obtain credit card account information. The thief provided his partner with a skimming device while she worked at a California Pizza Kitchen in Plymouth Meeting, Pa. from 2008 to 2009. Around 26 customer credit cards were fraudulently charged.

Information
Source: Databreaches.net
March 13, 2010 Beecher Carlson Boston, Massachusetts BSO PORT 5,432

Two laptops were stolen from employees attending an off-site company meeting in January. The laptops contained names and Social Security numbers for employees of Beecher Carlson's clients, including 1,012 people who live in Massachusetts.

UPDATE (8/17/10): The number is closer to 5,432 with an additional 2,824 living in New York, 66 living in Maine and 1,530 living in Maryland.

Information
Source: Databreaches.net
March 13, 2010 Nuance Communications Inc. Burlington, Massachusetts BSO PORT 1,191

Nuance Communications Inc., a Burlington speech technology company, reported a laptop stolen from a locked car in Burlington may have contained personal information such as names and Social Security numbers of 1,191 Massachusetts residents. The company notified its employees, installed security and encryption software on laptops, and purchased credit monitoring services for those workers whose information was on the laptop.

Information
Source: Databreaches.net
March 12, 2010 Beecher Carlson Holdings Inc. Atlanta, Georgia BSF PORT 1,012

Two laptops were stolen from employees while they were off-site. The laptops contained employee names and Social Security numbers. Many more people may have been affected since the total number of Massachusetts residents affected is 1,012.

Information
Source: Databreaches.net
March 11, 2010 monoprice.com Rancho Cucamonga, California BSR HACK Unknown

The company took their web site offline, after it received e-mails and phone calls from several customers complaining about fraudulent charges on their debit and credit cards that they had used on monoprice.com.

Information
Source: Databreaches.net
March 11, 2010 First Convenience Bank Killeen, Texas BSF INSD Unknown

A former employee sold customer information which led to the theft of at least $53,000 from customer accounts.

Information
Source: Databreaches.net
March 11, 2010 Bennett College Greensboro, North Carolina EDU HACK 1,100

A payroll computer was breached. Names, Social Security numbers, birth dates, pay rates, and bank transit numbers were exposed.

Information
Source: Databreaches.net
March 10, 2010 Atlanta Veterans Affairs Medical Center Atlanta, Georgia MED INSD Unknown

An assistant allegedly recorded two sets of patient data on to a personal laptop for research purposes. One set included three years' worth of patient data and another held 18 years of medical information. The physician assistant's laptop was never connected to the VA network and any data she recorded on her laptop was hand entered. The department has not disclosed the number of patients involved in the incident, what kind of personal data was copied, or whether it plans to notify the veterans whose records were downloaded.
Thrivent Financial for Lutherans
Mechanicsburg, Pennsylvania

BSF  PORT  At least 9,386

March 10, 2010

The only number reported so far is 9,386, the number of individuals from Maine affected.

Thrivent Financial for Lutherans, Minneapolis, experienced a break-in at one of its offices in Pennsylvania. A laptop computer was among the items stolen. The laptop had safeguards to protect sensitive information, including strong password protection and encryption. But Thrivent Financial says the information stored on the laptop may be at risk. The information on the laptop was personal information, including names, addresses, Social Security numbers and health information.

Wickenburg Unified School District
Wickenburg, Arizona

EDU  DISC  1,438

March 10, 2010

State auditors found that the District’s network was accessible to unauthorized users. Backup servers were kept in an easily accessible room. Names, Social Security numbers, addresses and birth dates of students were left exposed.

LPL Financial
Boston, Massachusetts

BSF  PORT  Unknown

March 9, 2010

An unencrypted portable hard drive was stolen from a car of an LPL representative. As a result of the theft, private client information, including names, addresses, dates of birth and Social Security numbers may have been breached.

Arrow Electronics
Melville, New York

BSR  PORT  4,044

March 8, 2010

A laptop containing current and former employee personal information was stolen. The information included names, Social Security numbers, addresses, telephone numbers, and some corporate and personal credit cards.

Huntington Place Senior Community
Chalmette, Louisiana

MED  DISC  Unknown

March 8, 2010

Personal documents were found in the abandoned nursing home. The documents included names, Social Security numbers, medical records and dates of birth of patients.

McNair Eye Center
Heber Springs, Arkansas

MED  STAT  9,000

March 8, 2010

A computer server with patient personal information was stolen.

Arrow Electronics
Melville, New York

BSO  PORT  4,004

March 8, 2010

The theft of a laptop from the office of Arrow Electronics has resulted in the company notifying 4,004 current and former employees that their personal information was on the laptop. The laptop was stolen during a break-in on February 18. Personal information on the laptop included names, addresses, telephone numbers, and for some of those who used company Blackberry, wireless AirCard and calling card services, their Social Security numbers, some credit card information such as last four digits, security code, and expiration date.
A man and his wife who were previously charged with selling patient information in 2009, were charged with stealing personal information of individuals transported by Randle Eastern Ambulance Service Inc. (American Medical Response). The information was then sold to South Florida personal injury attorneys and clinics. The stolen information included names, telephone numbers, medical diagnoses, and addresses. They used the help of a former AMR employee.

Information Source: Databreaches.net

March 6, 2010 Westin Bonaventure Hotel & Suites Los Angeles, California
BSO HACK Unknown

Westin Bonaventure Hotel & Suites four restaurants in Lake View Bistro, Lobby Court Bar, Bonavista Lounge and L.A. Prime, along with its valet parking operation, may have been hacked at some time between April and December, disclosing names, credit card numbers and expiration dates printed on customers’ debit and credit cards.

Information Source: Dataloss DB

March 5, 2010 Arkansas Army National Guard Camp Robinson, Arkansas
GOV PORT 35,000

An external hard drive has gone missing. Approximately 35,000 current and former members of the Arkansas Army National Guard are affected by the loss. The drive included names, Social Security numbers and other personal information which potentially places the affected soldiers at risk for identity theft.

UPDATE (5/18/10): The external hard drive containing personal information on over 32,000 current and former Arkansas Guardsmen that was reported missing on February 22 has now been recovered and destroyed. The drive was reported missing by an Arkansas Soldier who used the device as a personal backup of his work related information. This included a copy of the Guard’s personnel database which contained personal information on all Soldiers who have served in the Arkansas Army National Guard since 1991.

Information Source: Dataloss DB

March 5, 2010 UT Southwestern Medical Center Dallas, Texas
MED INSD 200

UT Southwestern recently sent out a mass mailing to 10,000 of its patients, claiming that a former employee disclosed patients’ information to a third party that intended to use it for credit, loans and open bank accounts. UT Southwestern representatives claim 200 patients were actually affected.

Information Source: Dataloss DB

March 5, 2010 University of Texas Southwestern Medical Center Dallas, Texas
GOV INSD 200

A former employee was arrested on patient information and identity theft. The stolen patient information includes names, Social Security numbers, birth dates, addresses, phone numbers and financial data. The employee allegedly sold the patient information of at least 200 people to an outside party for the purpose of creating bank accounts and misusing credit and loans.

Information Source: Databreaches.net

March 5, 2010 Hancock Fabrics Baldwyn, Mississippi
BSR DISC Unknown

Employee documents were found near a dumpster behind the Huntsville, Alabama store. The documents were not shredded and contained payroll records dating back to 2005 with Social Security numbers, names, and pay rates.

Information Source: Databreaches.net

March 4, 2010 Wake Forest United Baptist Medical Center (WFUBMC) Winston-Salem, North Carolina
MED PORT 554

A bag containing a document with the names and Social Security numbers of 554 patients was stolen from an employee’s locked car.

UPDATE (6/2/2011): The theft occurred on February 15 at an outpatient clinic parking lot.

Information Source: HHS via Databreaches.net

records from this breach used in our total: 0

542
March 4, 2010  **Courage to Change**  Houston, Texas  MED INSD Unknown

The owner of the business used patient Medicaid information to fraudulently claim $968,583 from Medicaid between January of 2003 and September of 2006.

**Information Source:** PHIPrivacy.net

March 4, 2010  **Akel Business Services (also Silva Bookkeeping and Tax Services)**  La Mesa, California  BSF INSD 32

A dishonest business owner filed fraudulent tax returns by using his clients’ information. He also created fictitious identities by using the Social Security numbers of his clients’ children. At least 32 people were affected.

**Information Source:** databreaches.net

March 3, 2010  **Small Dog Electronics**  Waitsfield, Vermont  BSR HACK 3,000

After Small Dog began collecting and matching customer donations for Haiti relief efforts, a hacker breached the website and began stealing customer credit card information. The breach lasted from December of 2009 to January of 2010.

**Information Source:** databreaches.net

March 3, 2010  **7-Eleven**  Martinez, California  BSR CARD 200

The devices were found at locations in Martinez, San Mateo, Benicia, Livermore, Hayward, Oakland and Sacramento.

Two men were charged with placing skimming devices on 7-Eleven gas pumps across central and northern California. The men both face 32 counts of identity theft and conspiracy charges. At least eleven skimmers were found on gas pumps.

**UPDATE** (10/13/10): A third suspect has been linked to these incidents and now faces similar charges.

**UPDATE** (1/11/11): Over 200 people were affected. Two of the four members of the fraud group were sentenced. Two other members await sentencing.

**Information Source:** databreaches.net

March 2, 2010  **Shands at UF**  Gainesville, Florida  MED PORT 12,500

Shands at UF sent notification letters to about 12,500 people Monday warning them that a laptop containing their personal and medical information was stolen. An employee had uploaded the information onto his home laptop for work-related purposes. The laptop held information about patients referred to the gastroenterology clinical services department. Included were names, addresses, medical record numbers, and in the case of 650 patients, Social Security numbers.

**Information Source:** Dataloss DB

March 2, 2010  **Open Door Clinic of Greater Elgin**  Elgin, Illinois  MED HACK 260

According to a lawsuit, the clinic stores patient information, including Social Security numbers, addresses, telephone numbers, insurance information and medical history on a file-sharing network. That network is accessible to employees’ personal laptops and home computers. A spreadsheet with information of about 260 of its patients was leaked as a result of the installation and use of file sharing software on computers containing patients’ personally identifiable information.

**Information Source:** Dataloss DB

March 2, 2010  **Family Health Center**  Reston, Virginia  MED DISC Unknown

Boxes containing patient information ended up in a dump. The easily accessible information included health history, surgeries performed, test results, pictures, insurance cards, bank account information and addresses. The boxes were traced back to Family Health Center on Town Center Parkway.

**Information Source:** PHIPrivacy.net
A former employee of Diabetes Direct Inc is accused of stealing patient information to commit identity theft. The former employee also had multiple driver's licenses and was able to open utility, bank and credit accounts.

**Information Source:** Records from this breach used in our total: 0

March 1, 2010

**US Bank**

*Cleveland, Ohio*

A laptop was stolen from the desk of a financial adviser. The laptop contained personal information about bank customers.

**Information Source:** Records from this breach used in our total: 0

February 28, 2010

**Wyndham Hotels & Resorts**

*Dallas, Texas*

International hotel group Wyndham Hotels and Resorts (WHR) has suffered yet another serious data breach after hackers broke into its computer systems, stealing customer names and payment card information.


**UPDATE** (05/12/2011): Wyndham identified 42 additional New Hampshire residents who were affected by the 2010 breach. The total number of people affected by hacking incidents at Wyndham in 2009 and 2010 is likely to be large since 37 hotels under Wyndham's hotel group were affected.

**UPDATE** (06/26/2012): The FTC has filed a complaint against Wyndham hotels for failure to protect the personal information of consumers. Wyndham hotels and three of its subsidiaries are accused of data security failures that led to three data breaches at Wyndham hotels between 2009 and 2011. The FTC accused them of allowing failures that led to fraudulent charges on consumers' accounts, millions of dollars in fraud loss, and the export of hundreds of thousands of consumers' payment card account information to an internet domain address registered in Russia. The FTC statement can be read [here](http://www.ftc.gov/opa/2012/06/wyndham.shtm).

**UPDATE** (08/30/2012): Wyndham Hotel & Resorts LLC is contending that the FTC lacks the authority to regulate private companies' data security practices. Wyndham motioned to dismiss the FTC's Arizona federal court case with this assertion.

**UPDATE** (06/25/2014): On June 25th, The Federal Trade Commission "sufficiently alleged that several Wyndham Hotels entities operated as a common enterprise in the commission's data security enforcement action against them, the U.S. District Court for the District of New Jersey held June 23, in an unpublished opinion. The court is allowing Wyndham Hotels and Resorts LLC a interlocutory review of portions an an earlier April 7th opinion denying the company's separate motion to dismiss, Judge Esther Salas wrote in a second unpublished opinion (FTC v. Wyndham Worldwide Corp., 2014 BL 174519, D.N.J., No. 2:13-cv-01887, unpublished opinion 6/23/14)."

**UPDATE** (12/09/2015): Wyndham Hotels has settled with the FTC that it failed to properly secure customer credit card information.

"A consent order outlining the settlement was filed with the federal court in Newark, New Jersey, 3-1/2 months after the 3rd U.S. Circuit Court of Appeals in Philadelphia said the FTC had authority to regulate corporate cyber security.

Under the order, Wyndham must establish a comprehensive information security program designed to protect cardholder data including payment card numbers, names and expiration dates, the FTC said."


February 27, 2010

**AT&T**

*Chicago, Illinois*

A former employee of an unknown service provided for AT&T removed documents that contained customer credit card information. The information may have also included Social Security numbers, driver's license numbers, names and addresses.

**Information Source:** Records from this breach used in our total: 0

February 27, 2010

**GroupM**

*New York, New York*

Eight laptops were stolen from an office. They most likely contained unencrypted employee information such as Social Security numbers and bank account information.
February 27, 2010  California Business Bureau Inc., Medical Billing Services  Monrovia, California  MED  INSD  8,861

A former employee accessed unencrypted files between December of 2006 and March of 2008. The files contained patient Social Security numbers, names, addresses, and dates of birth.

February 27, 2010  Ameripath  Palm Beach Gardens, Florida  MED  PORT  Unknown

A laptop containing sensitive information was stolen from an employee. The data included names, Social Security numbers, and addresses for patients, employees, or both.

February 25, 2010  Wyoming Department of Health  Cheyenne, Wyoming  GOV  DISC  9,000

The personal information of about 9,000 children in the state’s children’s health insurance program could have been exposed on the Internet. The error resulted in the names, birthdays, Social Security numbers, addresses and phone numbers of Kid Care CHIP participants being accessible on an unsecured Web page for months.

February 25, 2010  Logic World Medical  Houston, Texas  MED  INSD  Unknown

The owner and operator of Logic World Medical used the names, addresses, and account numbers of Medicaid beneficiaries to file false claims for payment of services and goods that he never provided. Approximately $1,101,865.37 was fraudulently claimed between April of 2004 and August of 2006.

February 24, 2010  Citigroup  New York, New York  BSF  DISC  600,000

About 600,000 Citigroup customers got a shock earlier this month when they received their annual tax documents with their Social Security numbers printed on the outside of the envelope. The digits were not identified as a Social Security number, and they were printed at the lower edge of the mailing envelope with other numbers and letters that together resembled a mail routing number.

February 24, 2010  University of Washington Medical Center (UWMC)  Seattle, Washington  MED  INSD  210

The UWMC sent letters to patients telling them that their Social Security numbers, credit card information, birth dates and addresses were accessed by dishonest persons. The personal information was found in the possession of a convicted felon who had ties to an employee who works with the hospital. The employee worked at NCO Financial Systems, a company which UWMC uses to process patient payments.

February 24, 2010  7-Eleven  Sandy, Utah  BSR  CARD  Unknown

A skimming device monitored transactions at a gas station pump in Sandy, Utah. The device could have been active for 60 days before being discovered and was used to steal over $11,000.

February 22, 2010  SunTrust Bank  Atlanta, Georgia  BSF  CARD  200

Throughout the summer of 2009, four men put skimming devices on SunTrust Bank ATMs in the Florida counties of Hillsborough and Pinellas. Well over 200 people were affected.
February 19, 2010  
**TennCare**  
**Nashville, Tennessee**

An electronic error caused information such as Social Security numbers for about 3,900 enrollees to be sent to incorrect addresses. The error was the result of a modification to the system that pulls addresses into an electronic file for TennCare, the state’s expanded Medicaid program. Letters and cards that contained one or more pieces of personal information were sent to incorrect addresses.

February 19, 2010  
**Valdosta State University**  
**Valdosta, Georgia**

A Valdosta State server that was reported as being breached could have exposed the information of up to 170,000 students and faculty. Valdosta State officials reported the discovery of a breach on Dec. 11 and estimated it began on Nov. 11. The university said the grades and Social Security numbers of up to 170,000 students and faculty were exposed in the breach.

February 17, 2010  
**Cardiology Consultant Inc.**  
**Pensacola, Florida**

Cardiology Consultants Inc. today reported that a laptop used to process ultrasound images was stolen from one of its Pensacola offices. The computer did not contain patient financial information or Social Security numbers. The stolen computer did contain the first and last names, dates of birth, medical record numbers, exam dates and in some cases, the reason for the ultrasound.

February 17, 2010  
**Southern Illinois University**  
**Carbondale, Illinois**

A computer security breach at Southern Illinois University may have put hundreds of alumni at risk of identity theft. A faculty member’s computer in the Mathematics Department was found to be infected with malicious software. When the computer files were searched, university officials discovered there were Social Security numbers for approximately 900 students who took introductory math classes at SIU in 2004 and 2005 stored on the hard drive.

February 17, 2010  
**Dairy Queen**  
**Hanceville, Alabama**

Hanceville police are cautioning residents to be on guard against a sophisticated debit card wire scam that has leached hundreds of thousands of dollars from customers whose card numbers have been stolen remotely from pay terminals at one or more local businesses. The primary target in the theft so far has been the Dairy Queen restaurant. It’s unsure whether this is ultimately involving other businesses. At the Dairy Queen location, somebody has apparently tapped into the Internet server and hacked into the debit card system. They are printing the customers’ debit card numbers and using them all over California and Georgia.

February 17, 2010  
**T.G.I. Friday’s (TGIF)**  
**Coon Rapids, Minnesota**

A former employee used a skimming device to gain credit card information from customers of the Coon Rapids T.G.I. Friday’s. The dishonest employee was involved with a partner who used skimming devices in a variety of locations throughout Minnesota.
February 16, 2010

**New York Social Security Administration**
New York, New York

GOV PORT 969

A computer disc containing detailed personal information about 969 New Yorkers was lost by a Social Security Administration employee traveling to Queens from the Bronx. The disc was lost as the employee was going to the Queens Social Security hearing office, and the information on it included administrative decisions, medical evidence and internal agency documents containing people's names and Social Security numbers.

February 16, 2010

**Eclipse Property Solutions**
St. Petersburg, Florida

BSO INSD Unknown

A St. Petersburg man has been charged with stealing customers' credit card numbers from a marketing company he worked for to buy nearly $30,000 in dinners, limos and other luxuries. The man and another employee listened from their cubicles as co-workers repeated customer credit card information aloud to confirm accounts.

February 15, 2010

**West Memphis Police Department**
Memphis, Tennessee

GOV INSD Unknown

FBI is investigating, after the security of the West Memphis Police Department's computer network was apparently compromised. The FBI had information that somebody had used a computer that shouldn't have used it. The suspect in the breach was a detective in the police department. Files containing the names and Social Security numbers of police department employees were stored on the computer network, making the employees vulnerable to identity theft.

February 12, 2010

**Galeton, Gloves Inc.**
Mansfield, Massachusetts

BSR HACK At least 89

The Gloves Inc. website for Galeton was hacked. Customer names, addresses, credit card numbers and expiration dates were exposed.

February 12, 2010

**Daedalus Books Inc.**
Columbia, Maryland

BSR HACK At least 1,285

A hacker accessed a database with customer information. The information included names, addresses, and credit card numbers from people who made orders between August 25, 2009 and November 23, 2009.

February 12, 2010

**ING Fund**
Amsterdam, Noord Holland

BSF DISC 106

Customer information was accessible through a web search from August of 2008 through January of 2010. The information included names, Social Security numbers, addresses, and account numbers of shareholders in New Hampshire and other locations.

February 11, 2010

**Equifax**
Atlanta, Georgia

BSF DISC 35 New Yorkers affected (at least 35)

An unknown number of current and former employees of credit reporting firm Equifax received W-2 forms in the mail with their Social Security numbers visible through a window on the envelope. Some of the tax forms mailed by Equifax's payroll vendor through the U.S. Postal Service had the Social Security number in a Control Number field, which was partially or fully viewable through the return address window.
The University of Texas Medical Branch has mailed letters notifying 1,200 patients that sensitive information about them had been available to a woman charged with identity theft in an unrelated case. Officials sent out the letters this week after MedAssets, which the medical branch hired to assist with billing from third-party payers, warned of a security breach by one of its employees. Law enforcement officials notified MedAssets that a former employee had been arrested and charged with identity theft. The person also was alleged to have used a stolen identity to misrepresent herself and gain employment at Georgia-based MedAssets and had been involved in other instances of identity theft. That employee is implicated in a widespread identity theft investigation involving cases from Texas to Wisconsin and losses upward of $1 million.

**UPDATE (3/9/10):** Twelve hundred more letters were sent out to people whose financial information may have been exposed.

**UPDATE (10/14/10):** From Databreaches.net: "Katina Candrick of LaGrange, Texas, was sentenced to 15 years in federal prison and ordered to pay $163,185.19 restitution for unlawful possession of fraudulent identification documents and conspiracy to commit identity theft...According to court records Candrick schemed to steal and use for her own benefit personal identification information of others, which she used to pay for living expenses, vehicles and other items. From July 6, to November 13, 2009, Candrick was employed as a Patient Account Representative by MedAssets."

After its security system was disabled, customer credit and debit card information was exposed. The exposure of the information led to some unauthorized transactions.

An employee used customer credit card information to purchase $200,000 worth of Wal-Mart shopping cards.

A former employee accessed health care professionals' Social Security numbers, names, dates of birth, and home addresses. Between 2007 and 2010, the employee created fictitious identities and created e-mail addresses, opened bank accounts and credit card accounts.

**UPDATE (05/10/2010):** The former employee was sentenced to 28 months in prison followed by three years of supervised release. She was also ordered to pay $2,914.95 in restitution. She pleaded guilty to one count of mail fraud and one count of aggravated identity theft on February 9. Around 40 health care professionals such as doctors, psychologists, nurses, and dietitians were victims of fraudulent financial activity.

The personal security of nearly 50,000 people may have been breached by the California Department of Health Care Services. Social Security numbers were printed on the address labels of letters that were mailed by the department. State employees mistakenly included the numbers in a list of patient addresses. The list was sent to an outside contractor, who printed and mailed the envelopes.

Personal banking information for 6,000 state employees was inadvertently included in an e-mail distributed to dozens of payroll officers of state agencies. The e-mail from an unnamed administrative-services employee included an attached spreadsheet listing 6,000 state employees whose bank accounts are to be moved from National City Bank, which was bought by PNC Bank.
About 145 employees at the Kansas City Art Institute have been notified of potential identity theft in connection with the disappearance of a computer from the campus. An Apple computer that contained Social Security numbers, dates of birth and other personal information about the school’s professors and staff employees was stolen from the human resource office.

University of Texas at El Paso is notifying students that their Social Security numbers were visible when their tax forms were sent out. The University notified 15,000 students but they don’t know exactly how many students were affected. UTEP blames a glitch in a machine used to fold letters when student’s forms were sent out. Some of the forms were folded in such a way that the document shifted on the envelope and allowed for the Social Security numbers to be visible through the mailing window on the envelope.

AvMed Health Plans announced that personal information of some current and former subscribers may have been compromised by the theft of two company laptops from its corporate offices in Gainesville. The information included names, addresses, phone numbers, Social Security numbers and protected health information. The theft was immediately reported to local authorities but attempts to locate the laptops have been unsuccessful. AvMed determined that the data on one of the laptops may not have been protected properly, and approximately 80,000 of AvMed’s current subscribers and their dependents may be affected. An additional approximate 128,000 former subscribers and their dependents, dating back to April 2003, may also have been affected.

UPDATE (06/03/2010): The theft of the laptops compromised the identity data of 860,000 more Avmed members than originally thought. The total now nears 1.1 million.

UPDATE (11/17/2010): Five AvMed Health Plans customers filed a class-action lawsuit against the health insurer on behalf of the 1.2 million people who were affected by the breach. At least two of them believe that their personal information was misused as a result of this particular breach.

UPDATE (09/24/2012): An appeals court ruled that the plaintiffs were "explicitly" able to prove a link between the breach and ID theft they incurred. The case had been thrown out by a lower court in August 2011, but the appeal ruling may allow victims of identity theft to make it easier to prove that the identity theft was caused by a data breach.

UPDATE (09/05/2013): AvMed Inc. agreed to settle with customers who were affected by the 2009 data breach on September 3, 2013.

UPDATE (10/29/2013): AvMed will pay $3 million.

UPDATE (3/6/2014): "Last week, a judge for the Southern District of Florida gave final approval to a settlement between health insurance provider AvMed and plaintiffs in a class action stemming from a 2009 data breach of 1.2 million sensitive records from unencrypted laptops. The settlement requires AvMed to implement increased security measures, such as mandatory security awareness training and encryption protocols on company laptops. More notably, AvMed agreed to create a $3 million settlement fund from which members can make claims for $10 for each year that they bought insurance, subject to a $30 cap (class members who experienced identity theft are eligible to make additional claims to recover their monetary losses)".

Applicants of the Wyoming Kid Care CHIP program had their information exposed online. Family home addresses and the Social Security numbers of children involved were available to the general public via a Google search.
Highmark notified 3,700 members that documents containing their names, policy identification and Social Security numbers were missing. This is the second such data spill involving the region’s dominant health insurer in four months. In January, the company mailed a premium billing statement to Boscov’s Department Store, a client in Reading, according to Highmark. The envelope arrived damaged and torn; pages were also missing. The pages included the names and other identifying information for 3,700 members.

Information Source: Dataloss DB

February 4, 2010 Ozarks Area Community Action Corporation Springfield, Missouri

The organization printed two 1099 forms on one piece of paper. They were supposed to separate them and send each to the rightful owner. Instead one person got both. The mistake sent tax forms and Social Security numbers to strangers. More than 500 landlords work with OACAC. On January 28, 2010, half of those landlords didn’t receive tax forms. The other half got their forms and someone else’s private information.

Information Source: Dataloss DB

February 4, 2010 Ceridian Corporation Bloomington, Minnesota

A hacker attack at payroll processing firm Ceridian Corp. of Bloomington has potentially revealed the names, Social Security numbers, and, in some cases, the birth dates and bank accounts of 27,000 employees working at 1,900 companies nationwide. In a Jan. 29 letter to an affected worker obtained by the Star Tribune, Ceridian said a hacker attacked its Internet payroll system Dec. 22 and 23.

UPDATE (6/1/2011): The Federal Trade Commission reached a settlement agreement with Ceridian. According to the FTC, Ceridian did not adequately protect its network from reasonably foreseeable attacks and failed to encrypt the sensitive personal information that was stored on its network. The settlement requires the company to establish a comprehensive information security program and to undergo 20 years of independent security audits. Ceridian provides payroll and HR services.

Information Source: Dataloss DB

February 4, 2010 HyCentral Medical Supplies and Equipment Derry, New Hampshire

The owner of the business used Medicare client information to obtain approximately $1.6 million worth of fraudulent claims.

Information Source: PHIPrivacy.net

February 3, 2010 Private Dental Practice in Medical Commons One Greensburg, Pennsylvania

A laptop containing patient information was stolen.

Information Source: HHS via Databreaches.net

February 3, 2010 Private Practice in Medical Arts Building Greensburg, Pennsylvania

A laptop containing patient information was stolen.

Information Source: HHS via Databreaches.net

February 2, 2010 P.F. Chang’s Bistro Scottsdale, Arizona

According to notification letters from the company: "Password protected electronic equipment belonging to the Company was stolen" on December 19 of 2009. Some current and former employee information was on the equipment. Employee dates of birth and Social Security numbers may be at risk. Reports state that 73 employees from New Hampshire, 1,823 from Massachusetts, and 3,080 from New York were affected.

UPDATE (8/09/10): Another 3,205 people who are residents of Maryland were affected.
February 1, 2010, West Virginia University, Morgantown, West Virginia

Around 53 West Virginia University students' personal information was available to others following an "operational error" during a routine update of tax information. The students' 1098-T forms, which include their Social Security number and tax identification numbers, among others, were uploaded to the University's 1098-T Web site. The forms are distributed to WVU students who are U.S. citizens who paid tuition during the 2009 calendar year. They can be used to claim federal tax credit. Students can typically access their forms on the site for tax purposes, but the error made the information viewable to any WVU student on the site.

January 31, 2010, Iowa State Racing and Gaming Commission, Des Moines, Iowa

The Iowa Racing and Gaming Commission says someone gained access to a computer server that holds more than 80,000 records containing casino employee information. The person who hacked into the system was traced back to China and had used a computer with an external account. The server contains records including names, birth dates and Social Security numbers.

January 30, 2010, Ameriquest Mortgage Company, Apple Valley, Minnesota

A man working for Ameriquest Mortgage Company as a mortgage associate for only six weeks used personal information he lifted from mortgage applications. It was a pretty fruitful month and a half for him -- and a pretty costly one to nearly 100 people and several financial institutions. He also used information taken from mail and even some items taken from gym lockers of a couple of hundred more victims. The man eventually stole more than $150,000 from at least eight banks. The man used stolen personal information to create fraudulent identification documents and checks, which he then used to obtain cash, pay for services and buy items. For example, he used one victim's identification to obtain a credit card through U.S. Bank. With that card, he wound up withdrawing $30,529.63 in cash from ATMs throughout Minnesota. Those withdrawals were charged to the victim.

January 29, 2010, Curian Capital, Denver, Colorado

On January 19, 2010, a technical error caused client data to be mismatched during a posting of routine fee statements to the secure online filing cabinets of individual financial professionals. A limited number of customer fee statements which included client names, Curian account numbers and account balances, and Social Security numbers were made available to other clients for less than a day.


Hundreds of papers were found along a road in Des Plaines. Some were job applications for Rabjohns Financial Group/New England Financial in Chicago and corresponding UF forms. W-2 forms and investment statements from 2009 were also among the papers. It is unclear how the information ended up in the road.


The names, birth dates and Social Security numbers of 77,000 people were lost in their Chicago office. The people at risk for identify theft are those who were in the PERS and TRS system in 2003-04 as active or inactive employees or retirees. Price Waterhouse Coopers has agreed in a settlement to pay for credit monitoring and other security measures and cover any losses to individuals caused by its mishandling of the information. A number of people associated with the State of Alaska had their information exposed.

January 28, 2010, Humboldt State University, Arcata, California
A Humboldt State University computer infected with a virus may have exposed the personal information of 3,500 people employed by the school between 2002 and 2006. The computer was found to have a sophisticated virus that is used to steal login information.

Information Source: Dataloss DB

January 28, 2010

University Medical Clinics
Port St. Lucie, Florida

A woman found the files and notified police after receiving an anonymous tip.

Information Source: NAID

January 27, 2010

Department of Commerce
Washington, District Of Columbia

A Department of Commerce employee inadvertently transmitted over the Internet a file containing the Personally Identifiable Information (PII) of Commerce employees to other Department employees. Although the Department employees were authorized to send and receive the PII, the transmission of the PII over the Internet in unencrypted form may have compromised their name and Social Security numbers.

Information Source: Dataloss DB

January 27, 2010

University of California, San Francisco (UCSF) School of Medicine
San Francisco, California

A laptop containing files with information on 4,400 patients was stolen from a UCSF School of Medicine employee. Information “potentially exposed” included name, medical record number, age and clinical information, but the stolen laptop did not contain any Social Security numbers or other financial data. The same laptop also contained data for approximately 2,900 patients at Beth Israel Deaconess Medical Center in Boston.

Information Source: Dataloss DB

January 27, 2010

Seattle Municipal Court
Seattle, Washington

Those with questions may call (206) 553-4110.

A former customer service representative sold the names and credit card information of court customers to ID thieves who then used the information to make fake credit cards in the victims’ names.

UPDATE (6/24/2011): The leader of an ID theft ring was sentenced to five years in prison, five years of supervised release and over $220,000 in restitution for bank fraud and aggravated identity theft on June 17, 2011. The information that the ID thieves obtained from the Seattle Municipal Court employee included the personal information and credit card numbers of people who used credit cards to pay parking and traffic fines. One member of the ID theft ring also managed to obtain financial information from the customers of an unnamed fast food restaurant where the defendant worked. At least five people participated in the ID theft ring.

Information Source: Databreaches.net

January 27, 2010

Methodist Hospital
Houston, Texas

Methodist Hospital notified people that someone stole a laptop from an office at the Smith Tower in the Texas Medical Center. A thief took the laptop on January 18. The computer was attached to a medical device that tests pulmonary function and contained private health information and Social Security numbers.

Information Source: Dataloss DB

January 22, 2010

Brio Tuscan Grille in Country Club Plaza
Kansas City, Missouri

A man used a skimming device to obtain the credit card information of customers while working as a waiter at Brio Tuscan Grille of Kansas City, Missouri.

UPDATE (7/26/10): The former employee was sentenced to three years of federal prison time for credit card fraud and mail fraud. He originally gained access to the customer information during July and August of 2008. His fraudulent purchases
An investigation is under way after hundreds of city health workers’ personal information was stolen. Investigators have identified a person of interest in connection with the stolen information. The person of interest was an employee within the department over the past three years. Current employees and those who previously worked at the department within the last three years may be affected.

CHASE customer information that was sold to another business was accidentally posted on a website. The information included names, addresses and bank account numbers.

It was discovered that an hourly employee of 19 years was forging checks by using the information of companies who were fined for OSHA violations. The employee had handled checks for 12 years and may have been involved in a larger fraud operation. The employee was arrested and fraudulently obtained less than a thousand dollars on average from each company. A total of 759 companies who paid OSHA fines between January 1, 2009 and November 18, 2010 were affected. One business owner discovered that a fraudulent check had been cashed for $745 after he paid an OSHA fine of $315.

A man broke into a Goodwill store and stole a safe, but instead of money that thief got the names, addresses, dates of birth, and Social Security numbers from thousands of people.

A list of the names, addresses and Social Security numbers of employees of the City of Oakridge was sent out with monthly water bills. The town has about 1,400 households. The city has signed up all employees for a credit monitoring service. The city does not know how many people received the list of employee information in a newsletter included with their water bill.
An error at the U.S. Department of Defense Document Automation and Production Service caused pay statements containing names and sensitive information about the finances of about 18,000 recipients of a special pay for disabled retirees to be sent to wrong addressees. The statements, a page of which contained information about annual increases in Concurrent Retirement and Disability Pay, mistakenly listed data including at least a portion of another recipient's name, their bank or insurance company name, the amount of their allotment and the allotment type. There is “no indication” that any Social Security numbers, bank account numbers or phone numbers were listed on the erroneously mailed pages.

**Information Source:** Media

**January 14, 2010**  
**Lincoln National Corporation (Lincoln Financial)**  
**Radnor, Pennsylvania**  

http://www.finra.org/Newsroom/NewsReleases/2011/P122940

Lincoln National Corp. (LNC) last week disclosed a security vulnerability in its portfolio information system that could have compromised the account data of approximately 1.2 million customers. In a disclosure letter sent to the Attorney General of New Hampshire Jan. 4, attorneys for the financial services firm revealed that a breach of the Lincoln portfolio information system had been reported to the Financial Industry Regulatory Authority (FINRA) by an unidentified source. The unidentified source sent FINRA a username and password to the portfolio management system. "This username and password had been shared among certain employees of [Lincoln Financial Services] and employees of affiliated companies," the letter says. "The sharing of usernames and passwords is not permitted under the LNC security policy."

**UPDATE** (2/17/2011): Lincoln National Corporation was fined $600,000 by the Financial Industry Regulatory Authority for failing to adequately protect customer information. Failing to require brokers working remotely to install security software on personal computers led to the fine.

**Information Source:** Media

**January 14, 2010**  
**BlueCross BlueShield (BCBST)**  
**Chattanooga, Tennessee**

Additional locations: Memphis, Jackson, Knoxville, Nashville and additional locations in Tennessee

The theft of 57 hard drives from a BlueCross BlueShield of Tennessee training facility last October has put at risk the private information of approximately 500,000 customers in at least 32 states. The hard drives contained 1.3 million audio files and 300,000 video files. The files contained customers' personal data and protected health information that was encoded but not encrypted, including: names and BlueCross ID numbers. In some recordings—but not all—diagnostic information, date of birth, and/or a Social Security number were exposed. BCBS of TN estimates that the Social Security numbers of approximately 220,000 customers may be at risk.

**UPDATE** (4/29/10): The number of plan members whose data were exposed has grown from 521,761, an estimate made in March, to nearly one million, as of April 2, according to a report issued by Mary Thompson, spokeswoman for the Tennessee Blues.

**UPDATE** (11/3/10): According to a letter sent to the New Hampshire Attorney General's Office, the total number of individuals affected was 1,023,209. BCBS used a three-tier system to categorize individuals affected by the breach. The total includes 451,274 clients whose Social Security numbers were involved, 319,325 clients whose personal and diagnostic health information was involved and 239,730 clients who had personally identifiable information that was neither medical nor their Social Security number. BlueCross Blue Shield also reported receiving fewer than 10 requests for credit restoration services from those who had their Social Security numbers exposed.

**UPDATE** (3/14/2012): Blue Cross Blue Shield of Tennessee (BCBST) reached a $1.5 million resolution agreement with the U.S. Department of Health and Human Services. BCBS of Tennessee kept the drives and network data closet in a facility that was secured by a property management company. The closet was secured by biometric and keycard scan security with a magnetic lock and an additional door with a keyed lock. BCBST eventually vacated most of the leased office space. Thieves may have taken the opportunity to steal the 57 unencrypted hard drives from the closet while the space was not fully occupied.

**Information Source:** Dataloss DB

**January 14, 2010**  
**Perinton Square Post Office**  
**Perinton, New York**

A group of thieves was able to obtain letters from an outdoor mailbox. They used the information to forge around $75,000 worth of checks; and affected 20 victims.

**Information Source:** Databreaches.net

**January 12, 2010**  
**Suffolk County National Bank**
Hackers have stolen the login credentials for more than 8,300 customers of small New York bank after breaching its security and accessing a server that hosted its online banking system. The intrusion at Suffolk County National Bank happened over a six-day period that started on November 18. It was discovered on December 24 during an internal security review. In all, credentials for 8,378 online accounts were pilfered, a number that represents less than 10 percent of SCNB’s total customer base.

**Information**
**Source:** Dataloss DB
**BSF** **PHYS** **Unknown**
**January 12, 2010**

The financial planning company left sensitive retirement information in a publicly accessible dumpster. The information included account ID numbers, personal addresses, and Social Security numbers. Information about people living in Shreveport, Haughton, Minden, Monroe, Farmerville, Eros and Downsville, Louisiana was found. Information from people living in Orange, Port Neches, Vidor and Deweyville, Texas was also found.

**Information**
**Source:** NAI
**Records from this breach used in our total:** 0

An electronic storage device stolen from an employee's car in Sacramento last month contained health information from 15,500 patients, including about 800 in the Fresno area. Information included patient names, medical-record numbers and, for some individuals, ages, dates of birth, gender, phone numbers and other information related to their care and treatment.

**Information**
**Source:** Dataloss DB
**EDU** **HACK** 13,000
**January 6, 2010**

Hackers breached the security of a computer server containing the names, phone numbers and employee ID numbers of current and former Eugene School District employees. The server in question did not contain other personal information but was attached to servers that contain Social Security numbers and other sensitive data. It is possible that the individuals responsible may have accessed names, addresses, dates of birth, Social Security numbers, tax identification numbers and direct-deposit bank account information for current and former staff members.

**Information**
**Source:** Dataloss DB
**Records from this breach used in our total:** 13,000

Inmates used the library logs at Passaic to obtain the personal information of other inmates. The inmates then called outside conspirators in order to defraud American Express and inmates of over $450,000. Fake American Express credit cards were created from the information and used to deposit funds into Bank of America accounts or to make purchases. The scheme occurred between September of 2007 and April of 2008.

**Information**
**Source:** Dataloss DB
**GOV** **DISC** **Unknown**
**January 6, 2010**

The names, addresses and bank account numbers of people who wrote checks to the ABVI were misused by a former employee in 2008 and 2009. The employee was part of a larger check fraud and identity theft operation that was uncovered by police. Clients and donors generally had fewer than one thousand dollars taken from their accounts.

**Information**
**Source:** Dataloss DB
**NGO** **INS** 50
**January 5, 2010**

Personal documents relating to section 8 were left in an unsecured and abandoned office. The documents included copies
of birth certificates, driver's license numbers, pay stubs, and Social Security cards.

Information Source: NAID

January 5, 2010  
Metropark  
Los Angeles, California  
BSR DISC Unknown

Personal documents were found at the Palisades Mall in West Nyack, New York. The documents had names, Social Security numbers, contact information, and other personal information. They appeared to be mishandled applications from a clothing store called Metropark.

Information Source: Databreaches.net

January 5, 2010  
Milagros II Home Health  
Alamo, Texas  
MED PHYS Unknown

A man found files with names, Social Security numbers, addresses, and phone numbers on his way to the grocery store. Some were blowing in the wind and others were lying in the street. All appear to be from Milagros II Home Health in Weslaco.

Information Source: Dataloss DB

January 3, 2010  
Logan International Airport  
Boston, Massachusetts  
GOV INSD 16

A Lynn couple is accused of selling the identities of at least 16 TSA workers at Logan. The ID data was taken by a female TSA contract worker who is related to one of the two Lynn suspects. The couple got the stolen TSA employee names from their niece, a contract clerical worker in the TSA human resources department at Logan. She no longer works there. The couple sold the names, Social Security numbers and dates of birth for $40 each to a contact who set up phony cable, gas and cell phone accounts.

UPDATE (12/17/10): One member of the couple pleaded guilty to conspiracy, misrepresenting a Social Security number with intent to defraud, possessing 15 or more unauthorized access devices with intent to defraud and aggravated identity theft. The other member of the couple previously pleaded guilty to other charges. Sentencing is scheduled for February and March of 2011.

UPDATE (5/17/2011): Michael Derring, AKA Michael Washington, was sentenced to five years of prison for his role in selling personal information of TSA workers. He was also sentenced to three years of supervised release and ordered to pay more than $50,000 in restitution.

Information Source: Dataloss DB

January 3, 2010  
Eastern Bank  
Lynn, Massachusetts  
BSF DISC 2,499

The bank account information of 2,499 customers was incorrectly mailed.

Information Source: Dataloss DB

January 1, 2010  
collective2.com  
Tenafly, New Jersey  
BSO HACK 25,000

Users of the do-it-yourself trading site collective2.com received an “urgent” e-mail notifying them that the company's computer database had been breached by a hacker and that all users should log in to change their passwords immediately. That e-mail stated that the information accessed by the hacker included names, e-mail addresses, passwords and credit card information.

Information Source: Media

January 1, 2010  
Washington Department of Corrections, Larch Corrections Center  
Tumwater, Washington  
GOV PHYS 43

A briefcase full of sensitive personnel records was stolen from the vehicle of a Larch Corrections Center manager. Larch human resources manager reportedly took the records home over last weekend to review them, then left his briefcase on the seat of his car while he worked out at the 24-Hour Fitness Center. While he was inside, someone smashed a window in the car. He returned to find the briefcase and 43 files missing. Others had spilled out of the briefcase inside the car. He took the files home to conduct an annual review required by the U.S. Department of Homeland Security. The files contained forms known as I-9s, which provide documentation that employees are legally able to work in the United States. They included driver’s license and Social Security information such as home addresses and dates of birth.
A class action suit was filed against Netflix, Inc., in United States District Court for the Northern District of California. Plaintiffs in the suit are claiming that Netflix has “perpetrated the largest voluntary privacy breach to date.” According to the Complaint, Netflix knowingly and voluntarily disclosed the sensitive and personal information of approximately 480,000 Netflix subscribers when Netflix provided participants in a contest initiated to improve Netflix’s movie recommendation systems with data sets containing over 100 million subscriber movie ratings and preferences. Netflix has claimed that the data sets provided to the contest participants were anonymized and that the subscribers’ movie ratings were accompanied only by “a numeric identifier unique to the subscriber” (as opposed to the subscriber’s name or other personal information). However, the complaint cites the results of several researchers who, in fact, were able to crack Netflix’s anonymization process and identify individual subscribers.

Information Source: Netflix

January 1, 2010
Los Gatos, California
BSO UNKN 100 million not added to total

Patients were notified on that a computer or laptop was stolen. The protected health information of patients was on the computer. The location of the theft was not reported.

Information Source: Ashley and Gray DDS

January 1, 2010
Independence, Missouri
MED STAT 9,309 (Unknown amount of SSNs and financial information)

Eastern Washington University is trying to notify up to 130,000 current or former students whose names, Social Security numbers and dates of birth were on a computer network involved in a security breach. The student information goes back to 1987. The notification process could take up to two weeks. The University recently discovered the breach during an assessment of its network. Information-technology staff also discovered that the hacker installed software to store and share video files on the system.

Information Source: Eastern Washington University

December 31, 2009
Cheney, Washington
EDU HACK 130,000

The incident occurred in Florida. The location listed is the corporate headquarters.

Information Source: Time Inc., Harvard Business Review

December 31, 2009
New York, New York
MED INSD Unknown

A customer service center employee may have misused customer credit card information.

UPDATE (8/09/10): Harvard Business Review customers were affected as well.

Information Source: Providence Health

December 28, 2009
Portland, Oregon
MED DISC 4,500

Providence Health Plans is re-issuing thousands of insurance cards after personal information was accidentally sent to the wrong policy-holders. Officials with Providence Health Plans say about 4,500 mailings were sent out with the incorrect group and member ID numbers, meaning that some policy holders received others’ information. Officials noticed the problem Monday.

Information Source: Providence Health

December 23, 2009
University Park, Pennsylvania
EDU HACK 30,000

The University sent out letters notifying those potentially affected by malware infections, which are believed responsible for breaches. The areas and extent of the records involved in the malicious software attack included Eberly College of Science, 7,758 records; the College of Health and Human Development, 6,827 records; and one of Penn State’s campuses outside of University Park, approximately 15,000 records.
University officials discovered that student employee information was viewable online. The information included names, addresses and Social Security numbers.

Information Source: Databreaches.net

December 18, 2009  
**Dickinson School of Law**  
Carlisle, Pennsylvania

EDU HACK 261

A computer in the Dickinson School of Law that contained 261 Social Security numbers from an archived class list was found to be infected with malware that enabled it to communicate with an unauthorized computer outside the network.

Information Source: Dataloss DB

December 17, 2009  
**North Carolina Libraries**  
Raleigh, North Carolina

EDU HACK 51,000

Library users at 25 campuses were the victims of a security breach in August. The libraries collect driver's license and Social Security numbers to help identify computer users. The information is stored on a central server in Raleigh. Other campuses affected are Alamance, Beaufort, Bladen, Blue Ridge, Brunswick, Central Carolina, College of the Albemarle, Gaston, Halifax, Haywood, Lenoir, Martin, Nash, Pamlico, Piedmont, Richmond, Roanoke-Chowan, Rowan-Cabarrus, Sandhills, Southwestern, Tri-County, Vance Granville and Wilson.

Information Source: Dataloss DB

December 15, 2009  
**U.S. Army**  
Fort Belvoir, Virginia

GOV PORT 42,000


A laptop computer belonging to a Family and Morale, Welfare and Recreation Command (FMWRC) employee was stolen. Types of information compromised included name, Social Security number, home address, date of birth, encrypted credit card information, personal e-mail address, personal telephone number and family member information.

Information Source: Dataloss DB

December 15, 2009  
**RockYou**  
Redwood City, California

BSR HACK 32 million (No SSNs or financial information reported)

The security firm Imperva issued a warning to RockYou that there was a serious SQL Injection flaw in their database. Such a flaw could grant hackers access to the service's entire list of user names and passwords in the database. Imperva said that after it notified RockYou about the flaw, it was apparently fixed over the weekend. But that's not before at least one hacker gained access to what they claim is all of the 32 million accounts; 32,603,388 to be exact. The database included a full list of unprotected plain text passwords and email addresses.

UPDATE (4/21/2011): The 32 million email addresses and passwords exposed include log in information from social networking sites like Facebook and MySpace.

On April 18, 2011 a court ruled that the loss of information caused injury. The court determined that "the unauthorized disclosure of personal information via the Internet is itself relatively new, and therefore more likely to raise issues of law not yet settled in the courts." The court also found that RockYou.com's privacy policy language, which stated that RockYou.com's servers were secure, did not automatically preclude the plaintiff's allegation that a contract had been breached because the plaintiff alleged that the servers were not secure.

UPDATE (3/27/2012): The Federal Trade Commission is alleging that RockYou violated the Children's Online Privacy Protection Act Rule (COPPA Rule) by collecting information from approximately 179,000 children. A proposed FTC settlement order requires RockYou to pay a civil penalty of $250,000 to settle COPPA charges. In addition to the penalty, the company would be barred from future deceptive claims regarding company privacy and data security, required to implement and maintain a data security program, and barred from future violations of the COPPA rule.

Information Source: Databreaches.net

(877) TBS-5060
The theft of a laptop exposed applications for study abroad students. Names and Social Security numbers were exposed. An unknown number of NH residents were affected.

**Information**

**Source:** Dataloss DB

**December 15, 2009**

*Detroit’s Health Department*

*Detroit, Michigan*

**GOV** **PORT** **5,000**

(877) 737-4780

Police are investigating two incidents in which patients’ medical records -- including social security numbers -- were stolen from the city’s health department. The first theft occurred in late October when a flash drive was stolen from a health department employee’s car. It contained files with birth certificate information for babies born in 2008 and the first half of 2009 whose parents reside in the 48202 and 48205 zip codes. Also a part of the files were information on the mothers’ names and health conditions, the fathers’ names, addresses, Medicaid numbers and social security numbers. The second incident happened over the Thanksgiving break when five computers were stolen from the immunization program at the department’s Herman Kiefer Health Complex. One of the computers contained Medicare and Medicaid seasonal flu billing information for 2008.

**Information**

**Source:** Dataloss DB

**December 11, 2009**

*Lookout Services*

*Bellaire, Texas*

**BSO** **DISC** **500**

The state of Minnesota has directed all of its agencies to stop using a Texas company state officials hired to verify the identities of new employees. A state official told MPR News that it is notifying some 500 employees that their personal data -- including names, dates of birth and Social Security numbers -- may have been accessible on the company's Web site. For more than three months, state agencies have used Lookout Services of Bellaire, Texas, to verify that new hires are authorized to work in the United States. The state had paid the company $1.50 a name to run employee data through the federal Department of Homeland Security’s E-Verify program, which confirms that a worker has legal status and a valid Social Security number.

**Information**

**Source:** Dataloss DB

**December 10, 2009**

*Bushland Elementary School*

*Bushland, Texas*

**EDU** **PHYS** **100**

A Potter County school district has improved security protecting its student records after paperwork containing Social Security numbers, family incomes and student addresses was discovered at a recycling site in Canyon. The documents listed names of about 100 students at Bushland Elementary School who were eligible for free or reduced-price meals through a federal program during the 2003-04 and 2005-06 school years. Applications for subsidized meals from more than 20 families included their Social Security numbers, incomes, addresses and phone numbers.

**Information**

**Source:** Dataloss DB

**December 7, 2009**

*Gateway Community College*

*New Haven, Connecticut*

**EDU** **HACK** **Unknown**

The College attempted to notify potential victims of a breach caused by malware discovered on campus computers. College alumni who donated to the College, potential donors, and students receiving scholarships between 2004 and 2006 may have been affected.

**Information**

**Source:** Databreaches.net

**December 5, 2009**

*Wake County Schools*

*Raleigh, North Carolina*

**EDU** **DISC** **5,000**

The Wake County school system accidentally sent out about 5,000 postcards with students’ Social Security Numbers printed on the front. Wake schools mailed about 15,000 reminders asking parents to specify if they want to keep their children in magnet or traditional calendar schools. About a third of those cards had the Social Security Numbers printed alongside the child’s name - a holdover from recent years when those nine-digit numbers were used to identify students.

**Information**

**Source:** Dataloss DB

**December 4, 2009**

*Eastern Illinois University*

*Charleston, Illinois*

**EDU** **HACK** **Unknown**

A computer was compromised by a virus. It caused the University’s Office of Admissions server to be infected with a number of viruses, including several that could allow an external person to access the server. The incident was
discovered during a routine security check. The investigation later determined the breach extended to two other
computers with personal data from student files or applications.

Information
Source: Dataloss DB

December 4, 2009

MedSolutions
Raleigh, North Carolina

MED DISC Unknown

For a period of time that has not been clearly defined the name, address, email, and taxpayer ID number (which in some
cases is the physician's Social Security number) for an undetermined number of NC physicians could be viewed on the
MedSolutions website. Access to this information apparently was not limited to physicians or physician staff. Based on
the information available at the time of this posting, any person with an email address could enter physician names and
view the information.

Information
Source: Dataloss DB

December 4, 2009

University of Nebraska
Omaha, Nebraska

EDU HACK 1,400

A computer in the College of Education and Human Sciences at the Lincoln campus was breached. The security breach
was discovered last month at the University of Nebraska involving the names, addresses and Social Security Numbers of
1,400 Hinsdale High School District 86 graduates. The University's investigation revealed the computer had not been
adequately secured, allowing unauthorized external access to the computer and its information.

Information
Source: Dataloss DB

December 4, 2009

Eastern Illinois University

EDU HACK 9,000

A computer was compromised by a virus. That caused the University's Office of Admissions server to be infected with a
number of viruses, including several that could allow an external person to access the server. The incident was
discovered during a routine security check. The investigation later determined the breach extended to two other
computers with personal data from student files or applications.

Information
Source: Dataloss DB

December 4, 2009

Deo B. Colburn Foundation Scholarship
Lake Placid, New York

EDU DISC 341

If you received the Deo B. Colburn scholarship for the 2003-04 academic year, your Social Security number may have been
made public. Hundreds of Social Security numbers of former students from all over the northern Adirondacks, including
Lake Placid, were released onto the Internet, potentially compromising those people's credit and financial status.
Information included names, addresses, academic institutions, the amount of money received and Social Security
numbers of the scholarship recipients.

Information
Source: Dataloss DB

December 1, 2009

Children's Hospital of Philadelphia
Philadelphia, Pennsylvania

MED PORT 942

A laptop computer containing Social Security Numbers and other personal information was stolen from a car outside an
employee's home on Oct. 20. The billing information on the computer was password-protected, but an analysis found it
was possible to decode the security controls on the laptop and gain access to the personal information.

Information
Source: Dataloss DB

November 29, 2009

Salem Housing and Community Services
Salem, Oregon

GOV DISC Unknown

Sloppy handling of confidential records by a state agency in Salem left people's names, Social Security numbers, ages
and addresses exposed in an open recycling bin outdoors. In a separate security lapse by another state agency,
confidential records with the names and Social Security numbers of former state parks and recreation employees landed
in the same recycling bin.

Information
Source: Dataloss DB

November 26, 2009

Penn State
University Park, Pennsylvania

EDU HACK 303

560
A Penn State professor's grade book from 2001 to 2004 that contained 303 students' Social Security numbers, among other personal information, was found to be compromised by a computer virus.

Information
Source: Dataloss DB
November 25, 2009  
Aurora St. Luke’s Medical Center  
Milwaukee, Wisconsin  
MED  PORT  6,400

6,400 people who were in-patients at St. Luke’s are being warned that their name, Social Security number and other information may have landed in the hands of thieves, due to a stolen laptop computer. All of the at-risk individuals were cared for there at some point by a hospitalist, a physician other than the patient’s primary care doctor, who works for an independent physician group called Cogent Healthcare. The computer was stolen from a locked office in a secure physician office building that is located adjacent to the hospital; the computer belonged to an employee of Cogent Healthcare of Wisconsin.

Information
Source: Dataloss DB
November 24, 2009  
ACORN  
San Diego, California  
BSO  DISC  Unknown

Documents that contained personnel information were accidentally thrown away in a dumpster. San Diego staff members were doing an office clean-up in preparation for a major 10-station phone bank program being set up in their offices; it appears that included in the piles of garbage being thrown out there were some documents containing private information.

Information
Source: Dataloss DB
November 24, 2009  
Farmers Insurance  
Nashville, Tennessee  
BSF  HACK  Unknown

A former insurance agent noticed that it was possible to extract client information from the website. The information included insurance policies, Social Security numbers, names and addresses. The former agent’s home was searched by police when it was discovered that client information had been hacked.

Information
Source: Databreaches.net
November 23, 2009  
Hancock Fabrics  
Baldwyn, Mississippi  
BSR  HACK  At least 140

Bank customers in California, Wisconsin and Missouri are reporting fraudulent ATM withdrawals that are tied to transactions conducted with the Hancock Fabrics retail chain. The Hancock Fabrics store in Napa was the "common thread" among the numerous people who reported credit and debit card fraud. The store had recently replaced its point-of-sale machines. At about the same time, as many as 70 Wisconsin victims reported suspicious ATM withdrawals from their accounts.

Information
Source: Dataloss DB
November 21, 2009  
Notre Dame University  
Notre Dame, Indiana  
EDU  DISC  Unknown

Notre Dame is warning university employees to keep an eye on their bank accounts after a security breach. Personal information of some past and current employees - including name, Social Security number and birth date - was accidentally posted onto a public website. The error was corrected and the information removed from the website.

Information
Source: Dataloss DB
November 20, 2009  
University Medical Center  
Las Vegas, Nevada  
MED  INSD  Unknown

Someone at UMC is selling a compilation of the hospital’s daily registration forms for accident patients. This is confidential information — including names, birth dates, Social Security numbers and injuries. Private information about accident victims treated at University Medical Center has apparently been leaking for months; allegedly so ambulance-chasing attorneys could mine for clients.

UPDATE (4/29/10): A man was indicted today by a federal grand jury in an alleged conspiracy to pay a University Medical Center employee for private information about traffic accident victims that was used to drum up clients. The man was indicted on one count of conspiracy to illegally disclose personal health information, in violation of the Health Insurance Portability and Accountability Act, better known as HIPAA. Between January and November 19, 2009 the man allegedly conspired with people, including a UMC employee, to use hospital “face sheets” to solicit personal injury cases for attorneys. The UMC employee faxed the registration sheets of trauma patients to the man on at least 55 occasions and
was paid about $8,000, the indictment said. The U.S. Attorney's press release said the man has been summoned for a May 14 hearing. If convicted, he faces up to five years in prison and a $250,000 fine.

UPDATE (5/11/2011): A man responsible for the breach was sentenced to 33 months in prison and three years of supervised release. He had been charged with conspiracy to illegally disclose personal health information.

A woman who worked as a patient services coordinator for Johns Hopkins Medicine has been sentenced to 18 months in prison for stealing patient information. The 31 year-old woman of Baltimore was also ordered to pay more than $200,000 in restitution. According to her plea agreement and court documents, from August 2005 to April 2007, the woman provided a conspirator with names, Social Security numbers and other identifying information of more than 100 current and former patients of Johns Hopkins. That information was used to apply for credit.

TAD Gear recently learned that their database was illegally accessed from an external source, and it appears that some customer data was taken, which may include customer names, contact information and credit card data. The possibility of a security breach came to their attention when certain customers notified them that unauthorized charges had appeared on their credit cards. Upon learning of the potential breach of security, TAD Gear immediately initiated an investigation, and took corrective steps.

An employee's laptop was stolen. The laptop contained a spreadsheet with Social Security numbers, dates of birth and names for 2,000 employees.

Thousands of Pennsylvanians are at risk for identity theft because postcards were sent to their homes with their Social Security numbers printed in plain view. The postcards were from the Universal American Action Network, a subsidiary of Universal American Insurance. 80,000 postcards with SSNs on them were sent to Universal clients throughout the country. More than 10,000 were mailed to Medicare participants in Pennsylvania.

The personal information for almost half a million Connecticut residents could be at risk after a portable disk drive disappeared from Health Net in May of 2009. Health Net is a regional health plan and the drive included health information, Social Security number and bank account numbers for all 446,000 Connecticut patients, 1.5 million nationally. The information had been compressed, but not encrypted, although a specialized computer program is required to read it. Patients in Arizona, New Jersey and New York were also affected.

UPDATE (1/22/2010): Connecticut Attorney General (AG) Richard Blumenthal is suing Health Net of Connecticut for failing to secure private patient medical records and financial information involving 446,000 Connecticut enrollees and promptly notify consumers exposed by the security breach. The AG is seeking a court order blocking Health Net from continued violations of HIPAA by requiring that any protected health information contained on a portable electronic device be encrypted. This case marks the first action by a state attorney general involving violations of HIPAA since the Health Information Technology for Economic and Clinical Health (HITECH) Act, which authorized state attorneys general to enforce HIPAA.

UPDATE (7/7/2010): Health Net and the Connecticut AG reached a $250,000 settlement in connection with this incident.

UPDATE (10/8/2010): Health Net faces an additional $375,000 fine for failing to safeguard the personal information of its members from misuse by third parties.
UPDATE (1/20/2011): The Vermont Attorney General filed a complaint and proposed settlement with Health Net, Inc. and Health Net of the Northeast, Inc. It would require Health Net to pay $55,000 in state fees, submit to a data-security audit and submit reports about the company’s information security programs throughout the next two years.

Information Source: Dataloss DB records from this breach used in our total: 1,500,000

November 17, 2009 Nebraska Workers' Compensation Court
Omaha, Nebraska

GOV HACK Unknown

Someone broke into a server that temporarily held injury reports. Whenever a worker has a job-related injury, a report is filed with the Workers’ Compensation Court and the information is temporarily stored on that server. Personal information, including birth dates and Social Security numbers, would have been on the server.

Information Source: Dataloss DB records from this breach used in our total: 0

November 10, 2009 Obsidian Financial Group
Woodbury, New York
BSF INSD Unknown

A former employee broke into a Woodbury financial services company, photocopied customers’ Social Security numbers and bank reference numbers and took the photocopied data with him when he left.

Information Source: Dataloss DB records from this breach used in our total: 0

November 7, 2009 Renal Treatment Centers Southeast, DaVita Inc.
Denver, Colorado
MED STAT Unknown

Multiple desktop computers were stolen from a facility in Dallas. The computers contained the names, addresses, Social Security numbers, insurance numbers, and other personal information of patients.

Information Source: PHIPrivacy.net records from this breach used in our total: 0

November 6, 2009 National Archives and Records Administration
College Park, Maryland
GOV STAT 250,000

The National Archives and Records Administration violated its information security policies by returning failed hard drives from systems containing personally identifiable information of current government employees and military veterans back to vendors. By agency policy, NARA is supposed to destroy the hard drives rather than return them. On two separate occasions the agency sent defective disk drives back to vendors under a maintenance contract, rather than destroying and disposing of them in-house.

UPDATE (1/12/2010): There was a rather large amount of data on this hard drive -- as much as two terabytes of data. The NARA is having to, in effect, do a forensic analysis to try to identify individuals and their information. They had a rolling production of notices to individuals. The total had been 26,000, and then their forensic contractor came up with a new group that contained as many as 150,000 names.

UPDATE (1/27/2010) Media stories now put the number of records involved at 250,000.

Information Source: Dataloss DB records from this breach used in our total: 250,000

November 6, 2009 Chaminade University
Honolulu, Hawaii
EDU DISC 4,500

www.chaminade.edu/infosecure
infosecure@chaminade.edu

Chaminade University inadvertently posted confidential information, including Social Security numbers, of thousands of students, on its Web site for months. An investigation determined the report was placed on obscure -- though publicly accessible -- Web pages because of human error, according to a university news release. The information was accessible for about eight months, although there is no evidence of its use, officials said. The university estimates that personally identifiable data for 4,500 students were in the report. Those affected include undergraduate students who attended the university from 1997 to 2006.

Information Source: Dataloss DB records from this breach used in our total: 4,500

November 6, 2009 MassMutual
Springfield, Massachusetts
BSF HACK Unknown

According to MassMutual, a "limited amount" of personal employee information maintained in a database by an outside vendor may have been subject to unauthorized access. The vendor engaged a forensics team to investigate, and at this time they believe that no misuse of the information or fraudulent activity involving the data has occurred. This database does not include client or field representative information; it also did not contain personal Social Security or bank...
A portable electronic device that may have contained protected health information was stolen from the vehicle of a DHSS employee on or around October 12, 2009. The Health and Human Services (HHS) Office for Civil Rights (OCR) began an investigation after the incident. OCR found evidence that DHSS did not have adequate policies and procedures in place to safeguard ePHI. DHSS was also found to have not completed a risk analysis, implemented sufficient risk management measures, completed security training for its workforce members, implemented device and media controls, or addressed device and media encryption as required by the HIPAA Security Rule. Alaska DHSS agreed to pay a $1,700,000 settlement.

Hundreds of people in Kentuckiana are worrying about identity theft after their employer accidentally released their Social Security numbers. 350 names and Social Security numbers of hospital employees appear on a list that was circulated in an e-mail.

Police in three Ohio cities are investigating the theft of three large storage bins from bank branches earlier this month. The storage bins were used to store paper waiting to be shredded. Three branches of the FirstMerit Bank in Streetsboro, Westlake and Elyria, OH each reported a bin missing beginning on October 7. One of the three bins contained personal documents of bank customers.

Personally identifiable information on members of CalOptima, a Medicaid managed care plan, may have been compromised after several CDs containing the information went missing. The unencrypted data on the CDs includes member names, home addresses, dates of birth, medical procedure codes, diagnosis codes and member ID numbers, and an unspecified number of Social Security numbers. The discs had been put in a box and sent via certified mail to CalOptima by one of its claims-scanning vendors, according to a statement by the health plan. CalOptima received the external packaging material minus the box of discs.

A Bullitt County Public Schools employee accidentally sent an e-mail message to about 1,800 school district workers that included the names and Social Security numbers of 676 district employees. The employees were identified as not having completed the district’s 2010 open-enrollment process for insurance, and the e-mail was intended as a reminder to complete the process.

Roane State Community College has announced that the names and Social Security numbers of 9,747 current or former students were on a data storage device stolen from an employee's vehicle, along with 1,194 current/former employees’ information. The Social Security numbers alone, with no names, were also stolen for 5,036 additional current or former
students. The data was on a 4GB USB drive used for work-related purposes. An employee took it home to do work after hours, and left it in the car. The employee forgot to lock the car doors. The USB drive was stolen along with a personal hand-held device.

Information Source: Dataloss DB

October 20, 2009 ChoicePoint
Alpharetta, Georgia BSO DISC 14,023

http://www.ftc.gov/opa/2009/10/choicepoint.shtm

ChoicePoint has been fined $275,000 by the U.S. Federal Trade Commission for a data breach that exposed personal information of 13,750 people last year. In April 2008, ChoicePoint turned off a key electronic security tool that it used to monitor access to one of its databases and failed to notice the problem for four months, according to an FTC statement. During that period, unauthorized searches were conducted for 30 days on a ChoicePoint database that contained Social Security numbers and other sensitive information.

UPDATE (9/22/10): The Federal Trade Commission mailed checks worth $18.17 to 14,023 ChoicePoint customers. These checks were meant to cover the money and time customers spent monitoring their credit after ChoicePoint's 2008 breach. ChoicePoint had been ordered to implement a comprehensive information security program after a 2006 breach. Due to ChoicePoint's failure to do this, they suffered another breach and were fined.

Information Source: Dataloss DB

October 17, 2009 Feeney Insurance Agency
Pittsburgh, Pennsylvania BSF STAT Unknown

A break in resulted in the theft of an unencrypted computer. The computer contained contact information, Social Security numbers, birth dates, and driver's license numbers.

Information Source: Databreaches.net

October 15, 2009 Virginia Department of Education
Richmond, Virginia EDU PORT 103,000

(877) 347-5224

A flash drive containing the personal information of more than 103,000 former adult education students in Virginia was misplaced. The information included names, Social Security numbers and employment and demographic information. The flash drive contained information on all students who finished an adult education course in Virginia from April 2007 through June 2009 or who passed a high school equivalency test between January 2001 and June 2009.

Information Source: Dataloss DB

October 15, 2009 Halifax Health
Daytona Beach, Florida MED PORT 33,000

A laptop computer from a Halifax Health employee's vehicle in Orange County was stolen -- which might have contained password protected patient information.

Information Source: Dataloss DB

October 15, 2009 PayChoice
Moorestown, New Jersey BSF HACK Unknown

Hackers broke into the company's servers and stole customer user names and passwords. The attackers then included that information in e-mails to PayChoice's customers warning them that they needed to download a Web browser plug-in in order to maintain uninterrupted access to onlineemployer.com. The plug-in was instead malicious software designed to steal the victim's user names and passwords.

Information Source: Dataloss DB

October 13, 2009 Pitt County Memorial Hospital
Greenville, North Carolina MED PORT 1,700

(877) 676-0376

Patient names and Social Security numbers were placed onto a portable computer storage device, used to move the information between different computer systems. Employees have since discovered that USB flash drive is missing from where it was stored.
Boxes full of documents that had the CLP Skilled Trade Solutions logo on them were found in a dumpster in the back of a Newport Café. Some of the information found included Social Security cards, tax papers, driver’s licenses and home IDs. Many of the documents were from a company that CLP acquired a few years ago.

A file containing identifying information for every physician in the country contracted with a Blues-affiliated insurance plan was on a laptop computer stolen from a BlueCross BlueShield Assn. employee. The file included the name, address, tax identification number and national provider identifier number for about 850,000 doctors. Some 16% to 22% of those physicians listed -- as many as 187,000 -- used their Social Security numbers as a tax ID or NPI number.

A recent breach involved a U.S. Army Special Forces document containing the names, Social Security numbers, home phone numbers and home addresses of 463 soldiers. The document also contained names and ages of soldiers’ spouses and children. The document was discovered in connection with a Congressional move to address the continuing risk of data leaks on peer-to-peer (P2P) networks. Through its research, the firm, Tiversa, turned up the document among 240 others belonging to federal government agencies and military branches, all sitting on P2P networks.

Suffolk Community College has agreed to pay a company for the next year to monitor the credit of 300 students whose last names and Social Security numbers were mistakenly listed in an attachment to an e-mail sent to those students last month.

The issue involves a defective hard drive the agency sent back to its vendor for repair and recycling without first destroying the data. The hard drive helped power eVetRecs, the system veterans use to request copies of their health records and discharge papers. When the drive failed last year, the agency returned the drive to GMRI, the contractor that sold it to them, for repair. GMRI determined it couldn’t be fixed, and ultimately passed it to another firm to be recycled. The drive was part of a RAID array of six drives containing an Oracle database that held detailed records on 76 million veterans, including millions of Social Security numbers dating to 1972, when the military began using individuals’ Social Security numbers as their service numbers.

Officials at Penrose Hospital believe someone has stolen the personal information of 175 patients. The missing information consists of names, addresses, phone numbers, Social Security numbers and the reason for the patients’ visits. The information was stored on a computer print-out and kept in a binder stored in a cabinet. The print out has gone missing.

The issue involves a defective hard drive the agency sent back to its vendor for repair and recycling without first destroying the data. The hard drive helped power eVetRecs, the system veterans use to request copies of their health records and discharge papers. When the drive failed last year, the agency returned the drive to GMRI, the contractor that sold it to them, for repair. GMRI determined it couldn’t be fixed, and ultimately passed it to another firm to be recycled. The drive was part of a RAID array of six drives containing an Oracle database that held detailed records on 76 million veterans, including millions of Social Security numbers dating to 1972, when the military began using individuals’ Social Security numbers as their service numbers.

Officials at Penrose Hospital believe someone has stolen the personal information of 175 patients. The missing information consists of names, addresses, phone numbers, Social Security numbers and the reason for the patients’ visits. The information was stored on a computer print-out and kept in a binder stored in a cabinet. The print out has gone missing.
A hacker has infiltrated a computer server housing the personal data of 236,000 women enrolled in a UNC Chapel Hill research study. The Social Security numbers of 163,000 participants were among the information exposed. The data is part of the Carolina Mammography Registry, a 14-year-old project that compiles and analyzes mammography data submitted by radiologists across North Carolina.

**UPDATE (10/6/10):** A lead researcher at the University is fighting a demotion and pay cut that resulted from the data breach in the medical study she directs. It appears that the incident first occurred in 2007 and was not discovered until 2009. An attorney representing the researcher claims that his client is not at fault because the University knew that the program's computer system had security deficiencies in 2006. The University claims that the researcher acted negligently, but the attorney claims that the researcher was not alerted to the security flaws and there is no evidence that the researcher violated or ignored rules in obtaining patient information.

**UPDATE (5/9/2011):** The researcher and University reached a settlement. The researcher agreed to retire at the end of 2011 and will receive her full rank and salary until that time.

**Information**

**Source:** Dataloss DB

**September 25, 2009**

**Tennessee Department of Human Services**

Nashville, Tennessee

GOV DISC Unknown

Various doctors' offices in Tennessee were involved.

Doctors' offices in Tennessee have been accidently sending patient information, including Social Security numbers and medical histories, to an Indiana businessman's fax machine for the past three years. The sensitive medical information was supposed to be sent to the Tennessee Department of Human Services, but the owner of SunRise Solar Inc. in Indiana, says hundreds of confidential medical faxes having been coming to him.

**Information**

**Source:** Dataloss DB

**September 23, 2009**

**Eastern Kentucky University**

Richmond, Kentucky

EDU DISC 5,045

(859) 622-7777, ecert@eku.edu

The names and Social Security numbers of about 5,000 Eastern Kentucky University faculty, staff and student workers were posted inadvertently on the Internet last September, where they have been displayed for a year.

**Information**

**Source:** Dataloss DB

**September 22, 2009**

**Bernard Madoff Investors**

Dallas, Texas

BSF PORT 2,246

More than 2,200 Bernard Madoff investors are learning that some of their personal and financial information has potentially been breached after the theft of a laptop in Dallas. The names, addresses, Social Security numbers and some Madoff account information on 2,246 investors was contained in a computer stolen from the car of an employee of AlixPartners Llp.

**Information**

**Source:** Dataloss DB

**September 22, 2009**

**Sagebrush Medical Plaza/Kern Medical Center**

Bakersfield, California

MED PHYS 31,000

Thousands of patients at a Kern County health clinic have been warned their personal information could have been stolen. A break-in happened at the Sagebrush Medical Plaza in July, and Kern Medical Center officials have notified 31,000 patients to take precautions against possible identity theft. One or more unknown individuals broke into a locked storage area that contained confidential patient information. All patient information has now been moved to a location inside the clinic building.

**Information**

**Source:** Dataloss DB

**September 21, 2009**

**Rocky Mountain Bank**

Pinedale, Wyoming

BSF DISC 1,325

A customer of the Rocky Mountain Bank asked a bank employee to send certain loan statements to a representative of the customer. The employee, however, inadvertently sent the e-mail to the wrong Gmail address. Additionally, the employee had attached a sensitive file to the e-mail that should not have been sent at all. The attachment contained confidential information on 1,325 individual and business customers that included their names, addresses, tax identification or Social Security numbers and loan information.

**Information**

**Source:** Dataloss DB

**September 17, 2009**

**Akron Children's Hospital**
A 38-year-old Avon Lake, Ohio, man is set to plead guilty to federal charges after spyware he allegedly meant to install on the computer of a woman he'd had a relationship with ended up infecting computers at Akron Children's Hospital. He allegedly sent the spyware to the woman's Yahoo e-mail address, hoping that it would give him a way to monitor what she was doing on her PC. But instead, she opened the spyware on a computer in the hospital's pediatric cardiac surgery department, creating a regulatory nightmare for the hospital. Between March 19 and March 28 the spyware sent more than 1,000 screen captures via e-mail. They included details of medical procedures, diagnostic notes and other confidential information relating to 62 hospital patients. He was also able to obtain e-mail and financial records of four other hospital employees as well, the plea agreement states.

Information Source: Dataloss DB

Downeast Energy & Building Supply
Brunswick, Maine

Downeast sent a notice after discovering that hackers had broken in and stolen more than $200,000 from the company's online bank account. Sometime prior to September, attackers planted keystroke logging malware on Downeast's computer systems, and stole the credentials the company uses to manage its bank accounts online. Hackers had gained access to the bank account the company uses to let customers pay for fuel with electronic transfers from their checking accounts. Then, on or around Sept. 2, the hackers used that access to initiate a series of sub-$10,000 money transfers out of the company's account to at least 20 individuals around the United States who had no prior business with Downeast Energy. The personal information to which the thieves had access included customers' names, banks and checking account numbers.

Information Source: Dataloss DB

University of Florida
Gainesville, Florida

(866) 876-HIPA (4472)

In August, the University's Privacy Office was notified of a privacy breach after the discovery of an unprotected computer file containing 34 names and 25 Social Security numbers. It's believed the personal information belongs to trainers working with the Florida Traffic and Bicycle Safety Education program in 2006. The file was immediately removed.

Information Source: Dataloss DB

Jones General Store/Root of the Hill
Boulder, Colorado

Boulder police are investigating two burglaries on University Hill that could have compromised some local shoppers' personal and credit card information. A manager for Jones General Store called police to report an overnight break-in and theft of credit card receipts. A short time later, an owner of Root of the Hill, a business in the same building, called officers to report a break-in, theft and extensive vandalism.

Information Source: Dataloss DB

School for the Physical City High School
New York, New York

Boxes of student records were piled in the street in front of the old home of the School for the Physical City. Some records contained the Social Security numbers, grades, signatures and even psychological reports of former students of the public intermediate high school. The boxes contained hundreds of records and were sitting next to a trash bin filled with old desks and other discarded school supplies. The School for the Physical City moved to a new location over the summer and apparently the records were thrown out with the trash during the relocation.

UPDATE (9/12/10): A parent and child are suing the New York City Department of Education.

Information Source: Dataloss DB

Mitsubishi Corp.
New York, New York

A Mitsubishi Corp. Internet shopping unit lost credit card details on 52,000 customers after its servers were hacked from overseas. The company has informed customers and relevant authorities of the leaks and has suspended the Web site until it can improve the system.

Information Source: Dataloss DB
A file containing the personal information including Social Security numbers of nearly 100 students at the Bluegrass Community and Technical College has been stolen.

Information Source: Dataloss DB

Naval Hospital Pensacola will be notifying thousands of beneficiaries who use its pharmacy services, following the disappearance of a laptop computer. The computer's database contains a registry of 38,000 pharmacy service customers' names, Social Security numbers and dates of birth on all patients that used the pharmacy in the last year. It does not contain any personal health information.

Information Source: Dataloss DB

Medical files were found in a dumpster. It seems a third party moving company was hired to transfer the boxes from one warehouse to another. It is unknown at this time how the files ended up in the dumpster. The information in the files contained Social Security numbers, driver's license copies, medical histories, and employers.

**UPDATE** (5/24/10): Prompt Med agreed to pay a $50,000 fine to the state of North Carolina.

Information Source: Dataloss DB

Nearly a year ago, hackers broke into a computer server that contained Social Security numbers and a very limited amount of credit card information for graduates of University of Massachusetts. Hackers gained access to one server on the university's computer system, which held information of students who attended UMass between 1982 and 2002, as well as a few who attended before 1982. A UMass spokesman declined to say how many people's records were exposed, except that it was a large number of undergraduate and graduate students who attended the university during the 20-year period.

Information Source: Dataloss DB

The theft of two desktop and 12 laptop computers from an office at Cal State Los Angeles is causing identity theft concerns for more than 600 students and faculty members. Someone broke a window in the office of the university's Minority Opportunities in Research program to steal the computer. The computers stolen contained individual names, Social Security numbers and addresses, according to campus.

Information Source: Dataloss DB

A Northern Kentucky University employee's laptop computer - which contained personal information about some current and former students -- was stolen from a restricted area. The personal information stored on the employee's computer included Social Security numbers of at least 200 current and former students.

Information Source: Dataloss DB

Some American Express card members' accounts may have been compromised by an employee's recent theft of data. The former employee has been arrested and the company is investigating how the data was obtained. American Express
declined to disclose any more details about the incident. The company has put additional fraud monitoring and protection controls on the accounts at issue.

**Information**

**Source:** Media

**August 14, 2009** Calhoun Area Career Center
Battle Creek, Michigan

Personal information from 455 students at Calhoun Area Career Center during the 2005-2006 school year was available online for more than three years. The information included names, Social Security numbers, 2006 addresses and telephone numbers, birth dates and school information. There were about 1,000 students at the career center during that time, but an investigation by the Calhoun County Intermediate School district found that information for 455 students was available.

**Information**

**Source:** Dataloss DB

**August 13, 2009** National Guard Bureau
Arlington, Virginia

An Army contractor had a laptop stolen containing personal information on 131,000 soldiers. The stolen laptop contained personal information on soldiers enrolled in the Army National Guard Bonus and Incentives Program. The data includes names, Social Security numbers, incentive payment amounts and payment dates.

**Information**

**Source:** Dataloss DB

**August 11, 2009** Bank of America Corp.
Charlotte, North Carolina

Charlotte-based BoA (NYSE:BAC) and Citigroup (NYSE:C) each recently issued replacement cards to consumers, telling them that their account numbers may have been compromised. Account information from certain Bank of America debit cards may have been compromised at an undisclosed third-party location. Bank officials are not certain if this is a new breach or a previously disclosed one.

**Information**

**Source:** Media

**August 11, 2009** Citigroup Inc.
New York, New York

Citigroup (NYSE:C) recently issued replacement cards to consumers and told them that their account numbers may have been compromised. Citigroup told credit-card customers in Massachusetts that their account numbers may have been illegally obtained as a result of a merchant database compromise and could be at risk for unauthorized use. Bank officials are not certain if this is a new breach or a previously disclosed one.

**Information**

**Source:** Media

**August 11, 2009** University of California, Berkeley School of Journalism
Berkeley, California

[https://security.berkeley.edu/school-info](https://security.berkeley.edu/school-info)

Campus officials discovered during a computer security check that a hacker had gained access to the journalism school’s primary Web server. The server contained much of the same material visible on the public face of the Web site. However, the server also contained a database with Social Security numbers and/or dates of birth belonging to 493 individuals who applied for admission to the journalism school between September 2007 and May 2009.

**Information**

**Source:** Dataloss DB

**August 4, 2009** New Hampshire Department of Corrections
Laconia, New Hampshire

A 64-page list containing the names and Social Security numbers of about 1,000 employees of the state Department of Corrections ended up under the mattress of a minimum security prisoner. The prison contracts with vendors to shred documents and investigators are trying to find out why documents were not destroyed.

**Information**

**Source:** Dataloss DB

**August 3, 2009** National Finance Center
Washington, District Of Columbia

<table>
<thead>
<tr>
<th>Source</th>
<th>Records from this breach used in our total: 1,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media</td>
<td></td>
</tr>
<tr>
<td>Dataloss DB</td>
<td></td>
</tr>
</tbody>
</table>
An employee with the National Finance Center mistakenly sent an Excel spreadsheet containing the employees' personal information to a co-worker via e-mail in an unencrypted form. The names and Social Security numbers of at least 27,000 Commerce Department employees were exposed.

**Information Source:**  
**Media**  
**August 1, 2009**  
**Williams Cos. Inc.**  
**Tulsa, Oklahoma**  
BSO PORT 4,400

A laptop containing personal and compensation information for more than 4,400 current and former employees was stolen from a worker’s vehicle. The computer had names, birth dates, Social Security numbers and compensation data for every Williams employee since Jan. 1, 2007.

**Information Source:**  
**Dataloss DB**  
**July 31, 2009**  
**Jackson Memorial Hospital**  
**Miami, Florida**  
MED INSD 3,360 (No reports of SSNs or financial information)

A Miami man was charged with buying confidential patient records from a Jackson Memorial Hospital employee over the past two years, and selling them to a lawyer suspected of soliciting the patients to file personal-injury claims.

**UPDATE** (10/26/10): Ruben E. Rodriguez was sentenced to 11 years in prison for selling patient records to lawyers for injury claims. Rodriguez stole 3,350 patient records in 2008 and 2009. He may have also sold information in 2007. The information included name, contact information and medical diagnoses.

**Information Source:**  
**Media**  
**July 29, 2009**  
**University of Colorado, Colorado Springs**  
**Colorado Springs, Colorado**  
EDU PORT 766

The university is notifying nearly 800 students and alumni that some of their personal information may have been on a stolen laptop. That laptop was taken from a professor’s home on July 5th after the home was burglarized. The laptop contained class roster information - name, student ID number, e-mail address, graduating class year and grade information - for current and past UCCS students. No financial information was stored on the laptop, but there is a possibility that Social Security numbers may have been involved for students enrolled prior to summer, 2005.

**Information Source:**  
**Dataloss DB**  
**July 24, 2009**  
**Hampton Redevelopment and Housing Authority**  
**Hampton, Virginia**  
NGO DISC 900

The Social Security numbers and other personal information of nearly 900 people who were banned from public housing in Hampton were accidentally given to a resident who requested the information. A housing authority employee printed a spreadsheet and mailed it but forgot to exclude the personal information.

**Information Source:**  
**Dataloss DB**  
**July 24, 2009**  
**Network Solutions**  
**Herndon, Virginia**  
BSO HACK 573,000

Hackers have broken into Web servers owned by domain registrar and hosting provider Network Solutions, planting rogue code that resulted in the compromise of more than 573,000 debit and credit card accounts over the past three months. Network Solutions discovered that attackers had hacked into Web servers the company uses to provide e-commerce services - a package that includes everything from Web hosting to payment processing -- to at least 4,343 customers, mostly mom-and-pop online stores. The malicious code left behind by the attackers allowed them to intercept personal and financial information for customers who purchased from those stores.

**Information Source:**  
**Dataloss DB**  
**July 22, 2009**  
**A Honolulu hospital**  
**Honolulu, Hawaii**  
MED INSD Unknown

In June 2009, a Hawaii woman was sentenced to a year in prison for illegally accessing another woman's medical records and posting on MySpace that she had HIV. The State of Hawaii brought charges under a state law that criminalizes unauthorized access to a computer as a class B felony. The defendant was employed by a hospital and had access to patient medical records.
July 17, 2009  Francis Howell School District  St. Charles, Missouri

EDU  PORT  1,700

A laptop computer theft could have compromised personal information. The computer could have contained names and Social Security numbers for 1,700 non-certified employees. Anyone who worked for the district from 2005 through 2008 could be affected. The computer belonged to a Francis Howell employee in the district human resources department.

July 16, 2009  Moores Cancer Center  San Diego, California

MED  HACK  30,000

A hacker breached the Center’s computers and gained access to patients’ personal information. A letter was sent to 30,000 patients informing them that their personal information may have been in the compromised databases. Types of information in breach included names, dates of birth, medical record number, diagnosis and treatment dates and some Social Security numbers. The majority of patients’ information did not include Social Security numbers.

July 16, 2009  Elance  Mountain View, California

http://www.elance.com/p/trust/account_security.html

BSO  HACK  Unknown

A warning from Elance’s customer service was emailed, saying that the site has been hacked or attacked in some way. The data accessed was contact information - specifically name, email address, telephone number, city location and Elance username. This incident did not involve any credit card, bank account, social security or tax ID numbers.

July 14, 2009  Canyons School District  Cottonwood Heights, Utah

EDU  PORT  6,000

Canyons School District officials are investigating the disappearance of a thumb drive that contained the personal information of more than 6,000 current and recent employees. The USB flash drive is believed to have contained employee addresses, phone numbers, dates of birth and Social Security numbers. A district-level worker was using it to transfer data for apparently legitimate, job-related purposes.

July 14, 2009  Leander School District  Leander, Texas

EDU  UNKN  Unknown

School officials sent a notice home with special needs students to alert parents that someone gained access to private information. It appears that one individual gained unauthorized electronic access to confidential information.

July 13, 2009  Florida Department of Education  Tallahassee, Florida

GOV  PHYS  475

The agency is notifying 475 student-loan borrowers of a breach that involved their financial records. The Office of Student Financial Assistance lost or misplaced 1,186 promissory notes that students signed while enrolled. The missing files include Social Security numbers, names, addresses, birth dates, personal references, and other private and financial information that could be used for identity thief.

July 13, 2009  LexisNexis  Dayton, Ohio

BSO  UNKN  13,329

LexisNexis has warned more than 13,000 consumers that a Florida man who is facing charges in an alleged mafia racketeering conspiracy may have accessed some of the same sensitive consumer databases that were once used to track terrorists. The accused would provide names, addresses and account numbers as part of a fake check-cashing operation. But he’s also accused of using computer databases to get information on potential extortion or assault targets as well as individuals suspected by the Enterprise members of being involved with law enforcement.
Northern California dumpsters Bay Area to Central Valley
San Francisco, California

BSF PHYS 1,500

A criminal complaint filed against 30-year-old suspect claims that he made more than 1,000 fake ID cards that he used to rip off people, stores and banks. He also allegedly admitted to stealing the identities of more than 500 people all across Northern California, ranging from the Bay Area to the Central Valley. Federal agents say the man said it was easy to find new victims: All he needed to do was visit a local bank and search their dumpsters. Using the sensitive materials he found in the trash, He was able to use a computer to mock up fake identification cards and blank checks, according to authorities. He also allegedly confessed to stealing between one to two million dollars in cash and merchandise.

Mountain Medical Center
Salt Lake, Utah

MED PHYS Unknown

Names, credit card numbers, Social Security numbers were found in a dumpster. A man was throwing away some stuff in a dumpster and found it was chock full of medical records. There’s everything in there from canceled checks to routing numbers, he said. Salt Lake Police packed away perhaps twenty boxes of papers, and said they would protect the documents, as they dug into the matter.

AT&T
Chicago, Illinois

BSO INSD 2,100

A temporary employee for AT&T was arrested today on charges she stole personal information on 2,100 co-workers and then pocketed more than $70,000 by taking out short-term payday loans in the names of 130 of them.

Carrell Clinic
Dallas, Texas

MED HACK Unknown

An Arlington security guard was arrested on federal charges for hacking into hospital’s computer system. The defendant allegedly posted video of himself compromising a hospital’s computer system on YouTube. The system and computers contained confidential patient information.

UPDATE (3/18/2011): Phiprivacy.net reports that the former security guard was sentenced to nine years in prison for installing malware. Jesse William McGraw was employed by the security company United Protection Service while working as a security guard for Carrell Clinic. He was also the leader of a hacker gang.

Bike Nashbar
Asheville, North Carolina

custserv@nashbar.com, 1-800-NASHBAR

The company’s computer servers were hacked and credit card information was compromised. Letters with more details will be mailed to affected customers.

Sutter Health
Sacramento, California

MED PORT 6,000

Hundreds of current and former employees with Sutter Health had their personal data compromised. The company’s Sacramento Sierra region was contacted by a computer repair shop. "The repair people did the right thing and told us they had our laptop", said Sutter Communication Coordinator. The laptop contained names and Social Security numbers of 6,000 Sutter Health workers.

University of Central Missouri Police Department (UCM)
Warrensburg, Missouri

EDU INSD 250

The University sent letters to 7,000 students, but the final number of affected individuals appears to be closer to 250
After two documents containing student personal information were stolen, it was discovered that a former University police officer and his wife were responsible. They used the names, Social Security numbers, and birth dates of students enrolled in 2005 and 2006 summer sessions. The thieves fraudulently opened bank accounts, received student loans, and applied for credit and debit cards. The losses total more than $30,000.

Information
Source: Databreaches.net

June 26, 2009 Massachusetts Technology Collaborative
Boston, Massachusetts

Residents who applied for the Massachusetts Commonwealth Solar rebate program had their personal information posted on a government website for 50 minutes. One user accessed the file during the incident. Names and Social Security numbers were exposed.

Information
Source: Dataloss DB

June 24, 2009 Florida Department of Revenue
Tallahassee, Florida

The names, addresses and Social Security numbers of about 3,000 people employed by a handful of state businesses were on a password-protected flash drive stolen from the car of a Florida Department of Revenue employee in Georgia. The people were current or past employees of six large corporations that are being audited by the state.

Information
Source: Dataloss DB

June 24, 2009 Battle Creek City
Battle Creek, Michigan

Some Battle Creek city employees are getting free identity protection help after the mayor posted a document with personnel information to a public Web site. Information on city workers, including Social Security numbers, was listed on a city check registry that the mayor put online and linked to using his Twitter.com account. The registry is no longer online and the city has worked with law enforcement and Twitter, to remove any archived references to the information.

Information
Source: Media

June 23, 2009 Cornell University
Ithaca, New York

A stolen Cornell University computer has compromised the personal information of thousands of members of the University community. The computer contains the names and Social Security numbers of current and former students as well as current and former faculty and staff members.

Information
Source: Dataloss DB

June 22, 2009 Baptist Medical Center
Montgomery, Alabama

Many folders that were found in a landfill dump site were labeled “Radiology Department, Baptist Medical Center.” Hundreds of medical records were out in the open, all with sensitive information. Sensitive patient information that was thrown out included names, x-rays, ultrasounds, MRIs, and Social Security numbers. Files from at least five other facilities were found at the same site; however Baptist Medical Center is believed to be the source of the breach.

UPDATE (8/5/08): A former employee of Baptist Hospital has been sentenced to two years and one day in federal prison for wire fraud and stealing the identities of patients, according to a Department of Justice press release. Adrienne Denise Stovall, 30, pleaded guilty in January to one count of wire fraud and one count of aggravated identity theft, which carries a mandatory sentence of two years. Stovall worked at Montgomery’s Baptist Hospital from August 2006 to early 2007. Her position gave her access to the hospital’s computer system. The system contained confidential information including patient names, dates of birth, and Social Security numbers. Stovall used the information to apply for credit lines and credit cards.


Information
Source: Media

June 22, 2009 Broadridge Financial Solutions, Inc.
Jersey City, New Jersey

Broadridge Financial Solutions, Inc. provides proxy services for clients, including the processing, distribution and tabulation of Annual Meeting Proxy materials for registered shareholders of publicly traded companies. The firm inadvertently disclosed Dynegy shareholder information including name, address, Social Security number and other account information to another client. The total number of share-owners affected was not reported.
Some members of Suncoast Schools Federal Credit Union have been notified that their debit card accounts were exposed to fraud. It is the latest casualty of last year’s breach of Heartland Payment Systems, one of the country’s largest credit card processors, where information from more than 100 million credit and debit card transactions was exposed. Not until the end of May did Suncoast discover that some of its customers who use Visa Check Cards could be in danger. The Tampa credit union is issuing new cards to all members whose accounts were compromised.

A computer that was stolen from a car in Charleston, SC, last year contained personal financial information on 84,000 University of North Dakota donors. The missing laptop belonged to Daniel Island-based software giant Blackbaud Inc., which stressed that all of the information was password-protected and encrypted.

An organized-crime ring that police believe is Russian or Armenian targeted a high-volume Redondo Beach Arco gas station, assigned a low-level soldier to infiltrate it and waited eight months while he worked himself into a position where he could implant a tiny, high-tech skimmer to steal customers’ credit-card information. Armed with a fresh batch of personal-information numbers, the gang began draining thousands of Southern California bank accounts soon after Erick, the model employee who was by then entrusted with opening the station every day at 5 a.m., vanished in late April along with 1,500 packs of cigarettes, $1,000, a laptop, his employee application form - and the two digital video recorders used for surveillance. The skimmer scam left a string of more than 1,000 victims, stretching from Santa Barbara to Newport Beach.

Unauthorization access to a human resources payroll database by a former employee exposes names, addresses and Social Security numbers of past and present employees.

Someone took a storage device from a counselor’s office in Iowa City. That device contained names and Social Security numbers for participants in the PROMISE JOBS program.

A physician’s laptop was stolen from a car parked at the doctor’s home. Patient names, treatment dates, short medical treatment summaries and medical record numbers were stored on the computer. There were no home addresses, billing information or Social Security numbers stored on the laptop.

UPDATE (08/11/10): It seems that as many as 4,000 patients may have been affected and Social Security numbers were involved.
T-Mobile USA is investigating claims that a hacker has broken into its data bases and stolen customer and company information. Someone anonymously posted the claims on the security mailing list Full Disclosure. In that post, the hacker claims to have gotten access to everything -- their databases, confidential documents, scripts and programs from their servers, financial documents up to 2009. They claim they have been in touch with the carrier's competitors trying to sell the data, but have been unsuccessful. They threatened to sell it to the highest bidder. T-Mobile later confirmed a hacker obtained a document.

Information
Source:

Ohio State Dining Services
Columbus , Ohio

Student employees had their Social Security numbers accidentally leaked in an e-mail. The hiring coordinator for Dining Services, an OSU student, received an e-mail with an attachment that included students' names and SSNs. He accidentally sent the attachment in an e-mail reminding student employees to sign their waivers for the Ohio Employees Retirement System. After realizing the mistake, the hiring coordinator called the Office of Information Technology, which stopped the e-mails before all of them were sent.

Information
Source:

Virginia Commonwealth University
Richmond, Virginia

A desktop computer was stolen from a secured area within Cabell Library in mid-April. The computer may have contained student names, Social Security numbers and test scores dating from October 2005 to the present. VCU discontinued use of Social Security numbers as ID numbers in January 2007. An additional 22,500 students are being notified that their names and test scores may have also been on the computer. No Social Security numbers were recorded with those names, but computer-generated student ID numbers may have been.

Information
Source:

Maine Office of Information Technology
Augusta, Maine

Through a printing error, 597 people receiving unemployment benefits last week got direct-deposit information including Social Security numbers belonging to another person. We received a print job and were running it, and there was an equipment malfunction, Thompson said. In restarting the piece of equipment, a mistake was made and it started one page off. It was an error and our quality assurance didn’t pick it up. Recipients received one page with their own information and another page with information belonging to a different person.

Information
Source:

Aviva
Concord, New Hampshire

The data breach affected customers who opened accounts in the U.S. or beneficiaries of accounts opened in the U.S. The breach, caused by malware on an Aviva computer, happened between Dec. 30 and Feb. 24. A vendor helping Aviva locate policyholders and beneficiaries whose mail was undeliverable found 3 Aviva USA customers' Social Security numbers and other personal information while searching for them. The company believed 550 customers had their Social Security numbers exposed in this manner. Aviva says it has removed the compromised hardware and taken steps to prevent future malware attacks.

Information
Source:

University of Nevada - Las Vegas
Las Vegas, Nevada

A UNLV computer was compromised and may have allowed loss of some personal data. The College of Sciences recently sent a letter to about 20 students as officials became aware of a virus affecting a computer in the College. The College found no information was leaked, but for legal reasons they still sent the letter.

Information
Source:

Aetna
Hartford, Connecticut

May 28, 2009

Information
Source:

June 7, 2009

T-Mobile USA
Bellevue, Washington

June 6, 2009

Ohio State Dining Services
Columbus , Ohio

June 5, 2009

Virginia Commonwealth University
Richmond, Virginia

June 4, 2009

Maine Office of Information Technology
Augusta, Maine

June 3, 2009

Aviva
Concord, New Hampshire

June 1, 2009

University of Nevada - Las Vegas
Las Vegas, Nevada

May 28, 2009

Aetna
Hartford, Connecticut
Aetna has contacted 65,000 current and former employees whose Social Security numbers may have been compromised in a Web site data breach. The breach was a spam campaign showing that the intruders successfully harvested e-mail addresses from the Web site, although it’s not clear if SSNs were also obtained. The spam purported to be a response to a job inquiry and requested more personal information. Aetna sent letters last week notifying the 65,000 people whose SSNs were on the site of the breach.

**UPDATE (6/11/09):** Hartford health insurer Aetna Inc. is being sued. The class-action suit was filed in a Pennsylvania District Court and demands credit monitoring, punitive damages, costs and other relief for current, former and potential employees.

**Information Source:** Dataloss DB

**Batteries.com**

**Carmel, Indiana**

On March 13th, Batteries.com received notice from a customer about potential unauthorized activity on their credit card. They later discovered the Batteries.com network had been breached from around February 25, 2009 to April 9, 2009. The hackers stole names, addresses and credit card information.

**Information Source:** Dataloss DB

**Warren County Virtual Community School**

**Lebanon, Ohio**

Contractors installing fiber on a nearby street to the school say they found a four-page list in a recycling dumpster when they went to dump some trash. The list had more than 140 students’ names, addresses, Social Security numbers and birth dates listed. Their parents’ names were on the list too.

**Information Source:** Dataloss DB

**Indianapolis Department of Workforce Development**

**Indianapolis, Indiana**

The Department of Workforce Development is notifying approximately 4,500 unemployment recipients concerning the accidental disclosure of their Social Security number to the incorrect employer. The release occurred during the printing of DWD’s Statement of Benefit Charges by print vendor, Pitney Bowes Management Services Inc. This form is sent to companies listing those who are collecting unemployment benefits against that employer’s account. The misprinted statements contained information from individuals who did not work for that company. Approximately 1,200 companies received incorrect statements.

**Information Source:** Dataloss DB

**Texas Lottery Commission**

**Austin, Texas**

A former Texas lottery worker was arrested while training for a new job and charged with illegally possessing personal information on 140 lottery winners and employees, including their names and Social Security numbers. The man was still working for the Lottery Commission in 2007 when he allegedly took the information, which was discovered last year on a state computer at the Comptroller of Public Accounts where he later was employed.

**Information Source:** Media

**Internal Revenue Service**

**Washington, District Of Columbia**

The U.S. Treasury Inspector General for Tax Administration found in a fiscal year 2008 audit that in more than a dozen IRS document disposal facilities, old taxpayer documents were being tossed out in regular waste containers and dumpsters. In addition, the investigation found that IRS officials failed to consistently verify whether contract employees who have access to taxpayer documents had passed background checks. Further, investigators had difficulty finding anyone responsible for oversight of most of the facilities that the IRS contracted with to burn or shred sensitive taxpayer documents. The review was performed at IRS offices in Phoenix, Tempe, and Tucson, Arizona New Carrollton, Maryland Holtsville, Garden City, and Westbury, New York and Ogden, Utah, and included questionnaires to 14 Territory Managers across the country during the period September 2007 through May 2008.
A computer processing error created a single image file of 120 account statements for the month of April. Statement files are delivered to the cardholder through the website in Adobe PDF format. Because of a load error, the system failed to detect page breaks between the account statements, thus resulting in the system believing that all of the pages belonged to a single statement. As a result, the PDF image file contained 119 statements in addition to the cardholder’s statement. (Note: Monthly account statements do not include customers’ Social Security numbers or PINs.)

Information Source: Dataloss DB
May 19, 2009 National Archives and Records Administration
College Park, Maryland

The National Archives lost a computer hard drive containing massive amounts of sensitive data from the Clinton administration, including Social Security numbers, addresses, and Secret Service and White House operating procedures. The Archives had been converting the Clinton administration information to a digital records system when the hard drive went missing. The hard drive was left on a shelf and unused for an uncertain period of time. When the employee tried to resume work, the hard drive was missing.

Information Source: Dataloss DB
May 19, 2009 Rudder
Houston, Texas

Rudder, a financial management company, erred in sending users’ confidential financial information to the wrong individuals. Through an online financial planning application, hundreds of individuals were able obtain the full details on others’ finances - their salary, debts, bank balance, and where they shop. Bank account numbers were apparently not exposed.

Information Source: Media
May 18, 2009 NJ Department of Labor and Workforce Development
Trenton, New Jersey

Unemployed New Jersey residents may have had their name and Social Security number accidentally delivered to an employer for which you did not work. The error occurred when department staff last month sent first-quarter reports to businesses that included a list of former employees receiving unemployment benefits. Because some companies had laid off a significant number of employees, the reports were longer than usual, requiring staff members to stuff the envelopes by hand rather by machine. Some reports were placed in the wrong envelopes.

Information Source: Dataloss DB
May 18, 2009 Anderson Kia Car Dealership
Boulder, Colorado

Police have chained up 10 recycling bins outside Boulder’s now-defunct Anderson Kia car dealership after learning that the bins were stuffed with personal information from the dealership’s former customers. Green recycling bins were piled full with folders, each headed with an individual’s name. All of the folders contained Social Security numbers, driver’s license information, photos, phone numbers and financial information for Kia customers.

Information Source: Dataloss DB
May 13, 2009 United Food and Commercial Workers Union 555
Tigard, Oregon

A union employee’s laptop was stolen on the East Coast. The laptop may have contained personal information of Local 555 members, including birth dates and Social Security numbers.

Information Source: Dataloss DB
May 12, 2009 Johns Hopkins Hospital
Baltimore, Maryland

An investigation suggests a former employee who worked in patient registration may have been linked to a scheme to create fake drivers’ licenses in Virginia. The employee had access to information such as name, address, telephone number, mother and fathers names, dates of birth and Social Security numbers, but not to any health or medical information.

UPDATE (10/1/10 via PHIPrivacy.net): The former employee and four others were indicted for fraud and aggravated identity theft. They are charged with using patient information to create fraudulent credit accounts. The former employee
worked at the hospital between August 2007 and March of 2009. It is believed that around 600 patients may have been
targets for identity theft, but only 50 incidents were linked to the former employee.

Information
Source: Office of the State Superintendent of Education D.C.
Washington, District Of Columbia

May 11, 2009

The D.C. agency that handles college financial aid requests had accidentally e-mailed personal information from 2,400
student applicants to more than 1,000 of those applicants. An employee of the agency's Higher Education Financial
Services Program inadvertently attached an Excel spreadsheet to an e-mail. The information included student names, e-
mail and home addresses, phone and Social Security numbers and dates of birth.

Information
Source: Multiple financial institutions
New York, New York

May 11, 2009

A band of brazen thieves ripped off hundreds of New Yorkers by rigging ATMs to steal account and password information
from bank customers. The first - a skimmer - went over the slot where customers insert their ATM cards. The skimmer
read, and stored, the personal information kept in the magnetic strip on the back of the bank card. The second device was
a tiny camera hidden in the lighted signs over the ATM. The pinhole camera lens pointed directly onto the ATM keypad
and filmed victims typing in their supposedly secret PIN codes. The thieves would then create their own phony ATM cards
and use their victims' PINs to access accounts.

Information
Source: University of California, Berkeley
Berkeley, California

May 7, 2009

Hackers infiltrated restricted computer databases. Personal information of 160,000 current and former students and
alumni may have been stolen. The University says Social Security numbers, health insurance information and non-
treatment medical records dating back to 1999 were accessed. The breach was discovered April 21, 2009, when
administrators performing routine maintenance identified messages left by the hackers. They found that restricted
electronic databases had been illegally accessed by hackers beginning on October 9, 2008 and continued until April 6,
2009. All of the exposed databases were removed from service to prevent further attacks.

Information
Source: East Burke Christian Ministries
Hildebran, North Carolina

May 5, 2009

A thief broke into a charity in Burke County and stole a laptop containing more than 1,000 Social Security numbers of
individuals seeking help.

Information
Source: Fulton County Board of Registration and Elections
Atlanta, Georgia

May 5, 2009

Boxes were found in a trash bin at Atlanta Technical College. They contained about 75,000 voter registration application
cards and 24,000 precinct cards. Many of the documents contained personal information on active voters, such as full
names and Social Security numbers.

Information
Source: Spencer House Apartment Complex
Beaverton, Oregon

May 5, 2009

Residents at an apartment complex blamed apartment management Monday for leaving their personal information out in
the open. The documents were found in an unlocked public container that was sitting off a side street in their apartment
complex. The documents included Social Security numbers, addresses, phone numbers, immigration numbers and names.

Information
Source: Kapiolani Community College
Honolulu, Hawaii

May 4, 2009

http://datatheft.berkeley.edu
More than 15,000 students at Kapiolani Community College are at risk of identity theft because of an Internet security breach. School officials found that a computer was infected with malware that can steal sensitive data. The computer contained the personal information of 15,487 students who applied for financial aid between January 2004 and April 15. The computer did not have sensitive information, but it was hooked up to a network that had access to names, addresses, phone numbers dates of birth and Social Security numbers.

**Information Source:**
Dataloss DB

**May 4, 2009**

**Virginia Prescription Monitoring Program**
**Richmond, Virginia**

MED HACK 531,400

The FBI and Virginia State Police are searching for hackers who demanded that the state pay them a $10 million ransom for the return of millions of personal pharmaceutical records they say they stole from the state’s prescription drug database. A notice posted on the DHP Web site acknowledged that the site is currently experiencing technical difficulties which affect computer and e-mail systems. Some customer identification numbers, which may be Social Security numbers, were included, but medical histories were not.

**UPDATE (6/4/09):** The state is mailing individual notifications to 530,000 people whose prescription records may have contained Social Security numbers. In addition, 1,400 registered users of the database, mostly doctors and pharmacists, who may have provided Social Security numbers when they registered for the program, are being notified. The database that was hacked contained records of more than 35 million prescriptions dispensed since 2006 for certain federally controlled drugs with a high potential for abuse.

**Information Source:**
Media

**May 1, 2009**

**LexisNexis, Investigative Professionals**
**Miamisburg, Ohio**

BSO CARD 40,000

Companies Lexis Nexis and Investigative Professionals have notified up to 40,000 individuals whose sensitive and personally identifiable information may have been viewed by individuals who did not have legitimate access. The data breach is linked to a Nigerian scam artist who used the information to incur fraudulent charges on victims’ credit cards. Of the 40,000 individuals whose information was accessed, up to 300 were compromised and used to obtain fraudulent credit cards. The private information viewed included names, dates of birth and possibly Social Security numbers.

**Information Source:**
Dataloss DB

**May 1, 2009**

**Littleton Regional Hospital**
**Littleton, New Hampshire**

MED INSD Unknown

A patient complaint in March of 2009 resulted in the firing of an employee. An audit revealed that the employee inappropriately accessed patient records for unknown reasons at least three times between 2008 and May of 2009. The records contained names, contact information, dates of birth, insurance information and other health information.

**UPDATE (8/10/10):** Another employee was fired for a similar unauthorized access incident during May of 2010.

**Information Source:**
PHIPrivacy.net

**April 29, 2009**

**Orleans Parish Public Schools**
**New Orleans, Louisiana**

EDU PHYS Unknown

The confidential records of Orleans Parish public-school employees have been discovered in an abandoned and unsecured warehouse in New Orleans. Personnel files, payroll records, and other documents with private data were uncovered. Inside were countless boxes filled with confidential information, not to mention stacks of other documents lying on the ground, listing payroll information, worker evaluations, notices of personnel action, and investigations into employee discrimination. Also found were full names, home addresses, and Social Security numbers on document after document.

**Information Source:**
Media

**April 29, 2009**

**Oklahoma Housing Finance Agency**
**Oklahoma City, Oklahoma**

GOV PORT 225,000

A laptop computer containing the personal information of about 225,000 Oklahomans was stolen from a city home last week. The names, Social Security numbers, tax identification numbers, birth dates and addresses of clients of the Section 8 Housing Voucher Program were on an employee’s laptop that was stolen.

**Information Source:**
Dataloss DB

**April 29, 2009**

**Illinois Department on Aging**
**Springfield, Illinois**

GOV DISC 170

A spreadsheet with worker names and Social Security numbers was found on the Internet. The data, prepared for an
outside auditing firm, was released to a so-called peer-to-peer network during a music transfer to an agency laptop. 160 employees and another 10 or so former staffers were alerted to the breach.

Information Source: Dataloss DB

April 28, 2009  West Virginia State Bar
Charleston, West Virginia

The West Virginia State Bar has hired forensic computer experts in hopes of finding those responsible for hacking into the group's website and internal computer network. Information about the State Bar's current and former members may have been compromised. The hacker was able to access the group's internal database server where there was information concerning lawyer identification numbers, names, mailing addresses, email addresses and some Social Security numbers.

Information Source: Dataloss DB

April 27, 2009  Federal Reserve Bank of New York
New York, New York

A former employee at the Federal Reserve Bank of New York and his brother were arrested on suspicion of obtaining loans using stolen identities. The former employee previously worked as an IT analyst at the bank and had access to sensitive employee information, including names, birthdates, Social Security numbers and photographs. A thumb drive attached to his computer had applications for $73,000 in student loans using two stolen identities. They also found a fake drivers license with the photo of a bank employee who wasn't the person identified in the license.

Information Source: Media

April 23, 2009  Oklahoma Department of Human Services
Oklahoma City, Oklahoma

(866) 287-0371

Some personal information may have been contained on a laptop computer stolen from an agency employee. Information on the stolen computer included names, Social Security numbers and dates of birth for people who receive DHS services.

Information Source: Dataloss DB

April 22, 2009  Marian Medical Center
Santa Maria, California

Recent patients of the emergency room and Urgent Care Center have been alerted that a Blackberry containing patient information was stolen from the hospital. The Blackberry contained an email message that included patient information, such as Social Security numbers, dates of birth and medical histories.

Information Source: Dataloss DB

April 22, 2009  New York State Tax Department
New York, New York

A former New York state tax department worker was accused of stealing the identities of thousands of taxpayers and running up more than $200,000 in fraudulent charges. The former employee gathered credit card, brokerage account and Social Security numbers that he used to open more than 90 credit card accounts and lines of credit between 2006 and 2008. Investigators searched the employee's home, they found more than 700 state tax forms containing identifying taxpayer information. They also found more than 300 birth certificates, more than 1,000 Social Security cards, credit card statements and applications, and some 2,000 notes with Social Security numbers, many accompanied by handwritten notes such as good prospect, had money and go with this one.

Information Source: Media

April 20, 2009  FairPoint Communications Inc.
Charlotte, North Carolina

A worker's failure to abide by security precautions caused a portable data-storage device containing employee information to disappear. The device contained information for all current FairPoint employees and some former employees, or about 4,400 individuals in total. Such data may have included names, home addresses and phone numbers, Social Security numbers, birth dates and certain compensation and employment information.

Information Source: Dataloss DB

April 16, 2009  MySpace

MySpace
Confidential employee information, including at least name, Social Security numbers and compensation, was taken by an employee in the company's benefit's department without authorization, beginning in June 2008 or earlier. The information was used to annoy selected individuals and the now former employee was arrested and is being prosecuted by the High Tech Crimes Division of the Los Angeles County District Attorneys Office.

An employee was caught accessing the Social Security numbers, names, compensation information and other personal information of employees. The former employee misused the information within the organization; but it is not known if they gave it to outside parties.

Identity thieves using the names and Social Security numbers of Irving Independent School District employees have made thousands of dollars in credit card purchases. At least 64 of the 3,400 teachers and other employees names were on an old benefits report that somehow ended up in the trash.

UPDATE (2/4/10): At least one woman involved in the crime was caught in January of 2009 and sentenced on February 4, 2010.

Moses Cone Hospital is offering free credit monitoring to 14,380 patients after a laptop computer containing confidential information was stolen from a VHA employee's car. The information on the laptop, including patients' Social Security numbers.

The office of CBIZ Medical was broken into on Feb. 23. Among the items stolen was a computer belonging to the hospital with stored radiology reports related to some patients. Patients between December 2007 and Feb. 23, 2009, may have had records saved on the stolen computer.

As many as 100,000 patients of Peninsula Orthopaedic Associates are being warned to protect themselves against identity theft after tapes containing patient information were stolen. Patients also were advised to keep an eye on benefits statements from their health insurance companies since they may also be at risk for medical identity theft. The records from Peninsula Orthopaedic were stolen March 25 while in transport to an off-site storage facility. Patients' personal information including their Social Security numbers, employers and health insurance plan numbers may have been among the information stolen.

The theft of seven laptop computers from an auditing firm has led the Borrego Springs Bank to send warning letters to all of its customers saying their personal financial information may be in the hands of criminals. The bank would not comment on the name of the accounting firm that was auditing the records or how or where the thefts occurred. The computer files contain sensitive personal financial information including account name, number and balance.
On March 23, the University confirmed that 10,868 Social Security numbers in historical data on a computer at Penn State Erie, The Behrend College, could have been breached. Longstanding security measures, designed to protect the network and systems from malicious software, alerted the University to the potential breach. As soon as the University became aware of the malicious software on this computer, the computer was immediately taken off line, data was examined and information was removed.

Metro Nashville students' names, Social Security numbers, addresses and dates of birth and parents' demographic information were available by searching Google. A private contractor unintentionally put student data on a computer Web server that wasn't secure. The data was available online from Dec. 28 to March 31.

Holders of Hawai‘i commercial driver’s licenses are being warned to take measures to prevent identity theft after a state computer containing personal information was stolen three weeks ago. The laptop computer contained the names, addresses, Social Security numbers and other personal information of 1,892 commercial vehicle license drivers.

Personal information for 7,845 town taxpayers was exposed on the Internet due to a vendor's mistake. The unidentified vendor had the records to reformat the town's personal property tax file for billing purposes. The files containing the names, addresses and Social Security numbers of residents were on a password-protected site that was compromised.

A former child support worker was arrested after attempting to sell the personal information - including names, Social Security numbers and bank account numbers - of 1,600 people. He sold a total of 35 names, dates of birth and Social Security numbers between October 2008 and last month, all to an undercover operative of the Tennessee Bureau of Investigation. He claimed to the operative that he had similar information that he was willing to sell for an additional 1,500 people, and was arrested while meeting with the operative to deliver the information.

A laptop computer recently stolen at the Palo Alto Medical Foundation's Santa Cruz office contained personal and medical information of 1,000 Santa Cruz County patients.

The names, Social Security numbers and other personal information of about 8,000 state employees could be compromised. The potential problem came to light when a torn and empty envelope from the company that manages the state's health savings account program arrived by U.S. mail. The envelope was missing an invoice that contains confidential information.
Symantec is warning a small number of customers that their credit card numbers may have been stolen from an Indian call center used by the security vendor. Symantec sent out warning letters, after the BBC reported that it managed to purchase credit card numbers obtained from Symantec’s call center from a Delhi-based man. The letters were sent to just over 200 customers. Most of those notified are in the U.S., but the company also notified a handful of customers in the U.K. and Canada.

A University-owned laptop was stolen from a staff member's residence. The stolen laptop was password protected and there is no factual evidence that any private information was stored on the laptop. The computer contained names and some personal information. It does not appear that any Social Security numbers were stored on the system.

Massachusetts General Hospital has put dozens of patients on notice that it has lost some of their confidential medical records, which were left on an MBTA Red Line train by a hospital employee. The MGH employee left the hospital, taking the records with her to do billing work on them over the weekend. The records belonged to at least 66 patients and included private information such as the patients’ diagnoses, their names, birth dates and billing information.

A filing error in Maryland's federal court resulted in health insurance information for 226 people - including 42 Social Security numbers - being made available to the public for more than two weeks. The private information of Washington area residents was included in requests for warrants to search the doctors' offices in Suitland, La Plata, Oxon Hill and Falls Church as part of a health care fraud investigation. The warrants were marked as being sealed and, therefore, were not supposed to be made public.

A Nashville mother who was walking along found confidential paperwork that lists Metro school students' names, Social Security numbers and disabilities. The Metro Schools spokeswoman said they will trace the documents and try to figure out how they got where they weren't supposed to be.

More than 900 current and former COTA employees recently learned their Social Security numbers had been sent to dozens of health-insurance companies. Central Ohio Transit Authority officials notified administrative employees who have or had worked for COTA since 2004 that personnel workers gave 51 companies their names and identification numbers. The information went to companies proposing to bid on providing long-term disability insurance to COTA. In 2006, COTA also sent information on union employees to 39 potential insurance providers.
University of West Georgia officials have notified nearly 1,300 students and faculty members that their personal information was on a laptop stolen from a professor traveling in Italy. The laptop was taken last summer, but university officials say they only recently learned that the computer contained sensitive information, including names, addresses, phone numbers and Social Security numbers.

Walgreens Health Initiative
Deerfield, Illinois

Names, dates of birth and Social Security numbers of roughly 28,000 state retirees were e-mailed to the Kentucky Retirement Systems without being properly encrypted for security purposes by its pharmacy benefit provider. The e-mail contained dates of birth, Social Security numbers and health insurance claim numbers but not personal health information. The file contained information only on members who were both Medicare-eligible and used the retiree pharmacy benefit through Walgreens in 2007.

New York City Housing Authority
New York, New York

Dozens of confidential files with city public housing residents’ birth dates, Social Security numbers, and eviction notices were dumped on an East New York street. City Housing Authority officials are investigating to determine how the files ended up scattered along Atlantic Ave. near Pennsylvania Ave.

Penn State Office of Physical Plant
University Park, Pennsylvania

The Social Security numbers of employees working for the Penn State Office of Physical Plant in 2000 may have been stolen. A virus infiltrated an administrative computer that contained more than 1,000 Social Security numbers of OPP employees.

University of Toledo
Toledo, Ohio

A computer stolen from the University of Toledo contained personal information for about 24,000 students and 450 faculty during the 2007-08 and 2008-09 academic years. The student data was directory and educational information, such as student identification numbers and grade point averages. The faculty information, however, was more personal and included names, Social Security numbers, birth dates, and more.

Comcast
Philadelphia, Pennsylvania

A list of over 8,000 Comcast user names and passwords were available to the public via Scribd for two months, before a Wilkes University professor discovered it over the weekend after doing a search for his identity online. Comcast is saying it looks like the result of a phishing scam and isn’t an inside job, and that there are so many duplicate entries on the list that it’s closer to 4,000 customers who were exposed.
An Army database that contains personal information about nearly 1,600 soldiers may have been penetrated by unauthorized users. The information that may have been breached includes the service members’ names, e-mail messages, phone numbers, home addresses, awards received, ranks, gender, ethnicity, and dates the soldiers deployed and returned from their deployment.

**Information Source:**
Media

**March 12, 2009**
**Dezonia Group**
Chicago, Illinois

The city of Chicago bills people for ambulance rides — $600 and up. It uses a third party, Dezonia Group, for billing. An employee's laptop, containing patient names, addresses and Social Security numbers, was stolen from the company. Reports differ as to whether or not the data was encrypted.

**Information Source:**
Dataloss DB

**March 11, 2009**
**Binghamton University**
Binghamton, New York

Binghamton University kept payment information for every student, possibly dating back at least ten years in a storage area next to one of the most trafficked lecture halls on campus, behind a door that was not only unlocked but taped open. The information itself contained Social Security numbers, credit card numbers, scans of tax forms, business information (including Social Security numbers and salary information for employees of students’ parents), asylum records and more, all kept in a haphazard and disorganized fashion, sprawled out in boxes, in unlocked (yet lockable) filing cabinets and shelving units. If the information inside the room pertained only to the current students enrolled and their parents that would mean the story would effect, roughly, forty-two thousand people. However, because the information goes back at least ten years, if not more, the potential number of people effect lies well in the hundred thousands.

**Information Source:**
Media

**March 11, 2009**
**Sprint**
Overland Park, Kansas

Sprint is warning several thousand customers that a former employee sold or otherwise provided their account data without permission. It appears this employee may have provided customer information to a third party in violation of Sprint policy and state law. They have terminated this employee. The information that may have been compromised includes name, address, wireless phone number, Sprint account number, security question answer, and the name of the authorized point of contact for account.

**Information Source:**
Dataloss DB

**March 7, 2009**
**Idaho National Laboratory**
Idaho Falls, Idaho

Idaho’s Congressional Delegation this week announced a potential identity theft threat involving information from 59,000 present and former workers at the Idaho National Laboratory at Idaho Falls. DOE notified delegation members that an encoded disc containing personal data from the employees was either lost or stolen in transit via United Parcel Service. The package, originally shipped from New York to Maryland, was found damaged.

**Information Source:**
Dataloss DB
Google contacted some of its users to let them know about a situation that affected its Google Docs users. They believe the problem affected less than 0.05% of all documents. Google identified and fixed a bug where a small percentage of users shared some of their documents inadvertently. The bug occurred when the document owner, or a collaborator with sharing rights, selected multiple documents and presentations from the documents list and then changed the sharing permissions. The bug did not affect spreadsheets.

Information Source: Media

March 7, 2009 Oklahoma Department of Human Services Shawnee, Oklahoma GOV PHYS Unknown

The state Department of Human Services is investigating how a child welfare worker’s records ended up with a local TV station. The files, which included names, Social Security numbers, contact information and details on child abuse investigations, reportedly were left behind when a DHS worker was evicted from a rent house in Guthrie.

Information Source: Dataloss DB

March 6, 2009 Federal Emergency Management Agency Region 5 Office Griffith, Indiana GOV PORT 50

A laptop containing Social Security numbers and other personal information from dozens of victims of last September’s floods was reported stolen from a housing inspector’s car. Representatives from the Federal Emergency Management Agency alerted roughly 50 flood victims from Gary, Hammond, Highland, Griffith and Munster whose information was stored in the laptop after they applied for federal disaster assistance. The password-protected laptop was stolen from a housing inspector’s car in Griffith on Nov. 4, containing names, Social Security numbers, dates of birth, addresses and phone numbers of people who applied for assistance.

Information Source: Dataloss DB

March 5, 2009 St. Rita’s Medical Center Lima, Ohio MED PHYS 242

A home-health employee for St. Rita’s Medical Center had a bag stolen during an automobile break-in. The bag contained information on some patients, including names, dated of birth, addresses, phone numbers, patient identification numbers, and the names of case managers and physicians. In some cases it also included Social Security numbers and the type of treatment being provided, according to a letter given to the patients involved.

Information Source: Dataloss DB

March 4, 2009 Elk Grove Unified School District Elk Grove, California EDU PHYS 520

A document with the Social Security numbers of more than 500 Elk Grove Unified School District employees was lost by a district employee.

Information Source: Dataloss DB

March 4, 2009 New York Police Department New York, New York GOV INSD 80,000

A civilian employee of the department’s pension fund is accused of stealing eight tapes containing the Social Security numbers and direct-deposit information for 80,000 current and retired cops. The employee, who served as the pension fund’s director of communications, has been charged with computer trespass, burglary and grand larceny. He is accused of removing the tapes from a backup data warehouse on Staten Island after disabling security cameras. Police found the missing tapes at his home before arresting him.

Information Source: Dataloss DB

March 3, 2009 Western Oklahoma State College Altus, Oklahoma EDU DISC 1,500

A computer breach at Western Oklahoma State College may have exposed Social Security numbers and other identifying information for 1,500 campus library users. An unauthorized program known as a rootkit was installed on a server.

http://googledocs.blogspot.com/2009/03/on-yesterdays-email.html
An unauthorized program known as a rootkit was installed on a server administered by an outside party. There is no indication that any of the data on the machine was actually compromised - only that the opportunity for someone to access it existed.

**Information Source:** Dataloss DB

**March 1, 2009**

**City of Muskogee**

**Muskogee, Oklahoma**

GOV PORT 4,500

The city of Muskogee recently discovered that a computer zip disk containing personal information has been in public circulation since 2000. The disk in some cases contained phone numbers and in other cases contained Social Security numbers. It’s believed that a forgetful employee scooped up the disk while putting together surplus items no longer used by the city.

**Information Source:** Dataloss DB

**February 26, 2009**

**Steamboat Springs School District**

**Steamboat Springs, Colorado**

EDU PORT 1,300

Social Security numbers for 1,300 past and present employees was compromised when a laptop was stolen from the Steamboat Springs School District office. The laptop had a spreadsheet containing the Social Security numbers and names of their owners. The spreadsheet was created as part of a requirement from a past district audit. The laptop was password-protected, but district officials are warning their employees to be on the lookout for any potential identity theft.

**Information Source:** Dataloss DB

**February 23, 2009**

**University of Florida**

**Gainesville, Florida**

EDU DISC 101

An undated statement on the University’s Web site indicates that on January 20, an LDAP Directory Server configuration error allowed outside access to a directory containing Social Security numbers and other personal data. Personal data belonging to about 101 people might have been compromised as a result.

**Information Source:** Dataloss DB

**February 23, 2009**

**Seaview Financial**

**Corona Del Mar, California**

BSF PHYS Unknown

Folders with personal information for numerous clients of a local mortgage broker sat for days at a public recycling site. The files contained bank account statements, completed tax forms, credit reports and Social Security numbers.

**Information Source:** Dataloss DB

**February 20, 2009**

**Del Mar College**

**Del Mar, California**

EDU PHYS 53

A class roster containing the names and Social Security numbers of some 53 Del Mar College students has been stolen. The roster was taken out of a professor’s vehicle parked at Cole Park. The G.E.D. teacher was taking work home Sunday, when he stopped at Cole Park and his car was broken into.

**Information Source:** Dataloss DB

**February 20, 2009**

**Arkansas Department of Information Systems, Information Vaulting Services**

**Little Rock, Arkansas**

GOV PORT 807,000

(888) 682-0411 <a href="http://notify.arkansas.gov">http://notify.arkansas.gov</a>

A computer storage tape with data from criminal background checks dating back to the mid-1990s is missing from an information-protection company’s vault. The background-check information includes names, dates of birth, Social Security numbers and addresses.

**Information Source:** Dataloss DB

**February 19, 2009**

**University of Florida**

**Gainesville, Florida**

EDU HACK 97,200

(877) 657-9133
A foreign hacker gained access to a University of Florida computer system containing the personal information of students, faculty and staff. The files included the names and Social Security numbers of individuals who used UF's Grove computer system since 1996.

Information Source: Dataloss DB  
February 19, 2009  
Northeast Orthopaedics, MRecord  
Raleigh, North Carolina  
MED DISC  1,000

Records of more than 1,000 patient visits to Northeast Orthopaedics, a large Albany surgical practice, have been posted on the Internet. The records appeared on the Web site visvabpo.com, which seems to be a defunct outsourcing company in India called Visva BPO. Those records include patient names, birth dates and Social Security numbers.

Information Source: Dataloss DB  
February 18, 2009  
CVS Pharmacies  
Woonsocket, Rhode Island  
MED PHYS Unknown

http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cvsresolutionagreement.html

The CVS Pharmacy chain, the largest in the country with 6,300 outlets, has agreed to a $2.25 million settlement with the U.S. Dept. of Health and Human Services. Indianapolis TV station WTHR engaged in an extensive investigation beginning in 2006 of local CVS Pharmacies and their pharmacies in other cities nationwide including Boston, Chicago, Cleveland, Detroit, Dallas, Louisville, Miami, New Haven (Conn.), Philadelphia, Phoenix, and CVS headquarters in Woonsocket, RI. They found that CVS pharmacies were disposing of documents, such as labels from prescription bottles and old prescriptions, in unsecured dumpsters. The HHS's Office of Civil Rights charged that CVS failed to implement adequate policies and procedures to reasonably and appropriately safeguard protected health information during the disposal process failed to adequately train employees on how to dispose of such information properly and did not maintain and implement a sanctions policy for members of its workforce who failed to comply with its disposal policies and procedures. In a coordinated action, CVS Caremark Corporation, the parent company of the chain, also signed a consent order with the Federal Trade Commission to settle potential violations of the FTC Act.

UPDATE (7/16/09): A state board has given final approval to settlements with Indiana’s two largest drugstore chains for leaving patient information in the trash. CVS has paid a $2.25 million fine to settle a probe by the U.S. Office of Civil Rights. Also CVS will donate $1,000 to charity as part of the state settlement.

Information Source: Dataloss DB  
February 18, 2009  
Rio Grande Food Project  
Albuquerque, New Mexico  
NGO PORT  36,000

A food pantry is warning its clients that tens of thousands of them are at risk for identity theft after a laptop computer containing their personal information was stolen. The computer contained sensitive personal data including addresses, birth dates and Social Security numbers.

Information Source: Dataloss DB  
February 17, 2009  
Broome Community College  
Binghamton, New York  
EDU DISC  14,000

Broome Community College, sent out a mailing last week with Social Security number posted prominently on the back cover. The winter/spring 2009 alumni magazine was mailed to 28,000 people, it assumed that less than 14,000 copies had Social Security numbers on the magazine.

Information Source: Dataloss DB  
February 16, 2009  
Wyndham Hotels & Resorts  
Parsippany, New Jersey  
BSO HACK  21,000


In mid-September 2008, the company discovered that a sophisticated hacker penetrated the computer systems of one of the hotels. By going through the centralized network connection, the hacker was then able to access and download information from several, but not all, of the other WHR properties and create a unique file containing payment card information of a small percentage of WHR customers. Potentially exposed through this breach are guest and/or cardholder names and card numbers, expiration dates and other data from the card’s magnetic stripe.

Information Source: Dataloss DB  
February 13, 2009  
University of Alabama  
Tuscaloosa, Alabama  
EDU HACK  37,000

589
Seventeen of 400 databases were tapped by hackers. Personal information may have been stolen. One of those computers contained lab results for people tested at the campus medical center. The servers had a database containing 37,000 records of lab data. They contain the names, addresses, birthdates and Social Security numbers of each person who has had lab work, such as a blood or urine test, done on the UA campus since 1994.

**Information**
**Source:** Dataloss DB
**February 11, 2009**
**Los Alamos National Laboratory**
**Los Alamos, New Mexico**
GOV STAT Unknown

The Los Alamos nuclear weapons laboratory in New Mexico is missing 69 computers, including at least a dozen that were stolen last year. The computers are a cybersecurity issue because they may contain personal information like names and addresses. But Los Alamos claims they did not contain classified information. Also missing are three computers that were taken from a scientist’s home and a BlackBerry belonging to another employee that was lost in a foreign country considered sensitive.

**Information**
**Source:** Dataloss DB
**February 10, 2009**
**SemGroup LP**
**Tulsa, Oklahoma**
BSO DISC 160

Online banking bandits pulled thousands of dollars from the accounts of current and former employees after personal information was inadvertently left on a bankruptcy court document made public.

**Information**
**Source:** Dataloss DB
**February 9, 2009**
**Parkland Memorial Hospital**
**Dallas, Texas**
MED PORT 9,300

A laptop computer that may have contained the names, birthdates and Social Security numbers of 9,300 employees of Parkland Memorial Hospital was stolen.

**Information**
**Source:** Dataloss DB
**February 9, 2009**
**Federal Aviation Administration**
**Washington, District Of Columbia**
GOV HACK 43,000 Total increased to 48,000

Hackers broke into the Federal Aviation Administration’s computer system, accessing the names and Social Security numbers of employees and retirees.

**Information**
**Source:** Dataloss DB
**February 9, 2009**
**U.S. Postal Service Santee**
**Santee, California**
GOV INSD Unknown

A mail carrier in San Diego County is accused of stealing dozens of gift cards, debit cards and Social Security documents sent through the mail. Deputies found 30 gift cards, stolen mail, debit cards and money when the carrier was arrested after he finished his route. Detectives also found Social Security documents and W-2 wage and tax statements at carrier’s home.

**Information**
**Source:** Dataloss DB
**February 8, 2009**
**Kaspersky**
**Woburn, Massachusetts**
BSO HACK Unknown

An unidentified hacker gained access to databases used by the usa.kaspersky.com Web site, allowing access to users’ accounts, activation codes and possibly personal data about Kaspersky customers. Kaspersky Lab is a security software company.

**Information**
**Source:** Media
**February 6, 2009**
**Catskill Regional Medical Center**
**Harris, New York**
MED INSD 431

A woman was fired for allegedly spying. The employee had access to company files. The files included Social Security numbers, birth dates, addresses and financial information.
<table>
<thead>
<tr>
<th>Date</th>
<th>Source</th>
<th>Company</th>
<th>Location</th>
<th>Industry</th>
<th>Type</th>
<th>Total</th>
<th>Record Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>February 6, 2009</td>
<td><strong>Kaiser Permanente</strong></td>
<td><strong>Oakland, California</strong></td>
<td>MED INSD</td>
<td>29,500</td>
<td></td>
<td></td>
<td>Dataloss DB</td>
</tr>
<tr>
<td>(877) 281-3573</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A law enforcement agency seized a computer file with Kaiser data from a person who was subsequently arrested. The suspect was not a Kaiser employee. Kaiser Permanente is notifying nearly 30,000 Northern California employees that the security breach may have led to the release of their personal information. The stolen information included names, addresses, dates of birth and Social Security numbers for Kaiser employees. <strong>UPDATE</strong> (9/28/2011): A former benefits clerk from Service Employees International Union-affiliated United Healthcare Workers West (SEIU-UHW) was sentenced to 12 years and four months in prison for stealing Kaiser union employee information.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>February 6, 2009</td>
<td><strong>Purdue University</strong></td>
<td><strong>West Lafayette, Indiana</strong></td>
<td>EDU DISC</td>
<td>962</td>
<td></td>
<td></td>
<td>Dataloss DB</td>
</tr>
<tr>
<td><a href="http://news.uns.purdue.edu/Payroll0901.html">http://news.uns.purdue.edu/Payroll0901.html</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A mailing error has resulted in 1099 tax forms being sent to the wrong recipients. The incident affected 248 companies and 962 individuals. Those affected by the incident received letters notifying them that their tax information had either been sent to another or that they themselves had received someone else’s information by mistake.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>February 5, 2009</td>
<td><strong>Mooresville's Dry Cleaning Station</strong></td>
<td><strong>Mooresville, North Carolina</strong></td>
<td>BSO INSD</td>
<td>Unknown</td>
<td></td>
<td></td>
<td>Dataloss DB</td>
</tr>
<tr>
<td>A Mooresville dry cleaner skipped town, taking her clients’ clothes and credit card numbers with her.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>February 5, 2009</td>
<td><strong>phpBB.com</strong></td>
<td><strong>Bellevue, Washington</strong></td>
<td>BSO HACK</td>
<td>400,000</td>
<td>Not added to total; SSNs were not accessed.</td>
<td>Dataloss DB</td>
<td></td>
</tr>
<tr>
<td>A popular bulletin board software package has been taken offline following a security breach that gave an attacker full access to a database containing names, email, address, and hashed passwords for its entire user base. The attacker gained access through an unpatched security bug in PHPList, a third-party email application.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>February 4, 2009</td>
<td><strong>Womancare Inc.</strong></td>
<td><strong>Lathrup Village, Michigan</strong></td>
<td>MED PHYS</td>
<td>unknown</td>
<td></td>
<td></td>
<td>Dataloss DB</td>
</tr>
<tr>
<td>Medical records were improperly disposed of. Pro-Life Society found the records in a dumpster behind the office.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>February 4, 2009</td>
<td><strong>Texas Veterans Commission</strong></td>
<td><strong>Waco, Texas</strong></td>
<td>GOV DISC</td>
<td>20</td>
<td></td>
<td></td>
<td>Dataloss DB</td>
</tr>
<tr>
<td>A Waco individual received a packet in the mail with the application for her daughter's tuition benefits. At the bottom of the packet, was a claims log that listed more than 20 veterans names, Social Security numbers and medical claim information. The Waco Veterans Commission and the VA’s regional office were not able to explain how the veterans’ personal information found its way into the envelope containing the unrelated information about the tuition benefits for the woman’s daughter.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>February 3, 2009</td>
<td><strong>Baystate Medical Center</strong></td>
<td><strong>Springfield, Massachusetts</strong></td>
<td>MED PORT</td>
<td>Unknown</td>
<td></td>
<td></td>
<td>Dataloss DB</td>
</tr>
<tr>
<td>A popular bulletin board software package has been taken offline following a security breach that gave an attacker full access to a database containing names, email, address, and hashed passwords for its entire user base. The attacker gained access through an unpatched security bug in PHPList, a third-party email application.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Several laptops were stolen from Baystate Medical Center's Pediatrics department. Some of those computers had patient information on them. All of the information is password protected and the computers had no financial or Social Security information on them.

**Information Source:**
Dataloss DB  
**Records from this breach used in our total:** 0

**February 3, 2009**  
**SRA International**  
Fairfax, Virginia

Malicious software may have allowed hackers to get access to data maintained by SRA, including employee names, addresses, Social Security numbers, dates of birth and healthcare provider information.

**Information Source:**
Dataloss DB  
**Records from this breach used in our total:** 0

**February 3, 2009**  
**Georgia State Board of Pardons and Paroles**  
Atlanta, Georgia

The offices of a state contractor in Roswell were burglarized and a computer was stolen. Information regarding current and past parolees that was lost in a burglary includes names, dates of birth and Social Security numbers.

**Information Source:**
Dataloss DB  
**Records from this breach used in our total:** 0

**February 2, 2009**  
**Southern Satellite**  
Orange City, Florida

Hundreds of folders containing names, addresses, Social Security numbers and credit card information were found in a dumpster.

**Information Source:**
Dataloss DB  
**Records from this breach used in our total:** 0

**February 2, 2009**  
**St. Anthony Central Hospital**  
Denver, Colorado

Boxes, filing cabinets and trash bags full of hundreds of U.S. passports, birth certificates, driver's licenses, Social Security cards and other documents - most stolen within the past two years were found in a storage unit. A hospital employee admitted to stealing the records. Also found were hospital records containing dates of birth, Social Security numbers and copies of the driver's licenses of 150 patients who had been admitted into the emergency room or general surgery.

**Information Source:**
Dataloss DB  
**Records from this breach used in our total:** 150

**January 31, 2009**  
**Columbia University**  
New York, New York

About 1,400 current, former and prospective students at Columbia University have been told that their personal information, including Social Security numbers, is vulnerable following a security breach. The university said information about the students, as well as some current and past employees, was on three password-protected notebook computers that were stolen from a Columbia College.

**Information Source:**
Dataloss DB  
**Records from this breach used in our total:** 1,400

**January 31, 2009**  
**HoneyBaked Ham**  
Indianapolis, Indiana

A computer server stocked with credit-card information was stolen from a store. Customers might be at risk.

**Information Source:**
Dataloss DB  
**Records from this breach used in our total:** 0

**January 31, 2009**  
**Ball State University**  
Muncie, Indiana

A employee sent out an e-mail, to verify contact information, to 91 special events staff with an excel spreadsheet attachment that, unbeknownst to the employee, included the Social Security number of 19 of the workers.

**Information Source:**
Dataloss DB  
**Records from this breach used in our total:** 19
January 30, 2009  Kansas State University  Manhattan, Kansas  

(785) 532 4441

Students who were enrolled in an agricultural economics class in spring 2001 inadvertently had some personal information exposed on the Internet through a K-State departmental Web site. Names, Social Security numbers and grades of those students have been exposed since 2001.

**Information Source:**
Dataloss DB

January 30, 2009  Coos Bay Department of Human Services  Coquille, Oregon

A scammer made off with Social Security numbers after sending a virus online to a computer at the Department of Human Services office. An application that was installed recorded keystrokes and sent them to an external address. The information was taken from Coos County residents.

**Information Source:**
Media

January 30, 2009  Indiana Department of Administration  Indianapolis, Indiana

Social Security numbers of current and former state employees were accidentally posted on a state Web site for about two hours. The Social Security numbers were erroneously included in a contract solicitation file posted on the department’s procurement Web site.

**Information Source:**
Dataloss DB

January 28, 2009  CityStage  Springfield, Massachusetts

A computer system might have exposed credit card information of customers on the Internet. The probably occurred in December while the theater’s Web contractor was changing servers. Credit card numbers might have been compromised.

**Information Source:**
Dataloss DB

January 27, 2009  U.S. Consulate

Hundreds of files - with Social Security numbers, bank account numbers and other sensitive U.S. government information - were found in a filing cabinet purchased from the U.S. consulate in Jerusalem through a local auction.

**Information Source:**
Media

January 27, 2009  Beaumont City  Beaumont, Texas

Personal information of current and former Beaumont city workers was accidentally posted online. The information, including birth dates and Social Security numbers.

**Information Source:**
Dataloss DB

January 27, 2009  Citi Habitats  New York, New York

During a refurbishing of their office, paper that should have been shredded was improperly placed as trash. Information found blowing in the street included bank statements, 401k statements, credit reports, tax returns, driver’s licenses, names, phone numbers and Social Security numbers.

**Information Source:**
Dataloss DB

January 26, 2009  Madison, WI. Human Resources Department  Madison, Wisconsin

An oversight by the city of Madison’s personnel office is the reason Social Security numbers of city employees were stored on a laptop computer stolen from a city office. Any official or employee - except those in the police, fire and transit departments - who was issued a new or replacement city identification card from the start of 2004 through 2007 may be at risk. Data on the laptop included photos, names and Social Security numbers.
A New Zealand man accesses U.S. military secrets on an MP3 player he bought from an Oklahoma thrift shop for $18. When the 29-year-old hooked up the player he discovered a playlist he could never have imagined - 60 files in total, including the names and personal details of American soldiers.

The database was illegally accessed and user IDs, passwords, names, e-mail addresses, birth dates, gender, ethnicity, and in some cases, users' states of residence were stolen.

These mortgage brokers have discarding consumers' tax returns, credit reports, and other sensitive personal and financial information in an unsecured dumpster in December of 2006. Approximately 40 boxes containing consumer records were found in a publicly-accessible dumpster. The records included tax returns, mortgage applications, bank statements, photocopies of credit cards, drivers' licenses, and at least 230 credit reports. The defendant, who has owned numerous companies that handle sensitive consumer information, kept the documents in an insecure manner in his garage before improperly disposing of them.

UPDATE (1/20/10): The mortgage broker paid a $35,000 civil penalty to settle FTC charges. The mortgage broker will also have to hire an independent security professional to review the security process every year for 10 years.

Personal information, including Social Security numbers for 565 foreign students at MSU was leaked this month when a university office sent an e-mail message soliciting their help with language tutoring. The email message they got had a spreadsheet attachment that contained names and Social Security numbers for international students.

People who received flu shots from the agency since October are being warned that their personal information may have been stolen by a former department temporary worker. Information included their names, Social Security numbers, addresses and other personal information.

After being alerted by Visa and MasterCard of suspicious activity surrounding processed card transactions, the company last week found evidence of malicious software that compromised card data that crossed Heartland's network. This incident may be the result of a global cyberfraud operation.

UPDATE (01/26/2009): Heartland Payment Systems has been sued. The lawsuit seeks damages and relief for the
inexplicable delay, questionable timing, and inaccuracies concerning the disclosures with regard to the data breach, which is believed to be the largest in U.S. history.

UPDATE (02/12/2009): According to BankInfoSecurity.com, the number of financial institutions that have come forward to say they have been contacted by their credit card companies Visa and MasterCard in relation to the breach has jumped from fewer than 50 to more than 200.

UPDATE (06/04/2009): While it’s hard to get a handle on just how many consumers were affected by the Heartland Payment Systems (HPY) data breach, the total number of institutions now reporting card compromises is at 656.

UPDATE (06/16/2009): Heartland lawsuits to be heard in Texas. The Judicial Panel on Multidistrict Litigation in Louisville, KY issued its decision to consolidate the class action suits. The lawsuits will be heard in the Southern District Court of Texas in Houston. Thirty-one separate lawsuits, on behalf of consumers, investors, banks and credit unions, have been filed against Princeton,N.J.-based Heartland.

UPDATE (07/06/2009): Heartland Payment Systems successfully completed the first phase of an end-to-end encryption pilot project designed to enhance its security.

UPDATE (08/20/2009): Albert Segvec Gonzalez has been indicted by a federal grand jury in New Jersey - along with two unnamed Russian conspirators - on charges of hacking into Heartland Payment Systems, the New Jersey-based card processing company, as well as Hannaford Brothers, 7-Eleven and two unnamed national retailers, according to the indictment unsealed Monday. Gonzalez, a former Secret Service informant, is already awaiting trial over his involvement in the TJX hack.

Total records breached: 100 million transactions per month. It is unclear how many account numbers have been compromised, and how many are represented by multiple transactions. The number of records breached is an estimate, subject to revision.

UPDATE (08/20/2009): According to the court document, hackers stole more than 130 million credit and debit card numbers from Heartland and Hannaford combined.

UPDATE (05/12/2010): The costs to Heartland Payment Systems Inc. from the massive data breach that it disclosed in January 2009 appear to be steadily adding up. Quarterly financial results released by Heartland last week show that the card payment processor has accrued $139.4 million in breach-related expenses. The figure includes a settlement totaling nearly $60 million with Visa, another of about $3.5 million with American Express and more than $26 million in legal fees. That total also includes $42.8 million that Heartland has set aside to fund proposed settlements with several other litigants over the breach. One example of what the fund is set up for is Heartland’s offer to settle several consumer class action lawsuits against it for four million. So far, Heartland has recovered about $30 million from insurance companies.

UPDATE (06/02/2010): Heartland Payment Systems has made a third settlement deal, this time with MasterCard, related to a massive data breach two years ago at the card payments processor. As part of the deal, Heartland has agreed to pay as much as US$41.1 million to MasterCard issuers that lost money as a result of the data breach. The deal is contingent on financial institutions representing 80 percent of the affected MasterCard accounts accepting the offer by June 25. MasterCard is recommending that issuers accept the offer.

UPDATE (09/01/2010): Heartland Payment Systems has agreed to settle with Discover for five million dollars. Discover will use the money to cover costs of fraud incidents and reissuing cards.

UPDATE (09/19/2010): Jerome Abaquin Gonzales is expected to surrender to police and serve jail time for participating in a credit card forgery ring which used information from the Heartland breach. The information came from the 4.2 million Discover credit card customers who used their cards at Hannaford Brothers.

UPDATE (09/22/2010): Thomas Michio Taniguchi was sentenced to prison for his role in the forgery ring in which Jerome Abaquin Gonzales also participated.

UPDATE (12/07/2011): Heartland legal representatives were able to successfully argue that most of the claims against Heartland that were filed by nine banks should be dismissed. All but one claim was dismissed.

UPDATE (02/12/2012): The nine banks may have had their claims against Heartland dismissed because Heartland reported that sharing a contractual relationship with the banks defeats their appeal. However, the credit-card-issuing banks are arguing that a New Jersey economic loss rule only bars claims for foreseeable economic losses when the parties are in a contractual relationship and does not bar their negligence claim against Heartland.

UPDATE (07/25/2013): Five more foreign hackers were charged for their role in stealing information from Heartland Payment Systems, NASDAQ, Dow Jones, JetBlue, and J.C. Penney.

Information Source: Dataloss DB

<table>
<thead>
<tr>
<th>Date</th>
<th>Company</th>
<th>Location</th>
<th>Source Code</th>
<th>Records Used in Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 16, 2009</td>
<td>Southwestern Oregon Community College</td>
<td>Coos Bay, Oregon</td>
<td>EDU PORT</td>
<td>200</td>
</tr>
<tr>
<td>January 14, 2009</td>
<td>Occidental Petroleum Corporation</td>
<td>Dallas, Texas</td>
<td>BSO INSD</td>
<td>Unknown</td>
</tr>
</tbody>
</table>

A laptop computer was stolen from the campus putting former and current students at risk.

Information Source: Dataloss DB
A former employee emailed himself (to personal email account) a spreadsheet of employee names, addresses, employee identification numbers, birth dates, starting dates, retirement dates and Social Security numbers.

**Information**

**Source:** Dataloss DB

**January 13, 2009**

**University of Oregon**
Eugene, Oregon

(541) 346-2510

A laptop computer containing data files for Youth Transition Program (YTP) participants was stolen. Those files contained names and social security numbers.

**Information**

**Source:** Dataloss DB

**January 13, 2009**

**Innodata Isogen, Inc.**
Hackensack, New Jersey

Laptop stolen from an employee’s car contained names, addresses, Social Security numbers of current and former employees.

**Information**

**Source:** Dataloss DB

**January 13, 2009**

**Seventh-Day Adventist Church**
Silver Spring, Maryland

A laptop stolen and recovered contained names and Social Security numbers.

**Information**

**Source:** Dataloss DB

**January 13, 2009**

**Continental Airlines**
Newark, New Jersey

A laptop containing fingerprints, Social Security numbers, names, addresses, was stolen from a locked Newark office.

**Information**

**Source:** Dataloss DB

**January 13, 2009**

**Blue Ridge Community Action**
Morganton, North Carolina

Social Security numbers were on an external computer hard drive that is missing or stolen. The hard drive contained information on clients from four counties who have used the organization’s services in the past four or five years. The external hard drive was used to back up information on clients.

**Information**

**Source:** Dataloss DB

**January 12, 2009**

**Columbus City Schools**
Columbus, Ohio

Columbus City Schools experienced a security breach, resulting in employees’ Social Security numbers being at risk. CPD officers went to serve drug and auto-theft felony warrants. During the arrest officers learned there might be stolen personal information in the house and found personal information on district employees. It is believed the suspects either stole or intercepted part of a mailing from the payroll division that was en route to annuity companies.

**Information**

**Source:** Dataloss DB

**January 11, 2009**

**University of Rochester**
Rochester, New York

Personal information including Social Security numbers of about 450 current and former University of Rochester students was stolen by hackers this week from a UR database. The information was taken from a non-academic student database and copied illegally to an off-campus IP address.

**Information**

**Source:** Dataloss DB

**January 7, 2009**

**Genica, Geeks.com**
Oceanside, California

596
Genica dba Geeks.com (Genica) recently discovered that customer information, including Visa credit card information, may have been compromised. In particular, it is possible that an unauthorized person may be in possession of your names, addresses, telephone numbers, email addresses, credit card numbers, expiration dates, and card verification numbers. They are still investigating the details of this incident, but it appears that an unauthorized individual may have accessed this information by hacking the eCommerce website.

Information Source: Dataloss DB

January 6, 2009  CheckFree Corp.
Atlanta, Georgia
BSF HACK 5,000,000

CheckFree Corp. and some of the banks that use its electronic bill payment service say that criminals took control of several of the company's Internet domains and redirected customer traffic to a malicious Web site hosted in the Ukraine. The company believes that about 160,000 consumers were exposed to the Ukrainian attack site. However, because the company lost control of its Web domains, it doesn't know exactly who was hit. It has warned a much larger number of customers. This breach was reported back in Dec. 3, 2008.

Information Source: Dataloss DB

January 5, 2009  Library of Congress
Washington, Delaware
GOV INSD 10

An employee in the human resources department of the Library of Congress was charged with conspiring to commit wire fraud in which he stole information on at least 10 employees from library databases. He passed the information to a relative, who used it to open the accounts. Together, the two are alleged to have bought $38,000 worth of goods through the accounts.

Information Source: Dataloss DB

January 2, 2009  Merrill Lynch
New York, New York
BSF STAT Unknown

A third-party consulting services firm working on behalf of Merrill Lynch reported, one of their employees was burglarized. The burglars took various items, including a computer, which had on it the names and Social Security numbers of current and former Financial Advisors and some applicants for employment.

Information Source: Dataloss DB

January 2, 2009  Pepsi Bottling Group
Somers, New York
BSR PORT Unknown

For More Info Contact: David Yawman David.Yawman@pepsi.com (914) 767-7620 or (866) 578-5410

A portable data storage device, which contained personal information, including the names and Social Security numbers of employees in the US is missing or stolen.

Information Source: Dataloss DB

December 31, 2008 New Hampshire’s Lakes Region General Hospital
Laconia, New Hampshire
MED PHYS 1,500

A package containing personnel medical information on patients is missing. UPS recently shipped the parcel from a Woburn, Mass. central processing agent to the hospital, but the package never arrived. Information contained in the package includes patient names, possible Social Security numbers, dates of service and diagnosis code numbers for different diagnosis or medical procedures.

Information Source: Dataloss DB

December 31, 2008 Ohio State University
Columbus, Ohio
EDU DISC 18,000

http://www.studentlife.osu.edu/dataexposure

Ohio State University has notified 18,000 current and former students that their personal information was mistakenly stored on a computer server exposed to the Internet. The data included student names, Social Security numbers, addresses and coverage dates for those enrolled in the health insurance plan for three quarters in 2005-06.
RBS WorldPay belatedly admitted that hackers broke into their systems. In the US up to 1.1 million Social Security numbers were exposed as a result of the breach. Pre-paid cards including payroll cards and open-loop gift cards were affected. RBS stated that PINs for all PIN-enabled cards have been reset.

**UPDATE** (2/3/09): Hackers orchestrated a highly coordinated, global attack on ATM cards involving the theft of a staggering $9 million from ATMs in 49 cities worldwide. Alleged hackers are still at large and could orchestrate another attack.

**UPDATE** (2/10/09): "Certain personal information" of 1.5 million card holders and Social Security numbers of 1.1 million people were compromised. A class action law suit has been filed against RBS WorldPay.

**UPDATE** (5/28/09): RBS WorldPay says it has returned to Visa's and MasterCard's lists of validated service providers. It was recently certified as compliant with Payment Card Industry Data Security Standard (PCI DSS) version 1.2.

**UPDATE** (4/05/10): Russian authorities have nabbed the man accused of masterminding a coordinated global ATM heist of $9.5 million from Atlanta-based card processing company RBS WorldPay.

**UPDATE** (8/09/10): Sergei Tsurikov of Estonia was brought to Atlanta by the FBI. He pleaded not guilty to computer fraud, conspiracy to commit computer fraud, wire fraud, conspiracy to commit wire fraud, and aggravated identity theft. The FBI is in the process of extraditing others involved in the international hack.

**UPDATE** (8/31/10): Another person has been charged with participating in the computer fraud attack. Vladislav Anatolievich Horohorin is alleged to have used a prepaid payroll card to conduct fraudulent attacks on ATMs in Moscow.

**UPDATE** (9/15/10): A previously unnamed member of the hacking group will be tried in a Russian court for his involvement in the RBS breach. Eugene Anikin's criminal case was forwarded to Zaeltsovskiy District Court in Novosibirsk for consideration.

**UPDATE** (2/7/2011): Yevgeny Anikin, 27, pleaded guilty to participating in a hacking ring that stole $10 million from former Royal Bank of Scotland division WorldPay.

**UPDATE** (8/21/2012): Sonya Martin was sentenced to 2.5 years in federal prison for fraudulently obtaining over $9 million from an Atlanta payroll company. She was a cell leader in the plan that involved organized computer hacking and ATM cashout schemes. She worked with other members of the network to target 2,100 ATMs in 280 cities around the world.

An unauthorized breach of private information resulted in the information release of 16,857 names, Social Security numbers, phone numbers, and other private details of people who had applied for benefits. The information was flashed on a pair of privately run Web sites, but for how long was unclear.

A former billing department employee is in custody on $895,000 bail for allegedly stealing the personal information of 1,000 hospital patients and using it to bilk insurance companies.

An external computer hard drive was discovered missing or stolen. Current and former wellness center members' Social Security numbers were on the hard drive.
Information Source: Dataloss DB
December 22, 2008  
**University of North Carolina School of the Arts**  
Winston-Salem, North Carolina  
EDU  DISC  2,700

Names and Social Security numbers may have been accidentally exposed in a security breach involving a university computer server. The security breach occurred in May of 2006 and affected students who were enrolled between 2003 and 2006.

Information Source: Dataloss DB  
December 21, 2008  
**Connecticut Department of Motor Vehicles**  
Wethersfield, Connecticut  
GOV  PHYS  155

The Connecticut Department of Motor Vehicles is notifying customers that their personal information may have been on a computer stolen from a mobile service center vehicle while it was being repaired. Personal data on the computer included names, addresses, date of birth, license numbers, photo and signature.

Information Source: Media  
December 19, 2008  
**Austin Peay State University**  
Clarksville, Tennessee  
EDU  PHYS  750

Two computers containing personal information were stolen. The computers contained names and Social Security numbers of students.

Information Source: Dataloss DB  
December 18, 2008  
**Bill Dube Ford/Toyota**  
Dover, New Hampshire  
BSR  PORT  10,000

Personal information from thousands of people in New Hampshire and Massachusetts has been compromised after a data backup tape was stolen. The data include names, addresses, Social Security numbers and driver's license information.

Information Source: Dataloss DB  
December 17, 2008  
**New Hampshire Department of Health and Human Services**  
Concord, New Hampshire  
GOV  DISC  9,300

Health and Human Services mistakenly released the Social Security numbers and other personal information of Medicare Part D recipients. The information was mistakenly attached to an e-mail to health care organizations including nursing homes.

Information Source: Dataloss DB  
December 15, 2008  
**University of North Carolina**  
Greensboro, North Carolina  
EDU  HACK  Unknown

A breach of the accounting computer systems at UNC-Greensboro may have exposed personal employee information to intruders. The breach was detected on a computer in the Accounting Services office, in the form of a virus that may have allowed unauthorized access.

Information Source: Dataloss DB  
December 15, 2008  
**Louisiana Department of Revenue**  
Baton Rouge, Louisiana  
GOV  DISC  299

The Louisiana Department of Revenue accidentally divulged the personal information of taxpayers to other people with tax debts. The department says letters mailed to taxpayers who owe money also listed the name, address, Social Security number and debt for a different taxpayer on the other side of the paper.

Information Source: Dataloss DB  
December 14, 2008  
**Zyacorp Entertainment Cinemagic Stadium**  
Merrimack, New Hampshire  
BSR  HACK  Unknown

Hackers broke into a Merrimack movie theater's servers and stole customers' credit card information.
December 12, 2008  
**DJO, Empi Recovery Services**  
St. Paul, Minnesota

A laptop was stolen from an employee’s car in Minneapolis. The laptop contained the names, addresses, account balances, insurance company, and Social Security numbers of patients.

December 12, 2008  
**Oregon Health and Science University**  
Portland, Oregon

A laptop stolen in Chicago this week contained health records. It was stolen from a hotel while an OHSU employee was there on business. The data could include medical record numbers, names, telephone numbers, dates of birth, gender, Social Security numbers, addresses, medical diagnosis category and category of treatment - but not the specific treatments.

December 11, 2008  
**Hewlett-Packard, Symantec**  
Houston, Texas

Several thousand employee records were contained on a laptop that was stolen from an HP employee based in the Houston area. At first HP thought that there was no sensitive information on the laptop, but after looking into back-up files, the company realized that it contained names and Social Security numbers of current and former employees.

December 5, 2008  
**Cal Poly Pomona**  
Pomona, California

A student informed the university that he accessed an Excel file containing his personal information and others while on the Internet. The information includes names, addresses, phone numbers and Social Security numbers.

December 3, 2008  
**Central California Appellate Program**  
Sacramento, California

A backup computer disk was in a safe taken by thieves who broke into a storage facility. Besides Social Security numbers, the disk contained tax identification numbers, addresses, telephone numbers and e-mail addresses.

December 2, 2008  
**US Army**  
Washington, District Of Columbia

A possible security breach regarding the personal information stored on a lost laptop computer may have affected more than 6,000 beneficiaries. Names, Social Security numbers and health information of at least 26 individuals were stored on the laptop. However, information on approximately 6,000 other patients also may have been on the missing computer.

December 2, 2008  
**Florida Agency for Workforce Innovation**  
Tallahassee, Florida

Employment information and more than a quarter million Social Security numbers were posted online. The breach occurred when several thousand Excel and text files containing millions of employment records were posted in the course of developing a new website.

November 26, 2008  
**Luxottica Group, Things Remembered**  
Mason, Ohio
A routine check by the information technology department discovered that a hacker had been inside a computer mainframe and downloaded the personal information of former workers. The victims lost names, addresses and Social Security numbers to the hacker.

**Information Source:**
Dataloss DB

**November 25, 2008**
**Weber State University**
Ogden, Utah

In a break in, thieves made off with approximately $1,600 in cash, three computers and a postal scale. Hard-copy records of post office box rental information was also taken from the center. Some of the stolen rental cards contained names, addresses and Social Security numbers for members of the campus community who rented post office boxes in the union building during the past eight years.

**Information Source:**
Dataloss DB

**November 24, 2008**
**Starbucks Corp.**
Seattle, Washington

A laptop containing private information on employees was stolen. The information included names, addresses and Social Security numbers.

**Information Source:**
Dataloss DB

**November 22, 2008**
**Maryland Department of the Environment**
Baltimore, Maryland

Two laptop computers containing the names and Social Security numbers of people formerly employed by the Maryland Department of the Environment were stolen.

**Information Source:**
Dataloss DB

**November 21, 2008**
**Jackson-Madison County School System**
Jackson, Tennessee

A computer disk containing Social Security numbers and test scores was stolen from a principal’s car.

**Information Source:**
Dataloss DB

**November 21, 2008**
**B.J. Accessories and Tax Preparation**
New Bern, North Carolina

A computer was stolen containing identity information on about 70 people. Information on the computer may have had Social Security Numbers on it.

**Information Source:**
Dataloss DB

**November 20, 2008**
**Law office of former Texas attorney**
Rio Grande Valley, Texas

An individual purchased a used computer and memory stick from a pawn shop. He discovered sensitive information on the computer and traced it to the law office of a Texas attorney who no longer practices law. The attorney, Aaron Pena, Jr., is now a Texas State Representative. His spokesperson told news sources that the computer’s hard drive had been wiped before the machine was donated to charity. The news team visited other pawn shops and found several other used computers which also contained sensitive personal information.

**Information Source:**
Media

**November 12, 2008**
**University of Florida College of Dentistry**
Gainesville, Florida

Some current and former dental patients have been notified that an unauthorized intruder recently accessed a College of Dentistry computer server storing their personal information. College information technology staff members were upgrading the server and found software had been installed on it remotely. Information stored on the server included names, addresses, birth dates, Social Security numbers and, in some cases, dental procedure information for patients dating back to 1990.

**Information Source:**
Dataloss DB
November 12, 2008  Pinellas County and Florida state agency offices  Pinellas County, Florida

Documents with Social Security numbers, medical information and other legally protected data were found in trash containers at government buildings. Also found were hundreds of improperly discarded records that included medical data, privileged communications between attorneys and clients, juvenile defendant records and child abuse materials.

November 11, 2008  Sinclair Community College  Dayton, Ohio

The names and Social Security numbers of almost 1,000 employees were inadvertently left open to public view on the Internet for about a year. A spreadsheet with information on people who worked at the school in 2000 and 2001 was placed in a computer folder by an employee. The employee didn't realize the folder could be viewed on the Internet.

November 9, 2008  Texas A&M University  Corpus Christi, Texas

Through an Internet search on the university's Web site, a student viewed a document that listed admissions applicants from 2005. The page listed names and Social Security numbers.

November 9, 2008  City of Charlottesville  Charlottesville, North Carolina

Two laptops containing voter registration information were stolen from a building at Tonsler Park in Charlottesville sometime after the polls closed. The information on the computers included names, addresses, date of birth and DMV customer number.

November 7, 2008  Christus Health Care  Houston, Texas

(800) 877-9056

Two computer back-up tapes were stolen. Someone broke into a car in a Houston parking lot and took the tapes. The information on the tapes included patient names, Social Security numbers, demographic information, and in some cases, diagnosis codes.

November 7, 2008  Arizona's Department of Economic Security  Phoenix, Arizona

(DES) is notifying the families of about 40,000 children that their personal data may have been compromised following the theft of several hard drives from a commercial storage facility. The information stored on the stolen disks included the names, addresses and phone numbers of families whose children were referred to the DES for early intervention services over the past several years. In the cases of families that had applied for and received services from the agency, their records also included Social Security numbers.

November 6, 2008  Express Scripts  St. Louis, Missouri

Express Scripts has received a letter demanding money from the company under the threat of exposing records of millions of patients. The letter, included personal information on 75 people covered by Express Scripts, including birth dates, Social Security numbers and prescription information. Express manages prescription benefits for roughly 50 million people.

UPDATE 10/1/09: Express Scripts notified about 700,000 consumers that their records may have been breached.
A computer tape containing Social Security numbers, addresses, and financial information was either lost or stolen. About 8,000 records of present and former clients contained Social Security numbers another 13,000 had other identification information that was contained on the tape.

A laptop computer belonging to a Division of Aging and Adult Services employee was stolen. The computer contained information about people receiving home and community services.

A laptop stolen had been used for background checks on school workers and included their fingerprints and some personal information such as their names, addresses, birthdates and race. The laptop did not have Social Security numbers and the data was stored in files that require a password to be opened.

Personal information, including Social Security numbers, was inadvertently released to a local union representing some district workers. The 5,000 employees are more than half the district’s work force. Included were about 700 members of International Union of Operating Engineers Local 609, which represents custodial, nutritional services, security- and alarm-monitoring workers.

Personal information, including some Social Security numbers, of patients at the Veterans Affairs Medical Center in Portland was inadvertently posted on a public Web site.

A laptop computer containing limited health information on 100,000 patients was stolen from an employee's car. Included were 7,400 patients whose Social Security numbers were stored on the computer.

Passport applicants in the D.C. area were notified of a breach in a database that allowed a ring of thieves to obtain confidential information so they could fraudulently use credit cards stolen from the mail. The compromised included information Social Security numbers, physical descriptions, names and places of birth of the applicants’ parents.
An IT contractor used the personal data of four Shell workers as part of an unemployment insurance claims scam. Employees of a third-party contractor misused information stored in a corporate database. The database includes records for a majority of current and former Shell employees. Misused data included names, dates of birth and Social Security numbers.

**Information Source:**
Data loss DB

**October 24, 2008**
*Shenendehowa Transportation Employees*
*Shenendehowa, New York*

A Shenendehowa sophomore was arrested after he allegedly accessed the personal data of some 250 transportation employees due to a school district error in configuring information on a new computer server. The student was able to use his student password to access an employee domain and 250 names of past and present Shenendehowa transportation employees, their Social Security numbers, driver’s license numbers and more.

**Information Source:**
Data loss DB

**October 23, 2008**
*Medical Mutual of Ohio*
*Columbus, Ohio*

Eleven computer disks containing personal information on Ohio retirees and employees are missing, disks are most likely somewhere in the postal system. It seems insufficient postage was placed on the envelopes [containing the disks], therefore they are believed that they are likely to still be safe within the postal system.

**Information Source:**
Data loss DB

**October 22, 2008**
*KRM Management*
*Fresno, California*

Offices of KRM Management were broken into and stole two dozen computers, on one of those hard drives were Social Security numbers, birth dates and addresses. One missing laptop computer is causing the most concern. It contained sensitive and confidential information on close to 5700 city employees who filed worker’s comp claims dating back to 1973. Hundreds are or were police officers.

**Information Source:**
Data loss DB

**October 19, 2008**
*Mary Washington Hospital*
*Fredericksburg, Virginia*

A security breach in an online computer system exposed the private medical information of some of its maternity patients. Social Security numbers, phone numbers, addresses, insurance carrier, birth dates and doctor’s names were exposed.

**Information Source:**
Data loss DB

**October 18, 2008**
*City of Goodyear*
*Goodyear, Arizona*

A list of their Social Security numbers was stolen from the car of a staffer who had taken the data home. Burglars took the list while the employee’s car was parked at her home.

**Information Source:**
Data loss DB

**October 17, 2008**
*The Planet*
*Houston, Texas*

A security breach that may have affected the customer portal account and server passwords, was discovered. The Planet identified the methods by which the systems were compromised and have closed those holes. Only two user accounts were definitely affected, and no credit card information is believed to have been compromised.

**Information Source:**
Media

**October 15, 2008**
*City of Indianapolis*
*Indianapolis, Indiana*

A spreadsheet containing the names, Social Security numbers and dates of birth for people charged with minor offenses in
2006 and 2007 was accidentally posted on the city of Indianapolis' new Web site.

**Information Source:**
Dataloss DB

**October 13, 2008**

**Southwest Mississippi Community College**

**Summitt, Mississippi**

EDU DISC 1,000

Former Southwest Mississippi Community College students had some of their personal information made available temporarily on the Internet. The breach involved names, addresses, and in some cases, Social Security numbers.

**Information Source:**
Dataloss DB

**October 7, 2008**

**University of North Dakota Alumni Association**

**Grand Forks, North Dakota**

EDU PORT 84,554

A laptop computer containing sensitive personal and financial information on alumni, donors and others was stolen from a vehicle belonging to a software vendor retained by the UND. The information, included individuals' credit card and Social Security numbers.

**Information Source:**
Dataloss DB

**October 7, 2008**

**West Virginia Dept. of Administration**

**Charleston, West Virginia**

GOV PORT 535

A laptop was taken from an auditor's vehicle. It contains payroll and benefits information for 425 employees of the state Insurance Commission and 110 employees of the Department of Health and Human Resources' Bureau of Medical Services and Child Support Enforcement Division. The information includes full names or first names and Social Security numbers.

**Information Source:**
Dataloss DB

**October 1, 2008**

**Foothills Parks and Recreation District**

**Littleton, Colorado**

GOV HACK Unknown

The district noticed unusual activity last week which they believe was caused by a virus introduced to cover up the actions of an intruder. Some customer information, including credit card information, may have been compromised.

**Information Source:**
Dataloss DB

**September 30, 2008**

**Dormitory Authority's**

**New York City, New York**

GOV PORT 3,600

On the trip from the Albany headquarters of this New York based construction organization, to their data center in New York City 5 tapes had fallen out of their yellow mailing envelope. The tapes contained personal private or sensitive information of over 600 employees and approximately 3,000 vendors. Social Security numbers and tax ID numbers were compromised.

**Information Source:**
Media

**September 30, 2008**

**University of Indianapolis**

**Indianapolis, Indiana**

EDU HACK 11,000

A hacker attacked the University of Indianapolis' computer system and gained access to personal information and Social Security numbers for 11,000 students, faculty and staff.

**Information Source:**
Dataloss DB

**September 30, 2008**

**Blue Cross & Blue Shield**

**Baton Rouge, Louisiana**

MED DISC 1,700

A document containing the personal data was accidentally attached to a general e-mail being sent out to brokers notifying them of a software upgrade. Information such as Social Security numbers, phone numbers and addresses were exposed.

**Information Source:**
Dataloss DB

**September 26, 2008**

**Fort Wayne Community Schools**

**Fort Wayne, Indiana**

EDU UNKN 3,348

605
A man arrested on forgery and counterfeiting charges may have used some employees' personal information in his possession. A 94-page document containing personal information belonging to 3,348 FWCS employees was found by police. The information included names, Social Security numbers, dates of birth and salary.

**Information Source:**
Dataloss DB

**September 23, 2008**

**Texas Lottery Commission**
Austin, Texas

A former Texas Lottery Commission computer analyst has been arrested for copying the personal data of Texas lottery winners. He downloaded his own work files off his computer and took them to his next job. The names and Social Security numbers of 27,075 mid-level lottery winners -- people who have won prizes from $600 up to around $1 million -- were on the employee’s hard drive.

**UPDATE** 10/31/08: 89,000 lottery winners are being notified their personal information, including Social Security numbers, may have been breached.

**Information Source:**
Dataloss DB

**September 22, 2008**

**Sonoma State University**
Sonoma, California

Social Security numbers have been exposed to the public through an internal department website.

**Information Source:**
Dataloss DB

**September 19, 2008**

**Texas A&M University**
College Station, Texas

A class roster was among some documents located on a computer server that was hacked. The class roster was for Economics-2301 held during the first summer session of 2004. Social Security numbers were part of the information on those documents.

**Information Source:**
Dataloss DB

**September 15, 2008**

**Forever21**
Los Angeles, California


If you shopped at the stores between November 26, 2003, and October 24, 2005, criminals may have hijacked your credit and debit card numbers from its computers. Approximately 20,500 of these numbers were obtained from the Fresno store transaction data. The data included credit and debit card numbers and in some instances expiration dates and other card data, but did not include customer name and address.

**Information Source:**
Dataloss DB

**September 13, 2008**

**State Farm Insurance**
Surprise, Arizona

An employee of State Farm fraudulently used customer information to open credit-card accounts. Customers' Social Security numbers, driver's license numbers, addresses and possibly financial account numbers could have been accessed.

**Information Source:**
Dataloss DB

**September 12, 2008**

**Tennessee State University**
Nashville, Tennessee

A flash drive containing the financial information and Social Security numbers of students was reported missing. The flash, which contained financial records of TSU students dating back to 2002.

**Information Source:**
Dataloss DB

**September 11, 2008**

**Marshall University**
Charleston, West Virginia

The names and Social Security numbers of Marshall University students were openly available on the Internet.

**Information**

606
Some students are being notified by the College that their personal information may have been exposed in a recent computer breach. The compromised computer contained a file with names and Social Security numbers of students stored on its hard drive.

Information Source: Dataloss DB

September 10, 2008

Ivy Tech Community College
Bloomington, Indiana

EDU DISC Unknown

http://www.ivytech.edu/about/security/

An employee of the college used an internal file sharing system to send a file that consisted of students enrolled in the spring 2008 semester for distance education courses. The employee intended to share the file with a single employee of the college. Instead, due to a clerical error, the invitation to view the file was sent to a list of all Indianapolis region employees.

Information Source: Dataloss DB

September 10, 2008

Franklin Savings and Loan
Cincinnati, Ohio

BSF HACK 25,000

(877) 579-2267, (513) 605-4378

An unauthorized person gained access to a database on a company web site containing personal information such as names, addresses, phone numbers, account numbers, account balances and Social Security numbers.

Information Source: Dataloss DB

September 9, 2008

University of Pittsburgh
Pittsburgh, Pennsylvania

EDU PORT Unknown

A laptop containing personal information including names and Social Security numbers was stolen. The laptop, stolen from Mervis Hall was being used by an employee to conduct surveys of alumni that are used in college rankings.

Information Source: Dataloss DB

September 5, 2008

East Burke High School
Morganton, North Carolina

EDU DISC 163

For the past five years, East Burke High School’s web site exposed files containing personal information including names, Social Security numbers, addresses, phone numbers, job titles, email addresses and unlisted phone numbers of teachers, bus drivers, custodians and other staff members on the Internet.

Information Source: Dataloss DB

September 2, 2008

Clarkson University
Potsdam, New York

EDU DISC 245

A non-malicious student intruder gained access to a restricted server and promptly reported the vulnerability to campus authorities. Approximately 245 employees and former employees had personal information, including name, social security number, and date of birth, compromised during the security breach. The file containing personal information was a record of employees that had university credit cards known as purchase cards (or p-cards). Any university member requesting a p-card must provide their Social Security number and date of birth on the application form.

Information Source: Dataloss DB

August 30, 2008

Ohio Police & Fire Pension System
Columbus, Ohio

GOV INSD 13,000

A former mailroom supervisor at the Ohio Police & Fire Pension System forwarded the names, addresses and Social Security numbers from his work e-mail address to his personal e-mail address before quitting his job. The file contains information for 13,000 of the approximately 24,000 retired members of the Ohio Police & Fire Pension System, most of whom are former police officers.
A recently stolen laptop contained the names, birth dates and Social Security numbers of about 12,700 applicants to the National Technical Institute for the Deaf and another 1,100 people at Rochester Institute of Technology. The laptop belonged to an employee and was stolen on Monday from an office at NTID. People at RIT, who are not affiliated with NTID, are affected because their personal information was being used as part of a control group in an internal study.

Thousands of medical charts were found in an abandoned storage unit that was purchased for $25.

A glitch during a computer upgrade caused the names, addresses and Social Security numbers of licensed agents to be exposed on the Internet. The commission was transferring its online programs to a new server when the sensitive electronic file, which is not normally posted on the Internet, was left unsecured and slipped in among the commission materials that could be seen online.

It was confirmed that several customers of the Camelot branch, at Cape Coral Parkway and Chiquita Boulevard, who used their debit cards have had their accounts fraudulently charged because someone placed a skimming device on the ATM. The device collected each person’s card information, including personal identification numbers, and allowed different debit cards to be created with that information.

The Washington Trust Co. has notified about 1,000 customers that their debit and credit card accounts might have been compromised in a suspected security breach at an unidentified MasterCard merchant. The company is investigating a suspected security breach of a U.S. e-commerce-based merchant’s Web server which contained debit card data.

Reynoldsburg school officials were phasing out the use of Social Security numbers in the district’s student database when someone stole a laptop containing that information. The district laptop, taken from a computer technician’s car, also included names, addresses and phone numbers for two-thirds of the district’s enrollment.

Customers who paid for items at a YMCA fund-raiser with checks or credit cards are being warned about a burglary at which credit and debit card numbers were taken.
An instructor for classes offered through the Division of Continuing Education, taught through the UFM Community Learning Center, reported an overnight theft of numerous items from a car, which was parked outside a Manhattan residence. Items taken included a backpack with a list of names and Social Security numbers of 86 K-State students who had taken that instructor’s classes from fall 2007 through summer 2008.

Information
Source: Dataloss DB

August 26, 2008 Pennsylvania Department of Public Welfare Harrisburg, Pennsylvania GOV DISC 2,845

Paper jams in a state Department of General Services mail inserter caused benefit renewal packets to go to the wrong Pennsylvania welfare client’s homes. Nearly half of them included the intended recipients’ Social Security numbers.

Information
Source: Dataloss DB

August 26, 2008 Prince William County Public Schools Manassas, Virginia EDU DISC 2,600

Personal information of some students, employees and volunteers was accidentally posted online by a Prince William County Public Schools employee. Information for more than 2,600 people was exposed through a file-sharing program by an employee working from home on a personal computer. The compromised information included: names, addresses and student identification numbers of more than 1,600 students names and Social Security numbers of 65 employees other confidential information for about 250 employees and the names, addresses and e-mail addresses of more than 700 volunteers.

Information
Source: Dataloss DB

August 22, 2008 Liberty McDonald’s Restaurant Liberty, Kentucky BSR INSD Unknown

An employee at a Liberty McDonald’s restaurant, took credit or debit cards from drive-through customers and used a device she had hidden near the window to swipe the cards to record their numbers. The information on the device then was downloaded and used to make new cards either in the names of the persons to which the original cards belonged or in the names of the perpetrators.

Information
Source: Media

August 19, 2008 Kingston Tax Service Kingston, Washington BSO PORT Unknown

Office computers were stolen from the business. On each of the computers is information which can be used by identity thieves including credit card information and Social Security numbers.

Information
Source: Dataloss DB

August 18, 2008 Dominion Enterprises Richmond, Virginia BSO HACK 92,095

(757) 351-7951

A computer server within InterActive Financial Marketing Group (IFMG), a division of Dominion Enterprises located in Richmond, Virginia, was hacked into and illegally accessed by an unknown and unauthorized third party between November 2007 and February 2008. The data intrusion resulted in the potential exposure of personal information, including the names, addresses, birth dates, and Social Security numbers of 92,095 applicants who submitted credit applications to IFMG’s family of special finance Web sites.

Information
Source: Dataloss DB

August 18, 2008 Keller High School Keller, Texas EDU DISC 45

Keller family’s received a mailing from Keller High School last week. Upon opening it, they found two enrollment forms. One was an emergency-care authorization form. But the other was a student information form containing another classmate’s Social Security number, student ID number, home address, phone number and contact information for his parents at home and at work. They quickly realized that their child’s private information, which they used to set up their college fund and other accounts, was mailed to someone else.
The test-preparatory firm accidentally published the personal data and standardized test scores of tens of thousands of Florida students on its Web site. One file on the site contained information on about 34,000 students in the public schools in Sarasota, Fl. Another folder contained dozens of files with names and birth dates for 74,000 students in the school system of Fairfax County, Va.

Information Source:
Dataloss DB

August 14, 2008  Wuesthoff Medical Center
Rockledge, Florida

Hundreds of people in Brevard County found out their personal information was stolen. Names, Social Security numbers and even personal medical information were posted on the Internet.

Information Source:
Dataloss DB

August 13, 2008  Charter Communications
Greenville, South Carolina

Computers were stolen from the company's Greenville offices and contained records of more than 9,000 Charter employees nationwide. The information included Social Security numbers, dates of birth and driver's license numbers.

Information Source:
Dataloss DB

August 12, 2008  Wells Fargo
Minneapolis, Minnesota

Wells Fargo is notifying customers that hackers have accessed their confidential personal data by illegally using its access codes. Personal information including names, addresses, dates of birth, Social Security numbers, driver's licence numbers and in some cases, credit account information was accessed by unauthorised persons.

Information Source:
Dataloss DB

August 12, 2008  Child Protective Services
San Antonio, Texas

Hundreds of private, personal records were discarded with the trash, including records detailing medical histories of clients with diseases and drug addictions. Documents showing sexual abuse and information that could be used for identity theft, such as Social Security numbers, were also found in the trash.

Information Source:
Media

August 7, 2008  Harris County Hospital
Houston, Texas

A lower-level Harris County Hospital District administrator downloaded medical and financial records for patients with HIV, AIDS and other medical conditions onto a flash drive that later was lost or stolen. This may have been a violation of law. The data on the device included the patients' names, medical record numbers, billing codes, the facilities where the office visits occurred and other billing information. It also included the patients' Medicaid or Medicare numbers, which can indicate their Social Security numbers or those of their spouses.

Information Source:
Dataloss DB

New York, New York

A laptop containing personal information for about 33,000 people was reported stolen in a possible security breach for the Clear Program. The laptop was stolen at San Francisco International Airport. The stolen information included names, addresses, dates of birth, and driver's license numbers or passport numbers.
A contractor who manages the student information database had a flash drive lost or stolen. Information on the drive included the names, addresses, credit card numbers and Social Security numbers.

**Information Source:**
Dataloss DB

**August 4, 2008**
**Arapahoe Community College**
**Littleton, Colorado**
EDU PORT 15,000

Thieves stole 10 desktop computers containing employees’ personal information from the Oakland school district’s main office. District officials are still determining what information was on each computer, but the machines may contain personal information provided to the district when employees were hired. It is unknown how many employees’ records were on the computers.

**Information Source:**
Dataloss DB

**August 3, 2008**
**Oakland School District**
**Oakland, California**
EDU STAT Unknown

The FBI on Friday arrested a former Countrywide Financial Corp. employee and another man in an alleged scheme to steal and sell sensitive personal information, including Social Security numbers. The breach occurred over a two-year period though July. The insider was a senior financial analyst at Full Spectrum Lending, Countrywide’s subprime lending division. The alleged data thief was said to have downloaded about 20,000 customer profiles each week and sold files with that many names for $500, according to the affidavit. He typically would e-mail the data in Excel spreadsheets to his buyers, often using computers at Kinko’s copying and business center stores. Some, perhaps most, and possibly all the names were being sold to people in the mortgage industry to make new pitches.

**UPDATE** (1/30/2009): Bank of America will pay Connecticut $350,000 as part of a settlement. The bank will also provide at least $25,000 to reimburse Connecticut residents forced to pay for freezing and unfreezing their credit reports.

**UPDATE** (4/09/2010): Employees of Countrywide Financial stole and sold “tens of thousands, or millions” of customers’ personal financial information, invading their privacy and exposing them to identity theft, according to class action claims in Ventura County Court, CA. Sixteen named plaintiffs sued Countrywide Financial, Countrywide Home Loans, and Bank of America, which bought Countrywide, the poster boy for the subprime mortgage crisis.

**UPDATE** (5/08/2010): For information about the settlement, visit www.CWdataclaims.com or call (866) 940-3612.

**UPDATE** (8/24/2010): Bank of America has settled over 30 lawsuits involving Countrywide Financial customer data theft. As many as 17 million customers who received a mortgage or used Countrywide to service a mortgage before July 1, 2008 will receive reimbursement and identity theft insurance. Identity theft claims can be filed after September 6.

**UPDATE** (9/28/2011): A former employee responsible for the breach was sentenced to eight months in prison and ordered to repay $1.2 million in costs.

**UPDATE** (7/13/2012): A small group of people objected to a proposed settlement and decided to split from a larger class action lawsuit. A court dismissed their claim because they could not sufficiently prove an out of pocket loss.

**Information Source:**
Dataloss DB

**August 2, 2008**
**Countrywide Financial Corp.**
**Calabasas, California**
BSF INSD 17,000,000

A laptop stolen from TVA contained Social Security numbers and reflects generally inadequate policies and procedures for tracking computers at the agency. The laptop was one of approximately 26 computer and computer-related items stolen from TVA between May 26, 2006, and Nov. 30, 2007, according to the IG, although the report stated it was unclear whether sensitive information was present on any of the laptops or PCs stolen from TVA.

**Information Source:**
Dataloss DB

**August 1, 2008**
**Tennessee Valley Authority**
**Knoxville, Tennessee**
GOV PORT Unknown

A flash drive with Social Security numbers and other personal information from former Dayton-area Delphi workers was removed from the unattended laptop of a state employee and is missing. The drive included the names, addresses, telephone numbers as well as the Social Security numbers of the workers.

**Information Source:**
Dataloss DB

**August 1, 2008**
**Ohio Department of Job & Family Services, Delphi Automotive**
**Columbus, Ohio**
BSO PORT 2,600

**City of Yuma**
**July 21, 2008**
GOV DISC 300
The Social Security numbers of about 300 city of Yuma employees were unintentionally released in an e-mail sent to city administrative personnel.

Information Source: Dataloss DB

July 31, 2008 University of Texas, Dallas
Dallas, Texas

http://www.utdallas.edu/infosecurity/

A security breach in UTD’s computer network may have exposed Social Security numbers along with names, addresses, email addresses or telephone numbers: 4,406 students who were on the Dean’s List or graduated between 2000 and 2003; 3,892 students who were contacted to take part in a survey by the Office of Undergraduate Education in 2002; 88 staff members from Facilities Management; 716 faculty and staff members listed in a space inventory record from 2001.

Information Source: Dataloss DB

July 29, 2008 Blue Cross and Blue Shield of Georgia
Atlanta, Georgia

Benefit letters containing personal and health information were sent to the wrong addresses last week. The letters included the patient’s name and ID number, the name of the medical provider delivering the service, and the amounts charged and owed. A small percentage of letters also contained the patient’s Social Security numbers.

Information Source: Dataloss DB

July 29, 2008 Anheuser-Busch
St. Louis, Missouri

A laptop containing personal information of current and former employees, including some from Hampton Roads, was stolen from a St. Louis-area Anheuser-Busch office. Information contained on the computer included employees’ Social Security numbers, home addresses and marital status.

Information Source: Dataloss DB

July 28, 2008 Facebook
Palo Alto, California

Facebook accidentally publicly revealed personal information about its members, which could be useful to identity thieves. The full dates of birth of many of Facebook’s 80 million active users were visible to others, even if the individual member had requested that the information remained confidential.

Information Source: Media

July 26, 2008 Connecticut College, Wesleyan University, Trinity College
Middletown, Connecticut

A Connecticut College library system was breached by hackers apparently looking to set up chat rooms or send spam e-mails. The system’s database included the names, addresses and Social Security or driver’s license numbers of approximately 2,800 Connecticut College library patrons, 12 Wesleyan University patrons and three from Trinity.

Information Source: Dataloss DB

July 25, 2008 Grady Memorial Hospital
Atlanta, Georgia

Hospital records were stolen, although it remains unknown how many patient records were compromised, which patients were affected or how the records were stolen. The records pertained to recorded physician comments that Grady sent to a vendor to transcribe into medical notes. The records were stolen from a subcontractor employed by the vendor.
July 25, 2008  
**Ohio University College of Osteopathic Medicine**  
Columbus, Ohio  

http://www.ohiocore.org/answers, (866) 437-8698

A clerical error led to the online posting of the names and Social Security numbers of people who spoke at Ohio University’s Centers for Osteopathic Research and Education. A spreadsheet that contained the information had been accessible since March 20 and was discovered when a nurse found the information last week while conducting online research. In addition to names and Social Security numbers, the spreadsheet included contact numbers, addresses, their speaking topics and federal employer identification numbers.

July 24, 2008  
**Village of Tinley Park**  
Chicago, Illinois

Computer backup tapes that contain thousands of Social Security numbers of Tinley Park residents have been lost. The tapes containing information from as long ago as 15 years were lost while being transferred from the village hall to another site within the Chicago suburb.

July 24, 2008  
**Saint Mary’s Regional Medical Center**  
Reno, Nevada

An unauthorized person may have accessed the St. Mary’s database. The database, used for Saint Mary’s health education classes and wellness programs, contained personal information such as names and addresses, limited health information and some Social Security numbers. The database did not contain medical records or credit card information.

July 24, 2008  
**Hillsborough Community College**  
Tampa, Florida

Hillsborough Community College warned its employees to monitor their bank accounts because an HCC programmer’s laptop was stolen from a hotel parking lot in Georgia. The programmer had been working on a payroll project for a group of employees using their names, bank-routing numbers, retirement information and Social Security numbers.

July 24, 2008  
**University of Houston**  
Houston, Texas

The names and Social Security numbers of University of Houston students were inadvertently posted on the Internet for more than two years. The posting occurred when a math department lecturer posted student grades on a UH Web server in October 2005.

July 23, 2008  
**San Francisco Human Services Department**  
San Francisco, California

Potentially thousands of files containing personal information was exposed after a San Francisco agency left confidential files in unsecured curbside garbage and recycling bins. In some cases entire case files were discarded. Blown up copies of social security cards, driver’s licenses, passports, bank statements and other sensitive personal information were all left in these unlocked bins.

July 21, 2008  
**Hawaii State Department of Public Safety**  
Honolulu, Hawaii

A reporter requested statistics from the State Department of Public Safety. Though the reporter only wanted the number
of people who use medical marijuana, he was sent an email with patient names, addresses, plant locations, certificate numbers, and the names of prescribing physicians. Patients became aware of the issue when information was printed in a front-page news story, though no patients were identified.

Information Source: Databreaches.net

July 19, 2008  Minneapolis Veterans Home
Minneapolis, Minnesota  GOV  STAT  336

A backup computer server stolen from the Minneapolis Veterans Home contained telephone numbers, addresses, next-of-kin information, dates of birth, Social Security numbers and some medical information, including diagnoses for the home’s 336 residents.

Information Source: Databreaches.net

July 17, 2008  Bristol-Myers Squibb
Jacksonville, Florida  BSO  PORT  42,000

A backup computer-data tape containing employees’ personal information, including Social Security numbers, was stolen recently. The backup data tape was stolen while being transported from a storage facility. The information on the tapes included names, addresses, dates of birth, Social Security numbers and marital status, and in some cases bank-account information. Data for some employees’ family members also were on the tape.

Information Source: Databreaches.net

July 17, 2008  University of Maryland
College Park, Maryland  EDU  DISC  23,000

University of Maryland accidentally released the addresses and Social Security numbers of thousands of students. A brochure with on-campus parking information was sent by U.S. Mail to students. The University discovered the labels on the mailing had the students' Social Security numbers on it.

Information Source: Databreaches.net

July 17, 2008  Department of Consumer Affairs
Sacramento, California  GOV  INSD  5,000

A Consumer Affairs personnel specialist in Sacramento, emailed an alpha personnel file containing names and Social Security numbers of the department’s more than 5,000 staff to a personal Yahoo email account at the end of the day, her last day at the department.

Information Source: Databreaches.net

July 16, 2008  Greensboro Gynecology Associates
Greensboro, North Carolina  MED  PORT  47,000

A backup tape of patient information was stolen from an employee who was taking the tape to an off-site storage facility for safekeeping. The stolen information included patients’ names, addresses, Social Security numbers, employers, insurance companies, policy numbers and family members.

Information Source: Databreaches.net

July 16, 2008  Indiana State University
Terre Haute, Indiana  EDU  PORT  2,500

A password-protected laptop computer containing personal information for current and former Indiana State University students was stolen. The laptop contained data for students who took economics classes from 1997 through the spring semester 2008. The information includes names, grades, e-mail addresses and student identification numbers and in some cases Social Security numbers.

UPDATE(7/22/08): The laptop computer was mailed anonymously back to the professor it was stolen from six days after it was stolen along with other personal items.

Information Source: Databreaches.net

July 15, 2008  Weber Law Firm
Houston, Texas  BSO  PHYS  Unknown

Sheriff’s deputies uncovered hundreds of people's personal financial files that had been discarded in a dumpster in
northwest Houston. Box after box of records including personal financial records, documents with Social Security numbers, people’s medical files and more were found in the dumpster.

Information
Source:
Dataloss DB

July 15, 2008
Missouri National Guard
Jefferson City, Missouri

GOV  UNKN  2,000

(888) 526-6664 ext. 7888, (312) 555-9500 ext. 7888 Soldier deployed overseas

The Missouri National Guard has called for a criminal investigation after it learned that the personal information of as many as 2,000 soldiers had been breached. The Guard would not release how the personal information had been taken -- whether by computer hackers or other means -- because it has asked for a full law enforcement investigation into the matter.

Information
Source:
Dataloss DB

July 15, 2008
University of Texas, Austin
Austin, Texas

EDU  DISC  2,500

The personal information of University of Texas students and faculty has been exposed on the Internet. An independent watchdog discovered more than five dozen files containing confidential graduate applications, test scores, and Social Security numbers. The files were inadvertently posted by at least four different UT professors to a file server for the School of Biological Sciences.

Information
Source:
Dataloss DB

July 14, 2008
Washington Metropolitan Area Transit Authority
Washington, District Of Columbia

GOV  DISC  4,700

Metro accidentally published the Social Security numbers of past and present employees on its Web site. The numbers were posted with a solicitation to companies for workers’ compensation and risk management services.

Information
Source:
Dataloss DB

July 10, 2008
Williamson County (TN) Schools
Franklin, Tennessee

EDU  DISC  5,100

Social Security numbers and other personal information of 4,000 children were posted on the Internet.

UPDATE 7/11/08 : 5, 100 students’ information may be compromised.

Information
Source:
Dataloss DB

July 9, 2008
Wichita Radiological Group
Wichita, Kansas

MED  INSD  Unknown

A former employee stole patient records before being fired from the Wichita Radiological Group. Tens of thousands of patient records were in the database could have been compromised.

Information
Source:
Media

July 9, 2008
Wagner Resource Group
McLean, Virginia

BSF  DISC  2,000

Sometime late last year, an employee of a McLean investment firm used the online file-sharing network LimeWire. In doing so, he inadvertently opened the private files of his firm to the public. That exposed the names, dates of birth and Social Security numbers of about 2,000 of the firm’s clients, including a number of high-powered lawyers and Supreme Court Justice Stephen G. Breyer.

Information
Source:
Dataloss DB

July 9, 2008
Division of Motor Vehicles Colorado
, Colorado

GOV  DISC  3.4 million

The DMV regularly sends large batches of personal information over the Internet without encryption and has failed to properly limit access to its database, according to a recent audit. At one point, 33 former DMV employees could access names, addresses, dates of birth and Social Security numbers.
Hackers obtained clients' unencrypted names, addresses and Social Security numbers from July 17, 2007, to February 15, 2008. They compromised the logon passwords of 14 financial advisers and four assistants.

**UPDATE** (9/11/08) : The U.S. Securities & Exchange Commission (SEC) fined LPL $275,000 and required that LPL strengthen its security safeguards involving customer information. It was found that the hacker(s) placed, or attempted to place, 209 unauthorized trades in 68 customer accounts of several of LPL's registered representative, for more than $700,000 in trades in securities of 19 different companies. LPL reversed or eliminated the trades and compensated the customers for the resulting trading losses, which totaled approximately $98,900.

A computer flaw in the Organ and Tissue Donor Registry database may have exposed thousands of donors' personal information, including their Social Security numbers. Other data included donors' names, addresses, birth dates and drivers' license numbers.

A laptop computer that was reported stolen from an Army employee's truck contained personal information on Fort Lewis soldiers. A 500 GB removable hard drive was also taken in the theft.

**UPDATE** (7/11/08) : A 17-year-old Lacey boy faces a charge of suspicion of possession of stolen property after Tumwater police uncovered items from vehicle prowls, including a stolen Army laptop containing information on Fort Lewis soldiers.

A contracted vendor released personal information on about 380 potential jurors to an employee's private e-mail address. The information provided to the e-mail account could have included names, addresses, Social Security numbers and birth dates.

Due to a breach by an unauthorized person in its information systems, there is a possibility that personal information, such as name, address, date of birth, Social Security number, and reason for coming to Baptist Health were compromised. Apparently, no information in the patients' medical records and no information about the patients' diagnoses or prognoses was accessed. A former employee was arrested for attempting to open a credit account at a retail merchant.

Officials at the University of Nebraska at Kearney discovered a security breach involving nine university computers. Of the nine computers involved, five contained names and partial or complete Social Security numbers.
Hackers extracted information from an online database that held credit card account information.

Information Source: Dataloss DB

June 26, 2008  Texas Department of Public Safety
Austin, Texas

The personal information of 826 state employees was stolen from a Wichita Falls home office. Notices are in the mail to inform the hundreds of victims that their names, home addresses, dates of birth, driver's license and Social Security numbers are in the hands of criminals.

Information Source: Dataloss DB

June 26, 2008  IGN Entertainment
Brisbane, California

A computer was stolen in an unspecified location on May 25 of 2008. The computer contained employee names, addresses, dates of birth, Social Security numbers, and dependent information.

Information Source: Dataloss DB

June 24, 2008  Southeast Missouri State University
Cape Girardeau, Missouri

(573) 986-6800, (573) 335-6611, ex.123, lbavolek@semissourian.com

A former employee has been indicted on two charges of identity fraud and one charge of computer trespass after being found in possession of 800 student names and Social Security numbers.

Information Source: Dataloss DB

June 23, 2008  Colt Express Outsourcing Services, CNET Networks
Walnut Creek, California

Burglars stole computer systems from the offices of the company that administers the Internet publisher's benefit plans. The computers contained names, birth dates, Social Security numbers and employment information of the beneficiaries of CNET's health insurance plans. CNET was only one of several clients affected.

UPDATE (8/26/08): Among the companies whose staffers have been exposed by the Colt break-in in Walnut Creek, California: Google, Bebe Stores, Alston & Bird, and the California Bankers Assn.

Information Source: Dataloss DB

June 23, 2008  Bank Atlantic
Tampa, Florida

Bank Atlantic confirms they had a data loss, involving their MasterCard debit cards. It happened through a local merchant, but at this time, isn't saying which one.

Information Source: Media

June 19, 2008  Citibank
New York, New York

A Citibank server that processes ATM withdrawals at 7-Eleven convenience stores has been breached. The breach of the Citibank server allowed two Brooklyn men to make hundreds of fraudulent withdrawals from New York City cash machines and pocket at least $750,000 in cash.

Information Source: Dataloss DB

June 19, 2008  Petroleum Wholesale
Houston, Texas

The company dumped hundreds of records in a publicly accessible trash container outside its former headquarters. The records included receipts with customers' names and full credit or debit card numbers, including expiration dates. The records also included returned checks and forms containing customers' names and bank routing, driver's license and Social Security numbers.

Information Source: Media
June 19, 2008

**Aon Consulting**

*Chicago, Illinois*

BSF  PORT  57,160

Verizon Inc. applicants were affected.

A laptop used to collect pre-employment screening information for Verizon Inc. employees was stolen from a restaurant in May of 2008. The personal information included names and Social Security numbers.

**Information Source:** Dataloss DB

June 18, 2008

**Domino's Pizza**

*Tucson, Arizona*

BSR  PHYS  Unknown

Investigators found credit card numbers blowing in the wind. These piles and papers contained hundreds of old receipts from Domino's Pizza stores. The former owner had been discarding boxes of old records and somehow all those receipts got loose.

**Information Source:** Media

June 15, 2008

**Connecticut Department of Administrative Services**

*Hartford, Connecticut*

GOV  DISC  Unknown

Department of Administrative Services posted the Social Security numbers of individual contractors on a state Web site. An audit also uncovered the Social Security numbers of prospective nursing employees accessible on an agency Web site for 19 months until a complaint was lodged.

**Information Source:** Media

June 13, 2008

**Texas Insurance Claims Services**

*Dallas, Texas*

BSF  PHYS  Unknown

Hundreds of files with people's names, Social Security numbers and policy numbers were found in a Richardson dumpster, apparently discarded by Texas Insurance Claims Services.

**Information Source:** Dataloss DB

June 12, 2008

**Columbia University**

*New York, New York*

EDU  DISC  5,000

Social Security numbers of some 5,000 Columbians were accidentally posted by a student employee on a Google-hosted site in February 2007. Student Services discovered the leak in June 2008 and removed the sensitive data after it had been available for 16 months.

**Information Source:** Dataloss DB

June 11, 2008

**Dickson County Board of Education**

*Dickson, Tennessee*

EDU  PORT  850

A computer containing sensitive personal information was stolen from the Dickson County Board of Education. The computer belongs to the new director of schools and was loaded with the name and Social Security number of every school employee from the 2006-2007 school year, a total of 850.

**Information Source:** Dataloss DB

June 10, 2008

**1st Source Bank**

*South Bend, Indiana*

BSF  HACK  Unknown

1st Source Bank is replacing ATM cards this month for all its account holders after cyber-thieves accessed an unknown amount of debit-related data.

**Information Source:** Dataloss DB

June 10, 2008

**University of Utah Hospitals and Clinics**

*Salt Lake City, Utah*

MED  PORT  2.2 million

Billing records of 2.2 million patients at the University of Utah Hospitals and Clinics were stolen from a vehicle after a
courier failed to immediately take the eight data tapes to a storage center. The records, contained Social Security numbers of 1.3 million people treated at the university over the last 16 years.

**UPDATE (2/5/09):** The data tapes were found within a month after being stolen.

**UPDATE (6/9/10):** An Englewood, Colo., insurance company has filed a federal lawsuit contending that it isn’t responsible for reimbursing the University of Utah for $3.3 million in costs related to a 2008 data breach caused by a third-party service provider.

The lawsuit filed in a Utah federal court by Colorado Casualty Insurance Co. contends that the insurer is not obligated to cover the costs sought by the University. Colorado Casualty was providing breach insurance to the University at the time of the breach.

The nine-page complaint, which seeks a declaratory judgment from the court, offers little explanation as to why exactly the insurer believes it is not obligated to pay the breach-related costs sought by the University.

http://www.computerworld.com/s/article/9177702/Insurer_says_it_s_not LIABLE_for_University_of_Utah_s_3.3M_data_breach

---

**Information Source:** Dataloss DB

**June 10, 2008**

**University of Florida**

Gainesville, Florida

EDU DISC 11,300

Current and former students had their Social Security numbers, names and addresses accidentally posted online. The information became available when former student employees of the Office for Academic Support and Institutional Service, or OASIS, program created online records of students participating in the program between 2003 and 2005.

**Information Source:** Media

**June 10, 2008**

**Wheeler's Moving Company**

Boca Raton, Florida

BSO PHYS Unknown

Personal files with tax information, Social Security numbers and license numbers, were found in a Boca Raton dumpster.

**Information Source:** Media

**June 9, 2008**

**University of South Carolina**

Columbia, South Carolina

EDU STAT 7,000

Several items were stolen from an office in the Moore School of Business. Among the items was a desktop computer. As a result of the computer being stolen, it is possible that some personally identifiable data could have been compromised.

**Information Source:** Media

**June 7, 2008**

**Soutthington Water Department**

Soutthington, Connecticut

GOV PHYS 26

Documents with the names and Social Security numbers of 26 people were found scattered by the Quinnipiac River.

**Information Source:** Media

**June 7, 2008**

**East Tennessee State University**

Johnson City, Tennessee

EDU STAT 6,200

6,200 people may have had their identities compromised by the theft of a desktop computer. The computer is password protected and files cannot be easily accessed. But there is a small possibility that the information could be compromised.

**Information Source:** Dataloss DB

**June 6, 2008**

**Stanford University**

Stanford, California

EDU PORT 72,000

 Stanford University determined that a university laptop, which was recently stolen, contained confidential personnel data. The university is not disclosing details about the theft as an investigation is under way.

**Information Source:** Dataloss DB

**June 4, 2008**

**Oregon State University**

Corvallis, Oregon

EDU HACK 4,700
The Oregon State Police are investigating the theft of personal information from online customers of the OSU Bookstore who used credit cards to purchase items.

Information
Source: Dataloss DB

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Industry</th>
<th>Type</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 2, 2008</td>
<td><strong>Walter Reed Army Medical Center</strong>&lt;br&gt;Washington, District Of Columbia</td>
<td>MED UNKN</td>
<td>1,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(877) 854-8542, ext. 9</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Sensitive information on patients at Walter Reed Army Medical Center and other military hospitals was exposed in a security breach. The computer file was found on a "non-government, non-secure computer network." The data file did not include information such as medical records, or the diagnosis or prognosis for patients, but may have included names, Social Security numbers, birth dates as well as other information.

Information
Source: Dataloss DB

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Industry</th>
<th>Type</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 2, 2008</td>
<td><strong>Connecticut Department of Labor</strong>&lt;br&gt;Wethersfield, Connecticut</td>
<td>GOV PHYS</td>
<td>2,100</td>
<td></td>
</tr>
</tbody>
</table>

Records with confidential information on about 2,100 people have been lost and might have been mistakenly shredded. The files contained copies of letters informing applicants that they were ineligible for the unemployment insurance. They were dated between May 2 and May 20 and contained names, addresses and Social Security numbers.

Information
Source: Dataloss DB

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Industry</th>
<th>Type</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 31, 2008</td>
<td><strong>Pocono Mountain School District</strong>&lt;br&gt;Swiftwater, Pennsylvania</td>
<td>EDU HACK</td>
<td>11,000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(570) 873-7121, ext. 10151</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A hacker apparently broke into the computers at Pocono Mountain School District and may have tapped into confidential information concerning students and their parents. Information may have included the students' birth dates, Social Security numbers, student IDs, home phones, and the parents' names, phone numbers and emergency phone numbers. "If you see any unauthorized activity, promptly contact your service provider and or the office of the director of technology at 570-873-7121, ext. 10151.''

Information
Source: Dataloss DB

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Industry</th>
<th>Type</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 30, 2008</td>
<td><strong>Circuit Court of Louisville</strong>&lt;br&gt;Louisville, Kentucky</td>
<td>GOV PHYS</td>
<td>312</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(502) 595-3273</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Louisville Metro Police made an arrest, and during that arrest they found 312 stolen court traffic files in that person's possession. All of the files contain personal information of people in Louisville such as, name, address, date of birth and in some cases Social Security numbers and copies of drivers' licenses.

Information
Source: Media

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Industry</th>
<th>Type</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 29, 2008</td>
<td><strong>State Street Corp, Investors Financial Services</strong>&lt;br&gt;Boston, Massachusetts</td>
<td>BSF STAT</td>
<td>45,500</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(415) 353-7427</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Computer equipment containing personal information on customers and employees of a State Street unit was stolen. The computer equipment was stolen from a vendor hired by Investors Financial Services to provide legal support services. The personal information included names, addresses and Social Security numbers.

Information
Source: Dataloss DB

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Industry</th>
<th>Type</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 28, 2008</td>
<td><strong>University of California, San Francisco</strong>&lt;br&gt;San Francisco, California</td>
<td>EDU HACK</td>
<td>3,569</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(415) 353-7427, <a href="mailto:PathHotline@ucsf.edu">PathHotline@ucsf.edu</a></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

During routine monitoring of a campus computer network, UCSF discovered unusual data traffic on one of its computers. During the investigation, UCSF determined that an unauthorized movie-sharing program had been installed on one computer by an unknown individual. Installation of this program required high-level system access. The computer contained files with lists of patients from the UCSF pathology department's database. The data included information such as patient names, dates of pathology service, health information and, in some cases, Social Security numbers.
May 23, 2008

R.E. Moulton
Irving, Texas

Thieves broke into the Irving, Texas, regional office and stole a laptop computer containing personally information of numerous individuals, including names and Social Security numbers. The company is in the medical stop-loss insurance industry.

Information Source:
Dataloss DB

BSF PORT 19,000 records from this breach used in our total: 19,000

May 22, 2008

HealthSpring Inc.
Franklin, Tennessee

A laptop computer containing personal information of about 450 state residents was stolen. The laptop, believed to contain names, dates of birth and Social Security numbers of about 9,000 individuals, was stolen from a HealthSpring employee's locked car.

Information Source:
Dataloss DB

MED PORT 9,000 records from this breach used in our total: 9,000

May 22, 2008

AT&T
San Antonio, Texas

A laptop was stolen from the car of an employee. The data on the computer was not encrypted -- a violation of company policy -- and included names, Social Security numbers and in some cases, salary and bonus information.

Information Source:
Security Breach Letter

BSO PORT Unknown records from this breach used in our total: 0

May 21, 2008

Oklahoma Corporation Commission
Oklahoma City, Oklahoma

The Oklahoma Corporation Commission is removing hard drives from all surplus computer equipment after a server containing the names and Social Security numbers of thousands of residents was sold at an auction.

Information Source:
Media

GOV STAT 5,000 records from this breach used in our total: 5,000

May 20, 2008

University of Florida College of Medicine
Jacksonville, Florida

(866) 876-4472

A UF assistant professor of plastic surgery at the UF College of Medicine-Jacksonville, stored unsecured digital photographs of his patients and identifying information on a computer. He then gave the computer to a family. The information included names, dates of birth, Social Security numbers, and Medicare numbers.

Information Source:
Dataloss DB

MED INSD 1,900 records from this breach used in our total: 1,900

May 20, 2008

New York University
New York, New York

Duke University's Fuqua School of Business is notifying former New York University students that some of their personal information was inadvertently accessible by targeted Internet searches. The personal data included names and Social Security numbers and was contained in the faculty member's research records. The information could have been accessed only if searched by specific student names, along with a search code for Social Security numbers.

Information Source:
Dataloss DB

EDU DISC 273 records from this breach used in our total: 273

May 17, 2008

University of Louisville
Louisville, Kentucky

Documents being copied and taken from a private office in the president's office, to its Internal Audit Office and Department of Public Safety may have resulted in a security breach. The documents contained personal information - including Social Security numbers, student and employee identification numbers and salary information - for current and recent student employees. The university learned of the theft when salary information was shared anonymously with some employees in the office.

Information Source:
Dataloss DB

EDU PHYS 20 records from this breach used in our total: 20

621
A laptop computer containing the personal information of students was stolen from an employee's car. The car burglars made off with her school laptop and an external flash drive. The flash drive contains students' Social Security numbers, personal information, schools those students attend, as well as their grade level and birthdates. The drive also contained the Texas Assessment of Knowledge and Skills test results.

Information
Source: Dataloss DB
records from this breach used in our total: 8,000

Index cards containing patients personal information, names, dates of birth, even Social Security numbers are gone. Hundreds of records have simply disappeared.

Information
Source: Dataloss DB
records from this breach used in our total: 0

Boxes filled with personal information were found in a dumpster. Information on athletes and their guardians included Social Security numbers and copies of birth certificates.

Information
Source: Dataloss DB
records from this breach used in our total: 0

A 15-year-old student gained access to files on a computer at Downingtown West High School. Private information, including names, addresses and Social Security numbers, of more than 50,000 people were accessed. The student apparently used a flash drive to save the personal data of about 40,000 taxpayers and 15,000 students.

Information
Source: Media
records from this breach used in our total: 55,000

A BB&T Insurance laptop containing the personnel information of some Harrisonburg City Schools employees was stolen. The laptop, used by an outside sales representative to develop an insurance proposal for the school system, was stolen from a car. The information contained names, dates of birth, Social Security numbers, and, in some cases, medical history.

Information
Source: Dataloss DB
records from this breach used in our total: 0

A breach in an Oklahoma State University computer server exposed names, addresses and Social Security numbers of students, staff and faculty who bought parking and transit services permits in the past six years.

Information
Source: Dataloss DB
records from this breach used in our total: 70,000

Three men have been charged with hacking into 11 Dave & Buster's networks and then remotely installing "packet sniffer" software on point-of-sale servers at locations throughout the U.S. A packet sniffer logs information being sent over a network. In this case, the criminals used it to log credit and payment card data as it was sent from the branch locations to corporate headquarters. The hacking took place from April to September 2007. At Dave & Buster's Islandia, New York, location, the hackers accessed details of about 5,000 payment cards. The information was sold to other criminals who then used the card numbers to scam online merchants. The criminals were able to post at least $600,000 in fraudulent transactions from 675 cards taken from this one store.

UPDATE (04/05/2010): In reaching a settlement with Dave & Buster's, the FTC quietly and without fanfare introduced a new security standard, requiring the company to monitor and filter outbound Internet traffic to block the unauthorized export of sensitive information. The consent decree puts companies on notice that they may face FTC scrutiny and penalties if they fail to use data loss prevention software.

UPDATE (07/19/2012): A member of the hacking ring was sentenced to seven years in prison. Around 80,000 payment card numbers were taken from the 11 Dave & Buster's locations. It appears that the hacker was part of a larger conspiracy.
that last between 2005 and 2008 and affected Hannaford Bros., grocery chain, Heartland Payment Systems, TJX retail chain, BJ's Wholesale Club, OfficeMax, Boston Market, 7-Eleven, JCPenney, Barnes & Noble, Sports Authority, and Forever 21. Two other members of the hacking ring were sentenced to 20 years in prison and 30 years in prison.

**Information Source:**

Dataloss DB

---

**May 12, 2008**

**Pfizer**

**New York, New York**

BSO PORT

13,000 (No SSNs or financial information reported)

(866) 274-3891

About 13,000 employees at Pfizer Inc., including about 5,000 from Connecticut, had their personal information compromised when a company laptop and flash drive were stolen. No Social Security numbers were on the laptop, but names, home addresses, home telephone numbers, employee ID numbers, positions and salaries were possibly compromised. Other information possibly lost included the department employees worked in, the Pfizer site where the employees worked, the name of employees' managers and descriptions of their jobs.

**Information Source:**

Dataloss DB

---

**May 9, 2008**

**Princeton University Tower Club**

**Princeton, New Jersey**

EDU DISC

103

Tower Club is taking steps to protect 103 of its alumni in the classes of 2006 and 2007 after a spreadsheet listing their names and Social Security numbers was e-mailed to current club members. The document was attached to an apparently unrelated e-mail that informed current members about a club event. The spreadsheet was attached unintentionally because of a technical glitch in an email program.

**Information Source:**

Dataloss DB

---

**May 8, 2008**

**Dominican University**

**River Forest, Illinois**

EDU HACK

5,000

Two students were able to access records on a staff network storage area. The files accessed were three spreadsheets that included students' names, addresses, phone numbers, birthdays and Social Security numbers.

**Information Source:**

Dataloss DB

---

**May 8, 2008**

**Las Cruces Public Schools**

**Las Cruces, New Mexico**

EDU DISC

1,800

A part-time computer analyst for Las Cruces Public Schools inadvertently posted personal data for 50 special education students and 1,750 district employees on the Internet. Information posted included Social Security number, date of birth, name, the nature of disability and caseworker's name.

**Information Source:**

Dataloss DB

---

**May 7, 2008**

**SAIC**

**Maryland**

BSO PORT

4,690

The breach appears to have occurred somewhere in Maryland. Please call (877) 277-8001 for more information.

SAIC stockholders are at risk of identity theft after a box of magnetic backup tapes went missing. The tapes contained names, addresses, Social Security numbers, stock account information, transaction activity and possibly bank account numbers for current or former shareholders.

**Information Source:**

Media

---

**May 6, 2008**

**Ohio State University Agricultural Technical Institute**

**Wooster, Ohio**

EDU DISC

192

Personal information on faculty and staff members was accidentally emailed to about 680 students. The email contained spreadsheet information listing the names, positions, salaries and Social Security numbers.

**Information Source:**

Dataloss DB

---

**May 6, 2008**

**International Visa Service**

**Atlanta, Georgia**

BSO INSĐ

1,000
An employee has been arrested and charged with stealing the personal information of people who were applying for a passport and sold the identities on the black market.

Information Source: Dataloss DB  
May 6, 2008  
Northeast Security  
West Haven, Massachusetts  
BSO  PHYS  Unknown

News Channel 8 found Social Security numbers, bank account numbers and even canceled checks inside a dumpster. The files appear to belong to Northeast Security, a subcontractor for Safe Home Security, based out of Rocky Hill. Northeast Security recently moved out of a West Haven storefront, and it seems they left their clients personal information behind.

Information Source: Dataloss DB  
May 5, 2008  
Target America Inc., University of California, San Francisco (UCSF)  
San Francisco, California  
MED  DISC

Information on UCSF patients was accessible on the Internet. The information accessible online included names and addresses of patients along with names of the departments where medical care was provided. Some patient medical record numbers and the names of the patients' physicians also were available online.

Information Source: Dataloss DB  
May 5, 2008  
Iredell County Tax Administration  
Statesville, North Carolina  
GOV  PHYS  486

(704) 878-3020

A courier vehicle providing services for First Citizens Bank was stolen in Charlotte. The stolen shipment contained a computer report of taxpayer’s check information, including account numbers, check numbers, check amounts and routing numbers from various banks on which the checks were drawn. There were also copies of tax bills that contained taxpayer names, addresses and other public information related to tax payments.

Information Source: Dataloss DB  
May 4, 2008  
Staten Island University Hospital  
Staten Island, New York  
MED  STAT  88,000

Computer equipment stolen from an administrator contained personal information from patients. Social Security numbers and health insurance numbers were contained in computer files on a desktop computer and the backup hard drive.

Information Source: Dataloss DB  
May 2, 2008  
Marine Corps Reserve Center  
San Antonio, Texas  
GOV  INSD  17,000

A former U.S. military contractor has pleaded guilty to exceeding authorized access to a computer and aggravated identity theft after he was accused of selling names and Social Security numbers of 17,000 military employees.

Information Source: Media  
May 1, 2008  
Cove Creek Mortgage, Front Range Mortgage  
Englewood, Colorado  
BSF  PHYS  Unknown

Sensitive mortgage files with people’s personal information were recently found in a Dumpster. The files and computers contained sensitive information on many former customers of Front Range Mortgage, including names and addresses, Social Security numbers and bank, credit card and investment account information.

Information Source: Media  
May 1, 2008  
Lunardi’s Supermarket  
Los Gatos, California  
BSR  CARD  100, updated amount 250
An ATM and credit card reader in a checkout aisle at the Los Gatos Lunardi’s supermarket was recently switched, resulting in cases of identity theft. Victims all had their card numbers stolen after officials from Lunardi’s contacted them about a problem with one of their card readers.

**UPDATE (8/4/08):** Police arrested a man Friday that was involved with the ATM scam at a Los Gatos supermarket that lost about $300,000. He was booked into the Santa Clara County Jail in connection with burglary, conspiracy, drunken driving, and further charges may be filed later, according to the district attorney’s office.

**Information Source:**
Dataloss DB

**April 28, 2008**
**Hough, MacAdam & Wartnik**
**North Bend, Oregon**

A notebook computer was stolen from a locked vehicle. The notebook’s hard drive may have contained names, Social Security numbers, and other personal information.

**Information Source:**
Dataloss DB

**April 27, 2008**
**General Internal Medicine of Lancaster**
**East Hempfield Township, Pennsylvania**

A laptop was stolen from a doctors’ office containing the Social Security numbers of patients. The clinic is notifying 12,000 potential-affected patients.

**Information Source:**
Media

**April 25, 2008**
**University of Colorado, Boulder**
**Boulder, Colorado**

Three computers in the Division of Continuing Education and Professional Studies were compromised, leaving people open to potential identity theft. One of the three computers had personal data, including names, Social Security numbers, addresses and grades.

**UPDATE (5/1/08):** Upon further analysis, the University concluded that no personal data had been exposed. 9,500 records were initially thought to be comprised, but later this was revised to zero.

**Information Source:**
Dataloss DB

**April 25, 2008**
**Canton WiseBuys**
**Canton, New York**

Someone apparently hacked into the Canton WiseBuys store computer system during a changeover between December 5, 2007 and December 20, 2007. The hacker obtained personal identification and banking numbers of hundreds of customers.

**Information Source:**
Media

**April 25, 2008**
**Baltimore Highway Administration**
**Baltimore, Maryland**

An employee transferred personnel transaction data from a secure drive to a SHA shared drive. Sensitive personal information concerning employees, included names and Social Security numbers.

**Information Source:**
Dataloss DB

**April 24, 2008**
**Harmony Information Systems**
**Madison, Wisconsin**

A computer program housing personal information about Wisconsin seniors and disabled people had a significant security hole. A senior center volunteer in McFarland said he could see hundreds of files of people’s private information from across the country in the system run by Virginia-based Harmony Information Systems. The information is entered into an electronic record that includes the person’s name and Social Security number.

**Information Source:**
Media

**April 24, 2008**
**Collections Lawyers Pellegrino & Feldstein**
**Denville, New Jersey**
Consumer information somehow escaped the New Jersey law offices and ended up posted on several websites. The Liberty Coalition discovered cached versions of an Excel file that contained the full names, Social Security numbers, dates of birth, addresses, account numbers, and financial information.

**Information Source:** Dataloss DB

**April 23, 2008**

**University of Texas Health Science Center**

*Tyler, Texas*

MED DISC 2,000

About 2,000 medical bills were mailed last week with patients' Social Security numbers visible on the envelope.

**Information Source:** Dataloss DB

**April 23, 2008**

**Southern Connecticut State University**

*New Haven, Connecticut*

EDU HACK 11,000

Southern Connecticut State University is taking action to prevent its students from becoming victims of identity theft. The move comes after a website with student and alumni information was found to be easily accessible to hackers. It appears that no financial information was accessed but Social Security numbers were vulnerable.

**Information Source:** Dataloss DB

**April 22, 2008**

**LendingTree**

*Charlotte, North Carolina*

BSF INSD Unknown

Outside loan companies may have accessed information, including Social Security numbers, between October 2006 and early 2008 and used it to market their own mortgages to LendingTree customers. Several former employees may have shared confidential passwords with a handful of lenders that were not approved by the company.

**Information Source:** Media

**April 22, 2008**

**University of Massachusetts, Amherst**

*Amherst, Massachusetts*

MED HACK Unknown

Hackers breached the computer system used by UMass Amherst’s Health Services, potentially gaining access to thousands of medical records. More than half of the student population at UMass Amherst are patients on record at the University Health Services.

**Information Source:** Dataloss DB

**April 22, 2008**

**HealthNow New York**

*Buffalo, New York*

MED PORT Unknown

Clients may be at risk for identity theft, after a former employee's laptop computer went missing with confidential information several months ago. The potential information includes names, dates of birth, Social Security numbers, addresses, employer group names, and health insurance identifier numbers.

**Information Source:** Media

**April 22, 2008**

**Fishback Financial Corp.**

*Brookings, South Dakota*

BSF HACK Unknown

There has been an unauthorized access to one of the database servers by a third party. The database includes names, addresses and Social Security numbers.

**Information Source:** Dataloss DB

**April 22, 2008**

**Central New England HealthAlliance**

*Leominster, Massachusetts*

MED PORT 384

Personal data could be at risk of exposure after a home health nurse reported that her handheld computer was missing. The unencrypted data include names, Social Security numbers, and health insurance records.

**Information Source:** Media

**April 22, 2008**

**Smithtown Post Office**

*Smithtown, New York*

GOV INSD Unknown

626
A Smithtown postal worker was arrested after he stole credit cards from the mail and went on a shopping spree.

Information Source: Media
April 22, 2008 CollegInvest Denver, Colorado

Customers had personal information stored on a computer hard drive that disappeared during a recent move. CollegInvest moved to a new office space, using an international relocation firm that offered specialists in moving computer equipment. CollegInvest discovered while unpacking at the new location that a hard drive was missing. CollegInvest is a not-for-profit division of the Colorado Department of Higher Education.

Information Source: Dataloss DB
April 21, 2008 Brunswick Corp. Lake Forest, Illinois

An electronic device that scans customers' drivers' licenses to make sure they're of legal drinking age was stolen from a company-owned bowling facility in suburban Naperville. The device contains information such as driver's license number, date of birth and first and last names of customers whose licenses were scanned.

Information Source: Media
April 20, 2008 Helping Homeless Veterans and Families Hoosier Veterans Foundation Indianapolis, Indiana

Hundreds of files containing medical histories and Social Security numbers were found in the trash on Indianapolis' east side. The records belong to homeless veterans. A lot of the things inside the folders are confidential information about the clients including Social Security numbers.

Information Source: Media
April 19, 2008 Central Collection Bureau Indianapolis, Indiana

A computer server containing Social Security numbers and other personal information was stolen last month from a Southside debt-collection bureau. The information includes customer-billing records for Indiana businesses, including Citizens Gas & Coke Utility, St. Vincent Health and Methodist Medical Group.

Information Source: Dataloss DB
April 17, 2008 SunGard, Connecticut State University System, Buffalo State, Northwest Missouri State University

http://www.sungardhe.com/custom.aspx?id=1554&LangType=1033

At least 18 colleges are scrambling to inform tens of thousands of students they are at risk of having their identities stolen. A laptop computer that was stolen from a vendor contained the data of current and former students from the four state universities, including Western Connecticut State University. The computer was password-protected but contained unencrypted files with personally identifiable data, including names and Social Security numbers.

Information Source: Dataloss DB
April 17, 2008 University of Miami Miami, Florida

(866) 628-4492

Computer tapes containing confidential information of Miami patients was stolen last month when thieves took a case out of a van used by a private off-site storage company. The data included names, addresses, Social Security numbers or health information.

Information Source: Dataloss DB
April 16, 2008 Hexter Elementary School Dallas, Texas

Employee and volunteer records were found at a recycling bin near the school. It's unknow what type of documents were found.
April 16, 2008  
**University of Virginia**  
Charlottesville, Virginia  
EDU  PORT  7,000  

A laptop stolen from a University of Virginia employee contained sensitive information about students, staff and faculty members. Stolen from an unidentified employee from an undisclosed location in Albemarle County, the laptop contained a confidential file filled with names and Social Security numbers.

April 15, 2008  
**First Federal Bank of California**  
Los Angeles, California  
BSF  UNKN  Unknown  

Additional locations: Brookfield, WI (headquarters of Fiserv, Inc)

This bank was not the only financial institute impacted by a security breach that occurred in a banking in a subsystem of a financial data processor, Fiserv, Inc. of Wisconsin last month. The bank said that it was company policy not to reveal any details about the breach including the number of banks involved, how many customers were impacted, the depth of information breached, how extensive the breach was geographically even which federal agencies were involved. However, non-public private account information might be at risk.

April 15, 2008  
**Oklahoma's Department of Corrections**  
Oklahoma City, Oklahoma  
GOV  DISC  10,597  

The names, addresses, and Social Security numbers of tens of thousands of Oklahoma residents were made available to the general public for a period of at least three years on the ODC's website.

April 14, 2008  
**Stokes County High Schools**  
Danbury, North Carolina  
EDU  STAT  800  

A school computer containing the names, test scores and Social Security numbers of students from three Stokes County high schools was stolen from a locked closet.

April 14, 2008  
**Utah Department of Workforce Services**  
Salt Lake City, Utah  
GOV  INSD  Unknown  

A former state employee who took applications from people seeking food stamps and other welfare aid worked with three others to steal the identity of Utah residents and charge tens of thousands of dollars in purchases.

April 13, 2008  
**University of Toledo**  
Toledo, Ohio  
EDU  DISC  6,488  

Personal information of the University of Toledo employees, the majority having worked on the Health Science Campus in 1993 and 1999 - last month was inadvertently placed on a server to which all employees had access. The information, which was used for payroll purposes, included names, addresses, and Social Security numbers and was accessible for about 24 hours.

April 12, 2008  
**Allied Waste**  
Boston, Massachusetts  
BSO  PHYS  Unknown  

A strap on a garage truck snapped and sent reams of intact financial reports over downtown Boston streets.

April 12, 2008  
**West Seneca School District**  
West Seneca, New York  
EDU  HACK  1,800

628
Several current and former students are believed to have broken into the school district’s computer system and copied secure files that included the personal information and Social Security numbers of school employees.

Information
Source: Dataloss DB
April 11, 2008
New York-Presbyterian Hospital, Weill Cornell Medical Center
New York, New York
MED INSD 49,841

An admissions employee is accused of selling 2,000 patients’ data in an identity theft scheme and accessing nearly 50,000 records illegitimately. Records contained names, phone numbers and, in some cases, Social Security numbers of patients. The employee has since been charged with one count of conspiracy involving computer fraud, identity document fraud, transmission of stolen property and sale of stolen property.

Information
Source: Dataloss DB
April 10, 2008
Joliet West High School
Joliet, Illinois
EDU HACK Unknown

A student using a school computer last month was able to access personal information about every student enrolled. The student allegedly downloaded a list of names and Social Security numbers to his iPod.

Information
Source: Dataloss DB
April 9, 2008
People’s United Bank
Bridgeport, Connecticut
BSF PHYS Unknown

For four months, a dumpster diver searched through trash bins outside People’s United Bank branches in Fairfield County. He pulled out bags of paperwork with private information, including customers’ Social Security numbers and account information.

UPDATE (5/1/08): The man who discovered bank records in the garbage outside local branches of People’s United Bank in Connecticut has been sued to prevent him from informing people about the discovery. The man, discovered financial documents, including customer names, Social Security numbers, and account information. He was a no-show at a scheduled appearance in court. The bank won a restraining order against the man, which ordered him not to talk to bank customers, or disclose what he had discovered. He disregarded the order and made a documentary about the discovery. The man has already been fined $800 USD for refusing to hold his tongue, and now he has also been ordered to pay the bank’s legal costs. According to the Connecticut Post, those costs are already up to around $40,000 USD.

Information
Source: Media
April 9, 2008
Norfolk’s Community Services Board
Norfolk, Virginia
NGO PHYS 30

The personal information of clients of Norfolk’s Community Services Board was compromised when a case worker’s briefcase was stolen. The briefcase was left in the worker’s car in a Virginia Beach parking garage, but someone smashed a window and stole it. It’s unclear what information was in the files but that it likely included Social Security numbers.

Information
Source: Media
April 8, 2008
WellPoint
Indianapolis, Indiana
BSO DISC 128,000

Personal information that may have included Social Security numbers and pharmacy or medical data for customers in several states was exposed online over the past year.

Information
Source: Dataloss DB
April 8, 2008
WellCare Health Plans Inc.
Atlanta, Georgia
MED DISC 71,000

Private records of members of health insurance programs for the poor or working poor were accidentally made available online for several days. Those whose data was made available on the Internet included members of Medicaid, the federal health program for the poor, and PeachCare for Kids, a federal-state insurance plan for children of the working poor. About 10,500 members’ Social Security numbers may have been viewed by unauthorized people on the Internet, all members of Medicaid or PeachCare. There is a possibility that an initial 59,000 members may have had some personal information made accessible.
April 7, 2008  Pfizer Inc  New York, New York  BSO  PORT  800

A laptop was stolen by a burglar from the home of a contractor who helps arrange planning travel and meetings for Pfizer. Information on the laptop included names, credit card numbers and, in some instances, credit card expiration dates, various addresses and phone numbers, hotel loyalty program numbers and other information. It did not appear that any Social Security numbers or PIN codes were exposed.

Information Source: Dataloss DB

April 7, 2008  Army Acquisition Support Center  Ft. Belvoir, Virginia  GOV  DISC  24

A spreadsheet containing a hidden column of Social Security numbers belonging to about two dozen officers and civilian employees of one Army agency was left on the agency’s website for five months after being notified of the presence of the personal information. The center has temporarily shut down its website to scrub the information from the spreadsheet.

Information Source: Media

April 7, 2008  Redbox  Oakbrook Terrace, Illinois  BSR  CARD  Unknown

Redbox rents DVD movies via vending machine in drugstores and supermarkets throughout the country. They announced that they’d found credit card skimmers attached to three of their kiosks.

Information Source: Media

April 4, 2008  Harley-Davidson, Inc. (HOG)  Milwaukee, Wisconsin  BSO  PORT  60,000

A laptop computer containing certain HOG members’ personal information was determined to be missing from their facilities. The personal information stored on the computer included names, addresses, credit card numbers, their expiration dates, and driver's license numbers.

Information Source: Media

April 4, 2008  University of California, Irvine  Irvine, California  EDU  UNKN  7,000

7,000 current or former graduate students could be at risk of identity thieves who already used stolen data to file fake tax returns for 93 students. UCI does not know how the information was stolen or who is using it.

UPDATE (10/22/10): A class action lawsuit against United Healthcare Services was settled. UCI graduate students were affected by a fraudulent tax return scheme after an employee of United Healthcare Services misused their information to file fraudulent tax returns.

Information Source: Dataloss DB

April 1, 2008  Okemo Mountain Resort  Ludlow, Vermont  BSO  HACK  28,168

(866) 756-5366

The Ludlow ski area announced that its computer network was breached by an intruder who gained access to credit card data including cardholder names, account numbers and expiration dates.

Information Source: Dataloss DB

March 31, 2008  Advance Auto Parts  Roanoke, Virginia  BSR  HACK  56,000

The retailer reported that a network intrusion had exposed financial information and was the subject of a criminal investigation. Fourteen of the retailer’s stores, including locations in Georgia, Ohio, Louisiana, Tennessee, Mississippi, Indiana, Virginia and New York, are believed to have been affected.

Information Source: Dataloss DB

March 29, 2008  Department of Human Resources  Atlanta, Georgia  GOV  PORT  Unknown
A thief has stolen computer records containing identifying information on current and former employees of the state Department of Human Resources, including names, Social Security numbers, birth dates and home contact information. An external hard drive that stored a database was removed by an unauthorized person.

Information
Source: Dataloss DB
March 29, 2008 San Quentin State Prison
San Quentin, California
GOV PORT 3,500

A flash memory drive containing names, birth dates and driver’s license numbers of people who either volunteered or visited San Quentin State Prison in a group tour has been lost.

Information
Source: Media
March 28, 2008 Antioch University
Yellow Springs, Ohio
EDU HACK 70,000

A computer system that contained personal information on about 70,000 people was breached by an unauthorized intruder three times. The system contained the names, Social Security numbers, academic records and payroll documents for current and former students, applicants and employees.

Information
Source: Dataloss DB
March 28, 2008 Museum of Science, Boston
Boston, Massachusetts
NGO DISC 140

The museum has notified 140 patrons that their names, credit card numbers, and other personal information were exposed on the museum’s website because of a contractor’s error.

Information
Source: Dataloss DB
March 26, 2008 Presbyterian Intercommunity Hospital
Whittier, California
MED STAT 5,000

About 5,000 past and current employees at Presbyterian Intercommunity Hospital had their private information stolen. The data included Social Security numbers, birth dates, full names and other records stored on a desktop computer that was stolen.

Information
Source: Media
March 26, 2008 Broward School District
Coconut Creek, Florida
EDU HACK 38,000

An Atlantic Technical High School senior hacked into a district computer and collected Social Security numbers and addresses of district employees.

Information
Source: Dataloss DB
March 26, 2008 Bank of New York Mellon
Pittsburgh, Pennsylvania
BSF PORT 4.5 million customer records, raised to 12.5 million

(877) 278-3451, (877) 278-346, www.bnymellon.com/tapequery

The company lost a box of computer data tapes storing personal information including names, Social Security numbers and possibly bank account numbers.

UPDATE (5/07/08): On February 27, Bank of New York Mellon gave the unencrypted backup tape containing information on about 4.5 million consumers -- hundreds of thousands of them People’s United Bank customers and investors -- and nine other tapes to a storage firm, Archive Systems, Inc., for transportation to a storage facility. When the storage company vehicle arrived at the storage facility, the tape was missing. The other nine tapes reached the facility safely.

UPDATE (5/31/08): The Hartford Courant reports the following figures regarding the number of Connecticut shareholders affected by the lost computer tape: 403,894 People’s United Bank 33,586 John Hancock Financial 18,361 Walt Disney Co. 10,000 the remaining shareholders

UPDATE (8/30/08): The estimated number of people affected by a data breach at Bank of New York Mellon Corp has been raised from 4.5 million to 12.5 million.
UPDATE (2/19/09): The Bank of New York Mellon will pay Connecticut $150,000 as part of a settlement. The bank will continue to provide those affected by the breach with credit monitoring and fraud alerts for a total of 36 months of protection. It will also reimburse anyone for funds stolen from their accounts as a direct result of the data breach.

Information Source: Media

March 24, 2008 National Institutes of Health
Bethesda, Maryland

A laptop was stolen from the trunk of a car. It contained information about heart disease patients, including their names, dates of birth and diagnoses of their medical conditions.

UPDATE (4/14/08): Ongoing review of the computer’s last-known contents, performed on data backed up from the laptop before it was stolen, has found a file that, unbeknownst to the lead researcher, had been loaded onto the laptop by a research associate. That file included Social Security numbers for at least 1,281 of the 3,078 patients enrolled in the multi-year study, which is sponsored by the NIH’s National Heart, Lung and Blood Institute.

Information Source: Dataloss DB

March 22, 2008 Agilent Technologies
Santa Clara, California

A laptop containing sensitive and unencrypted personal data on current and former employees of Agilent Technologies was stolen from the car of an Agilent vendor. The data includes employee names, Social Security numbers, home addresses and details of stock options and other stock-related awards. Agilent blamed the San Jose vendor, Stock & Option Solutions, for failing to scramble or otherwise safeguard the data - in violation of the contracted agreement.

Information Source: Dataloss DB

March 22, 2008 Western Carolina University
Cullowhee, North Carolina

Someone had hacked into a computer server and had access to the Social Security numbers of 555 graduates of the university who had signed up for a newsletter.

Information Source: Dataloss DB

March 21, 2008 Compass Bank
Birmingham, Alabama

A database containing names, account numbers and customer passwords was stolen. A credit-card encoder and software to encode the information onto blank cards was also used to acquire information from ATMs. A former programmer at Birmingham, Ala.-based Compass Bank stole a hard drive containing 1 million customer records and used some of that information to commit debit-card fraud. The thief had used the information stolen from Compass Bank’s database to create about 250 counterfeit debit cards. He was able to use about 45 of those cards to access and withdraw cash from customer accounts at the bank before he was arrested.

Information Source: Dataloss DB

March 21, 2008 Rhode Island Department of Administration
Cranston, Rhode Island

A state computer disk containing Social Security numbers is missing. The information was discovered missing within the last two weeks when human resources staff members who had relocated from Providence to Cranston could not find the data on the server.

Information Source: Dataloss DB

March 20, 2008 Rampage Marketing Services
Columbus, Ohio

The company, a licensed insurance agency, threw 14 boxes of files containing sensitive financial and medical information into a trash bin. An insurance agent for another company noticed the boxes in the shared bin and sent them back to the Insurance Department.

Information Source: Media

March 20, 2008 Pennsylvania Department of State
Harrisburg, Pennsylvania

The company, a licensed insurance agency, threw 14 boxes of files containing sensitive financial and medical information into a trash bin. An insurance agent for another company noticed the boxes in the shared bin and sent them back to the Insurance Department.
The state was forced to pull the plug on a voter registration Web site after it was found to be exposing sensitive data about voters. Because of a Web programming error, the Web site was allowing anyone on the Internet to view data such as the voter’s name, date of birth, driver’s license number, and political party affiliation. On some forms, the last four digits of Social Security numbers could also be seen.

Information Source: Media

March 20, 2008

Lasell College
Newton, Massachusetts

EDU HACK 20,000

A hacker accessed data containing personal information on current and former students, faculty, staff and alumni. Information included names and Social Security numbers.

Information Source: Dataloss DB

March 19, 2008

Affordable Realty
Flint, Michigan

BSO PHYS Unknown

Social Security numbers and financial records of customers. Affordable Realty occupied office space inside the Ben Agree building on Dort Highway for years. The company was evicted and all of its sensitive customer information ended up outside in a dumpster or on the ground nearby.

Information Source: Dataloss DB

March 19, 2008

The Dental Network
Baltimore, Maryland

MED DISC 74,256

A security breach of The Dental Network website left access to member personal data, including names, Social Security numbers, addresses and dates of birth unprotected for approximately two weeks. The Dental Network is an independent licensee of the Blue Cross and Blue Shield Association.

Information Source: Dataloss DB

March 19, 2008

UCLA Medical Center
Los Angeles, California

MED INSD 900

UCLA Medical Center has moved to fire 13 employees and suspended six others for unauthorized access to confidential medical records.

UPDATE (8/5/08): The latest report said 127 workers peeked into celebrities’ medical records without permission, leading to several firings, suspensions and warnings. The report also detailed the case of one employee who looked at the records of about 900 patients without any legitimate reason and viewed Social Security numbers, health insurance information and addresses, from April 2003 to May 2007.

Information Source: Dataloss DB

March 17, 2008

Hannaford Bros. Supermarket chain
Portland, Maine

BSF HACK 4.2 million

This security breach affects all of its 165 stores in the Northeast, 106 Sweetbay stores in Florida and a smaller number of independent groceries that sell Hannaford products. The company is currently aware of about 1,800 cases of reported fraud related to the security breach. Credit and debit card numbers were stolen during the card authorization transmission process. It’s unclear if personal information was exposed.


UPDATE (5/14/2009): A federal appeals court has revived a Tampa class-action suit seeking money for Florida shoppers whose credit and debit card numbers were swiped in a data breach that hit 109 Sweetbay Supermarkets. The suit seeks free credit monitoring, credit repair if necessary and undetermined money damages to be split up among victims of the breach, including those unaware they were victims.

UPDATE (5/22/2009): A Maine U.S. District Court dismissed most of a class action lawsuit against Hannaford, finding that there is no way to value the time and effort that consumers spent in correcting fraudulent activity resulting from the breach. The case of one named plaintiff was not dismissed. That plaintiff suffered actual monetary damages for unreimbursed fraudulent charges.


UPDATE (3/29/2013): A United States District Court for the District of Maine has denied a motion that would have allowed a lawsuit to proceed as a class action. The plaintiffs originally moved to certify the proposed class on September 4, 2012. http://tinyurl.com/bsg9xpu

Information
Source: Dataloss DB
March 17, 2008
Binghamton University
Binghamton, New York
EDU DISC 300

A university employee mistakenly sent an e-mail attachment containing the names, grade point averages and Social Security numbers of junior and senior accounting students to another group of School of Management students.

Information
Source: Dataloss DB
March 15, 2008
Starling Insurance and Associates
Colorado Springs, Colorado
BSF PHYS Unknown

A server stolen from the locked offices contained names, addresses and Social Security numbers, dates of birth, driver's license numbers and/or account information for an unspecified number of customers.

Information
Source: Media
March 15, 2008
Utah Division of Finance
Salt Lake City, Utah
GOV HACK 500 - not included in total because it is unclear whether Social Security numbers or financial information was involved

Computer files containing the personal information of approximately 500 individuals may have been accessed by unauthorized persons during a security breach. An initial investigation indicates it is highly unlikely the person who breached the computer system was able to access any personal information.

Information
Source: Dataloss DB
March 13, 2008
University Health Care
Salt Lake City, Utah
MED PORT 4,800

A laptop and flash drive containing patient data were stolen after hours from a locked office. Data included patients' names, addresses, and in some cases, medications, health insurance policy numbers, and Social Security numbers.

Information
Source: Dataloss DB
March 12, 2008
Harvard University
Cambridge, Massachusetts
EDU HACK 6,600

Harvard Graduate School of Arts and Sciences (GSAS) Web server may have compromised 10,000 sets of personal information from applicants and students, including 6,600 Social Security numbers and 500 Harvard ID numbers.

Information
Source: Dataloss DB
March 10, 2008
Texas Department of Health and Human Services
Austin, Texas
MED STAT Unknown

Information, including Social Security numbers that could be used to steal Medicaid clients' identity may have been stored on two computers stolen during a burglary. Computers could have contained personal information only on e-mails. The e-mails, however, would normally contain only an individual's case number. It is unlikely those e-mails would have listed Social Security numbers.

Information
Source: Media
March 10, 2008
Central Florida Regional Hospital
Sanford, Florida
MED PHYS 28
The medical records of Central Florida Regional Hospital patients were sold last month at a Salt Lake City surplus store for about $20. The records were sold to a local school teacher looking for scrap paper for her fourth-grade class. The records contained detailed medical histories, phone numbers, addresses, Social Security numbers and insurance information. They were lost en route to a Medicare auditor in Las Vegas, NV.

Information Source: Media

March 10, 2008 Blue-Cross Blue-Shield of Western New York Buffalo, New York

A laptop hard-drive containing vital information about members has gone missing. Blue-Cross Blue-Shield of Western New York says it is notifying its members about identity theft concerns after one of its company laptops went missing.

Information Source: Dataloss DB

March 8, 2008 MTV Networks Los Angeles, California

Computer files with confidential data on employees at MTV Networks were breached by someone outside the company. Personal information in the files included names, birth dates, Social Security numbers and compensation data.

Information Source: Dataloss DB

March 6, 2008 Cascade Healthcare Community Prineville, Oregon

A computer virus may have exposed to outside eyes the names, credit card numbers, dates of birth and home addresses of individuals who donated to Cascade Healthcare Community.

Information Source: Dataloss DB

March 5, 2008 Nevada Department of Public Safety Carson City, Nevada

A private firm working for the Nevada Department of Public Safety has lost a thumb drive containing personal information provided by individuals seeking jobs with the agency. Data included Social Security numbers, addresses and background check information.

Information Source: Dataloss DB

March 3, 2008 DaVita Inc. Denver, Colorado

A laptop containing employee information was stolen from an employee’s vehicle. The information included Social Security numbers and medical insurance information.

Information Source: Dataloss DB


A company-owned laptop computer was stolen from an employee of Kraft Foods traveling on company business. The laptop contained the names and may have contained Social Security numbers.

Information Source: Dataloss DB

February 29, 2008 Wellesley Health Department Wellesley, Massachusetts

Information in an envelope that had been mailed by the town’s health department to a Medicare office in Boston say when the envelope arrived, it was open and the contents were missing. The material included social security numbers, addresses and dates of birth of seniors who had received flu shots from the town last fall.

Information Source: Dataloss DB

February 27, 2008 Health Net Federal Services Rancho Cordova, California

Information from this breach used in our total: 28

March 10, 2008 Blue-Cross Blue-Shield of Western New York Buffalo, New York MED PORT 40,000

March 8, 2008 MTV Networks Los Angeles, California BSO HACK 5,000

March 6, 2008 Cascade Healthcare Community Prineville, Oregon MED HACK 11,500

March 5, 2008 Nevada Department of Public Safety Carson City, Nevada GOV PORT 109

March 3, 2008 DaVita Inc. Denver, Colorado MED PORT 8,800

March 3, 2008 Kaft Foods Northfield, Illinois BSO PORT 20,000

February 29, 2008 Wellesley Health Department Wellesley, Massachusetts GOV PHYS 480

February 27, 2008 Health Net Federal Services Rancho Cordova, California MED DISC 103,000

Information from this breach used in our total: 28
Thousands of doctors in eleven states had their personal information openly posted on a company website. Social Security numbers were part of the personal information exposed. The states involved include Wisconsin, Michigan, Illinois, Indiana, Ohio, Pennsylvania, Tennessee, Iowa, Missouri, Kentucky and West Virginia.

Information Source: Dataloss DB
February 25, 2008
Mecklenburg County
Charlotte, North Carolina

GOV PHYS 400

A County employee’s car was stolen, and in that car was a printout of bank draft transactions within the Park and Recreation Department. Bank account information of an unknown number of people in Mecklenburg County has been stolen.

UPDATE: Four hundred account numbers were stolen; the county alerted those who were affected via letter.

Information Source: Dataloss DB
February 18, 2008
First Magnus Financial
Ft. Lauderdale, Florida

BSF PHYS Unknown

Outside a University of Phoenix Building in Ft. Lauderdale, files and paperwork belonging to the defunct First Magnus Financial were just lying in stacked boxes inside an industrial garbage container. The paperwork contained Social Security numbers, credit card information, addresses, and properties.

Information Source: Dataloss DB
February 16, 2008
Texas A&M University
College Station, Texas

EDU DISC 3,000

A computer file containing the names and Social Security numbers of current and former Texas A&M University agricultural employees was inadvertently posted online and accessible to the public for three weeks.

Information Source: Dataloss DB
February 15, 2008
Systematic Automation Inc
Fullerton, California

BSO STAT 40,000

Police filed possession of stolen property charges against a prison parolee who was arrested for having a computer with more than 40,000 names, addresses and Social Security numbers of California residents. The computer was stolen from Systematic Automation Inc., which processes individualized annual statements customized for employees with a summary of their health and other employee benefits. The hard drive contained employee information from 19 agencies. Some of the agencies include the Modesto City Schools, Clovis Unified School District, Los Angeles Department of Water and Power, Nestle Waters North America and the Torrance Unified School District.

Information Source: Dataloss DB
February 15, 2008
Lexmark International
Lexington, Kentucky

BSO DISC Unknown

The employee personal data was inadvertently exposed, it included Social Security numbers, dates of birth, along with names and addresses. The data was accessed by two unknown parties when the data was loaded to a company file sharing site.

Information Source: Dataloss DB
February 15, 2008
Crosslines Ministries of Carthage
Carthage, Missouri

NGO PHYS 2,000

One of the largest aid agencies in Carthage was burglarized and files, containing the personal information of about 2,000 families, were stolen. Among the items stolen were paper files containing names, addresses, Social Security numbers and other personal information of individuals served by Crosslines.

Information Source: Dataloss DB
February 14, 2008
Tenet Healthcare Corporation
Dallas, Texas

MED INSD 37,000

A ex-employee worked at a Frisco, Texas, billing center for less than two years, and is confirmed to have stolen the
names, Social Security numbers and other personal information of about 90 patients. The employee also had access to 37,000 other accounts.

Information
Source: Dataloss DB
February 13, 2008
Los Angeles Department of Water and Power
Los Angeles, California
GOV PHYS Unknown

A computer was stolen from a contractor on February 11, 2008. Compromised information included name, Social Security number, date of birth, employee identification number, salary, work location, deferred compensation balances, insurance plan coverage and health care benefits selection for all active employees who were members of the DWP Retirement Plan during 2006 and 2007.

UPDATE (2/15/08): The contractor has been identified as Systematic Automation Inc. Nineteen organizations were affected by the breach.

Information
Source: Security Breach Letter
February 13, 2008
Milwaukee County
Milwaukee, Wisconsin
GOV DISC Unknown

Milwaukee County officials mistakenly released numerous confidential court records for a citizens group’s Web site that detail payments for tests and other costs linked to mental competency, paternity and guardianship cases. Entries for psychiatric examinations and guardianship fees in which the clients’ names were still listed.

Information
Source: Media
February 13, 2008
Lifeblood
Memphis, Tennessee
MED PORT 321,000

Laptop computers with birth dates and other personal information of roughly 321,000 blood donors are missing and presumed stolen. Stored inside both computers were names, birth dates and addresses at the time of the individual’s last donation or attempted donation. In most cases, the donors’ Social Security numbers were also stored, along with driver’s licenses, telephone numbers, e-mail addresses, ethnicity, marital status, blood type and cholesterol levels. Social Security numbers had been used to track blood from the donor to the recipients.

Information
Source: Dataloss DB
February 13, 2008
Middle Tennessee State University
Murfreesboro, Tennessee
EDU STAT 1,500

A professor left the university computer unattended in the mass communication department about two weeks ago and an unidentified person is believed to have used the machine to send spam e-mails. The computer contained the names and Social Security numbers of past and current students.

Information
Source: Dataloss DB
February 12, 2008
Modesto City Schools
Modesto, California
EDU PORT 3,500

(209) 576-4192

A computer hard drive holding the names, addresses, birth dates and Social Security numbers of Modesto City Schools' employees was stolen.

UPDATE (2/15/08): The breach has been attributed to a computer theft that affected a contractor named Systematic Automation Inc. Nineteen organizations were affected by the incident.

Information
Source: Dataloss DB
February 12, 2008
Long Island University
Brookville, New York
EDU PHYS 30,000

Students tax forms mailed to them last week in were in defective mailers. The mailers containing each student’s annual 1098-T Tuition Statement were supposed to have adhesive on all four sides. But one side of each envelope was missing adhesive. The statement contains the student’s name, address and Social Security number.
A special education technician had a personal laptop and jump drive stolen during a home robbery. Student name and date of birth, Student ID number, School location If the student has received district transportation additional information such as parent or guardian name and contact information, may also have been on the jump drive. The stolen information did not contain any Social Security numbers or financial information.

Information
Source: Dataloss DB
February 10, 2008
Administrative Systems, Inc
Seattle, Washington
BSO STAT Unknown

A desktop computer stolen from an Administrative Systems, Inc. (ASI) office in Seattle contained names and sensitive information about customers or employees of several of the firm's clients: Continental American Medical, EyeMed Vision/Kelly Services Vision, and Jefferson Pilot Financial Dental. Personal details may have included name, date of birth, mailing address, and Social Security number, depending on the service being provided.

Information
Source: Dataloss DB
February 8, 2008
MLSgear.com
Louisville, Kentucky
BSR HACK Unknown

Injection attacks on web servers hosted by a third-party service provider has compromised the personal data of an unspecified number of individuals who had shopped on Major League Soccer's MLSgear.com Web site. The compromised information included names, addresses, credit card data, debit card data, and MLSgear.com passwords.

Information
Source: Dataloss DB
February 7, 2008
Memorial Hospital
South Bend, Indiana
MED PORT 4,300

A laptop containing the personal information of full and part time employees and retirees is missing. The missing computer contains their names, addresses, birth dates, ID numbers and Social Security numbers.

Information
Source: Dataloss DB
February 4, 2008
Bellin Health
Greenbay, Wisconsin
MED PHYS 650

Patients received notification that their Social Security numbers may have been exposed. Invoices mailed from Bellin Health's unnamed bill processor had viewable Social Security numbers.

Information
Source: PHIPrivacy.net
February 2, 2008
Diocese of Providence
Providence, Rhode Island
NGO STAT 5,000

Four computers were taken, and one had personal information on current and former Catholic school employees. The theft possibly exposed names, addresses and Social Security numbers.

Information
Source: Dataloss DB
February 1, 2008
Marine Corps Bases Japan
Washington, District Of Columbia
GOV PORT 4,000

Additional location: Okinawa, Japan

A laptop was stolen which contained personally identifiable information for clients of Marine Corps Community Services' New Parent Support Program. The laptop may contain names, ranks, Social Security numbers, dates of birth, children's names and mailing addresses of U.S. military service members, U.S. government employees and Status of Forces Agreement personnel on Okinawa and Marine Corps Air Station Iwakuni. It does not include driver's license numbers or bank and credit card information.

Information
Source: Dataloss DB
January 31, 2008
South Carolina Department of Health and Environmental Control in Spartanburg, Cherokee, Union, Greenville and Pickens counties, South Carolina
GOV PORT 400
A laptop containing the names and Social Security numbers of state health department employees is missing. The computer was inside a worker’s vehicle when it was stolen last week from a convenience store. State officials say the password-protected computer contains personal information of state health department workers from Spartanburg, Cherokee, Union, Greenville and Pickens counties.

Information
Source: Dataloss DB
January 31, 2008 University of Minnesota Reproductive Medicine Center
Minneapolis, Minnesota

A doctor at the fertility clinic lost a flash drive that was used to back up his computer. The drive held details of infertility treatments for 3,100 patients going back to 1999. The lost drive included names, birthdates, and in some cases, diagnostic information, details of treatments, whether or not patients had conceived, baby names, and birth weights -- but apparently no SSNs or financial information.

Information
Source: Dataloss DB
January 30, 2008 Davidson Companies
Great Falls, Montana

A computer hacker broke into a database and obtained the names and Social Security numbers of virtually all of the Great Falls financial services company’s clients. The database also included information such as account numbers and balances.

UPDATE (4/12/10): D.A. Davidson was fined $375,000 for failing to adequately protect customer information. The Financial Industry Regulatory Authority (FINRA) found that the database should have been encrypted and had a blank password in place during the 2007 December 25 and 26 breach. On January 16, the hacker alerted D.A. Davidson to the incident and the fact that he had downloaded confidential customer information. The hacker offered to reveal security weaknesses and delete the customer information he had obtained in exchange for $80,000. The hacker was not caught.

UPDATE (11/10/10): A class action settlement was reached for those who were affected by the breach. Anyone receiving a notification letter from Davidson dated January 29, 2008 is a member of the Davidson data breach lawsuit. A $1 million settlement fund will be established to reimburse class members for damages related to having their names, Social Security numbers, addresses, emails, account numbers, tax identification numbers, financial consultant’s identification numbers, account balances and dates of birth exposed. Claim forms requesting reimbursement damages must be received by the Settlement Administrator no later than June 1, 2011.

Information
Source: Dataloss DB
January 30, 2008 Tuolumne General Medical, PHNS (now under ConJoin Group)
Cerritos, California

Four laptop computers and one desktop computer were stolen from a Cerritos PHNS office. PHNS handles insurance-billing information for multiple medical centers. Up to 20,000 people may have been affected. Patients had their billing information, but not medical information, exposed. The other organizations affected by the PHNS breach were not reported, but were mostly in California.

Information
Source: Dataloss DB
January 30, 2008 University of Massachusetts Dartmouth
Dartmouth, Massachusetts

A privacy organization discovered the names, grades, GPAs and partial Social Security numbers of 32 former students. It appears that the information is from a Fall of 2004 CIS 100 class. The discovery was made in December and all affected students were informed by March 3 of 2008.

Information
Source: Dataloss DB
January 29, 2008 Georgetown University
Washington, District Of Columbia

A hard drive containing the Social Security numbers of Georgetown students, alumni, faculty and staff was reported stolen from the office of Student Affairs.

Information
Source: Dataloss DB
January 29, 2008 Wake County (NC) Emergency Medical Services
Raleigh, North Carolina

A Panasonic Toughbook used by county paramedics to store patient information on ambulance runs went missing from the
WakeMed emergency department and now is thought to have been stolen. The laptop contained names, addresses and Social Security numbers.

**UPDATE (2/7/08):** The laptop also may have the names and Social Security numbers of emergency personnel. The number includes county paramedics, firefighters and contracted emergency medical technicians and paramedics from municipal agencies.

**Information Source:**
Dataloss DB

**January 29, 2008**  
**Horizon Blue Cross Blue Shield**  
**Newark, New Jersey**

More than 300,000 members names, Social Security numbers and other personal information were contained on a laptop computer that was stolen. The laptop was being taken home by an employee who regularly works with member data.

**Information Source:**
Dataloss DB

**January 29, 2008**  
**TransUnion, Intelenet Global Services,**  
**Chester, Pennsylvania**

Credit profiles of as many as 400 Americans have been altered by two employees of Mumbai, India-based Intelenet Global Services, an outsourcing company. The two arrested Intelenet employees had been accessing and altering data of individuals in the datafiles of the credit bureau TransUnion since August 2005. The bank account statements of the two men revealed that money was being deposited from an international source for the past few months.

**Information Source:**
Dataloss DB

**January 29, 2008**  
**Invitrogen**  
**Carlsbad, California**

A company laptop was stolen from an employee during a household burglary at the end of December. The laptop was stored in a safe and it is unlikely that the thieves were able to open the safe. Current and former employees may have had their names, Social Security numbers and addresses exposed. At least 1,004 Maryland residents were affected, but the total number of affected people nationwide was not revealed.

**Information Source:**
Dataloss DB

**January 29, 2008**  
**Wendy's International Inc., Mercer Outsourcing (Life Choices Service Center)**  
**Dublin, Ohio**

An administrative error at Life Choices Service Center caused 2008 Benefit Confirmation Statements to be sent to some incorrect addresses. The information of some Wendy’s employees included dependent information for other Wendy’s employees. Names, Social Security numbers and dates of birth may have gone to the wrong people. The error occurred on November 29.

**Information Source:**
Dataloss DB

**January 28, 2008**  
**T. Rowe Price Retirement Plan Services, CBIZ Benefits and Insurance Services Inc.**  
**Baltimore, Maryland**

Names and Social Security numbers of current and former participants in several hundred retirement plans were compromised when several computers were stolen. The machines were taken from the office of CBIZ Benefits and Insurance Services Inc.

**Information Source:**  
Dataloss DB

**January 28, 2008**  
**Kiwanis International, On-Net Services**  
**Indianapolis, Indiana**

On January 4, Kiwanis learned of an unauthorized intrusion into its Kiwanis Family Store Website and database that occurred sometime between December 1 of 2007 and January 4 of 2008. The unauthorized person or persons illegally accessed information by running a SQL injection program that gathered names, credit card numbers, expiration dates and billing/shipping addresses of individuals who had purchased items from the Kiwanis Family Store.

**Information Source:**
Dataloss DB
Dozens of boxes were found in an apartment complex dumpster. Hundreds of patient records, copies of Social Security cards and copies of driver’s licenses were left exposed.

**Information Source:** Dataloss DB

**January 25, 2008 Penn State University**
**University Park, Pennsylvania**

A university laptop containing archived information and Social Security numbers for 677 students attending Penn State between 1999 and 2004 was recently stolen from a faculty member.

**Information Source:** Dataloss DB

**January 25, 2008 Murray State University**
**Murray, Kentucky**

The personal information of students and professionals who attended Murray State was found online. Names, Social Security numbers, dates of birth and other personal information had been posted in a publicly accessible report titled “2000-2001 State Admissions Report.” It seems someone manipulated the Excel file to reveal confidential information. The report should have been posted as a PDF. The information was pulled from the website and affected individuals were contacted shortly after Murray was notified of the breach.

**Information Source:** Dataloss DB

**January 25, 2008 NSK Americas, Inc.**
**Ann Arbor, Michigan**

A folder that allowed access to employee names, Social Security numbers and salaries of current and former employees was accidentally placed on an internal server. A total of 360 employee could access the information of other employees. The breach was caused by an IT administrative error in June of 2006.

**Information Source:** Dataloss DB

**January 25, 2008 DCI Donor Services (DCIDS)**
**Nashville, Tennessee**

A laptop was stolen from a student intern’s home. It contained the Social Security numbers of donor recipients.

**Information Source:** Dataloss DB

**January 25, 2008 Philips Electronics**
**Somerset, New Jersey**

A recruiter’s laptop was discovered to be infected with a virus. The laptop was infected between December 20, 2007 and December 26. Prospective employees may have had their names, Social Security numbers, addresses and dates of birth exposed.

**Information Source:** Dataloss DB

**January 25, 2008 Citibank**
**San Antonio, Texas**

A third party ATM network breach of credit and debit card payment systems affected Citibank customers. Unauthorized users may have accessed Citibank Banking Card numbers and associated Personal Identification Numbers (PIN). Customers were issued new Citibank Banking Cards after Citibank learned of the breach. At least 1,279 New York residents were affected, but the total number of affected people nationwide was not reported.

**Information Source:** Dataloss DB

**January 24, 2008 Fallon Community Health Plan**
**Worcester, Massachusetts**

A vendor computer containing personal information on patients of Fallon Community Health Plan has been stolen. The data included names, dates of birth, some diagnostic information and medical ID numbers. Some of which may be based on Social Security numbers.

**Information Source:** Dataloss DB
An international gang of cyber criminals hacked into the bank’s records. They stole account numbers, created new PINs, fabricated debit cards, then withdrew cash from ATMs in Eastern Europe, Russia, Ukraine, Britain, Canada and New York. Fewer than 100 accounts, some of them dormant, were compromised.

A student employee breached the security of the Baylor Information Network to access the Bear ID and passwords of those logging on to the BIN. This access didn’t include sensitive information like Social Security Numbers, financial information or academic records. It was just unlawful access to Bear IDs and passwords. The information did, however, give access to Baylor e-mail and Blackboard accounts.

Medical documents with Social Security numbers were found in a dumpster.

Tax documents discovered in a dumpster contained customer names and Social Security numbers.

Three employees were discovered to have used customer account information to place fraudulent charges on Target Visa accounts. The account information included names, Social Security numbers, addresses, account numbers and telephone numbers. The total number of affected individuals was not reported. It appears that at least 40 people in four states had their accounts accessed; some of them became victims of fraud.

Nine thousand dollars worth of laptops were stolen from the office sometime during the week or January 18. One or more of the laptops contained personal information.

Malicious software was discovered on a computer used to collect customer information. The information included name, billing and shipping address, phone and fax number, credit card number and security code.

A privacy group discovered four files containing sensitive personal student information online. Students with some connection to the Warner College of Natural Resources had their Social Security numbers, usernames, passwords and other information posted sometime between 2000 and 2004. The breach was discovered on November 15 of 2007.
Information Source: Dataloss DB
January 17, 2008 GE Money, Iron Mountain
Boston, Massachusetts
BSF PORT 150,000

Personal information on customers of J.C. Penney and up to 100 other retailers could be compromised after a computer tape went missing. The missing information includes Social Security numbers for about 150,000 people.

Information Source: Dataloss DB
January 16, 2008 University of Wisconsin, Madison
Madison, Wisconsin
EDU DISC 205

The personal information, including e-mail addresses, phone numbers, Social Security numbers and campus ID numbers of faculty and staff who made purchases from the DoIT computer shop had been accessible on a campus Internet site.

Information Source: Dataloss DB
January 16, 2008 Aspen Grove Market
Boulder, Colorado
BSR DISC Unknown

Employee information and customer credit card information was stolen from a website.

Information Source: Dataloss DB
January 15, 2008 Department of Revenue Wisconsin
Madison, Wisconsin
GOV PHYS 5,000

Breach locations: Lena, Marinette, Little Suamico, Freedom, Kaukauna, Kimberly, Little Chute, Krakow, Keshena and Lakewood

Taxpayers in northeastern Wisconsin had their Social Security numbers exposed in a state mailing. A folding error, apparently the result of a faulty machine, allowed the Social Security numbers to be seen through the clear address window of the envelope.

Information Source: Dataloss DB
January 15, 2008 Naval Surface Warfare Center Dahlgren Division
White Oak, Maryland
GOV PHYS Unknown

(800) 352-7967

Officials at the Naval Surface Warfare Center are warning past and present employees that their identities and credit ratings could be at risk. Two pages of a Naval Surface Warfare Center Employment Verification Report was found when four people were arrested in Bensalem Township, Pa., last week for attempted identity fraud. The report included names, Social Security numbers, birth dates, position titles, tenure codes, pay grades, salaries and other information about the employees.

Information Source: Dataloss DB
January 15, 2008 BJ's Wholesale Club
Natick, Massachusetts
BSR PORT 156

An employee working on a project to replace Social Security numbers with employee ID numbers discovered that the thumb drive containing the information was missing. The thumb drive went missing sometime between December 31 and January 3. Names and Social Security numbers may have been exposed. At least 49 New York, 13 Maryland and 94 Massachusetts residents were affected by the breach. The total number of people affected by the breach nationwide was not reported.

Information Source: Dataloss DB
January 15, 2008 Casa Del Sol Day Care
Mission, Texas
BSO PHYS Unknown

Several boxes of Social Security numbers, bank account details and medical records were found in a dumpster.
A portable storage drive containing the names and Social Security numbers of 990 students has been lost. A school employee transferred the information onto a portable flash drive when the printer where he was working did not print. The employee noticed the drive was missing the next morning.

Information Source: Dataloss DB

January 14, 2008  Raymour and Flanigan Furniture New York, New York BSR INSD Unknown

An employee stole an unknown number of customer credit card details.

Information Source: Dataloss DB

January 12, 2008  California State University Stanislaus, Sodexho Turlock, California EDU UNKN Unknown

A possible data breach occurred on a food vendor’s computer server. Credit card numbers, cardholder names and expiration dates were exposed, leaving hundreds, possibly thousands, of university students, staff and guests open to identity theft, with victims reporting fake charges on their cards. Social Security numbers were not accessible.

Information Source: Dataloss DB

January 11, 2008  University of Akron Akron, Ohio EDU PORT 800

A portable hard drive containing personal information is missing and may have been discarded or destroyed. The device contained Social Security numbers, names and addresses of students and graduates.

Information Source: Dataloss DB

January 11, 2008  University of Iowa Iowa City, Iowa EDU DISC 216

Iowa College of Engineering has notified some of its former students that some of their personal information, including Social Security numbers, was inadvertently exposed on the Internet for several months.

Information Source: Dataloss DB

January 11, 2008  Virginia Department of Social Services Richmond, Virginia GOV INSD 1,500

The Department of Social Services has mailed about 1,500 letters to warn of a potential security breach involving a department computer that police suspect was used to commit fraud. A woman is accused of using her work computer while employed by Social Services last summer to apply for a credit card using her landlord’s information. She was charged with two felony counts, credit card fraud and forgery, and is accused of spending nearly $1,000 on the card.

Information Source: Dataloss DB

January 11, 2008  Bank of West West Richland, Washington BSF INSD 19

A loan officer misused customer information. No details were given about the length of the loan officer’s employment or fraudulent activity. One customer reported $20,000 in fraudulent charges.

Information Source: Dataloss DB

January 11, 2008  United States Transportation Security Administration, Desyne Web Services Arlington, Virginia GOV DISC 247

The TSA website designed by a contractor to help travels remove their names from airline security watch lists was found to be insecure. Around 247 travelers submitted personal information through an unsecured “file your application online” link. The site ceased operations on February 13 of 2007 after authorities became aware of the lack of security. It had been operating since October 6 of 2006.

Information Source: Dataloss DB

January 14, 2008  Tennessee Tech University Cookeville, Tennessee EDU PORT 990
January 10, 2008  
Select Physical Therapy  
Levelland, Texas  
MED  PHYS  4,000

The company dumped about 4,000 pieces of sensitive customer information in garbage containers behind its facility. The records included Social Security numbers, credit and debit card account numbers, names, addresses and telephone numbers.

Information Source:  
Dataloss DB  

records from this breach used in our total: 4,000

January 10, 2008  
Johns Hopkins Hospital  
Baltimore, Maryland  
MED  PHYS  190

On December 21, a briefcase with sensitive documents was stolen from an employee's car. The documents included names, Social Security numbers, addresses, dates of birth, phone numbers, physical and mental health information, medical ID numbers and demographic information. Current and former members of a program called Creative Alternatives were affected.

Information Source:  
Dataloss DB  

records from this breach used in our total: 190

January 8, 2008  
Wisconsin Department of Health and Family Services  
Madison, Wisconsin  
GOV  DISC  260,000

Social Security numbers were printed on about 260,000 informational brochures sent by a vendor hired by the state, Electronic Data Systems Inc. (EDS), to recipients of SeniorCare, BadgerCare and Medicaid. The company agreed to pay $250,000 to the state for the mistake, as well as paying for an identity theft monitoring service for the affected individuals, for a total of about $1 million.

Information Source:  
Dataloss DB  

records from this breach used in our total: 260,000

January 8, 2008  
University of Georgia  
Athens, Georgia  
EDU  HACK  4,250

Former and prospective residents of a University housing complex were affected by a hacker who was able to access a server containing personal information, including Social Security numbers. A computer with an overseas IP address was able to access the personal information - including Social Security numbers, names and addresses - of 540 current graduate students living in graduate family housing and 3,710 former students and applicants.

Information Source:  
Dataloss DB  

records from this breach used in our total: 4,250

January 8, 2008  
Alaron Trading Company, Alaron Financial Services  
Chicago, Illinois  
BSF  PORT  150

A laptop was stolen from the IT department on or around January 3. Employees may have had their names, Social Security numbers, addresses, salaries and dates of birth exposed.

Information Source:  
Dataloss DB  

records from this breach used in our total: 150

January 7, 2008  
Sears, ManageMyHome.com  
Cook County, Illinois  
BSR  DISC  Unknown

Sears' ManageMyHome.com site exposed customer purchase data to any online visitor who asked about it.

Information Source:  
Media  

records from this breach used in our total: 0

January 7, 2008  
Geeks.com  
Oceanside, California  
BSR  HACK  Unknown

Personal and financial data may have been compromised by an intrusion into the systems of the online retailer's Web site. Compromised information included the names, addresses, telephone numbers and Visa credit card numbers.

Information Source:  
Dataloss DB  

records from this breach used in our total: 0

January 7, 2008  
College Point Bus Depot  
New York, New York  
BSO  PHYS  100

Social Security numbers, copies of driver's licenses, grievance papers and other personal information were thrown into the trash. A witness saw a foreman throwing out the papers.
January 7, 2008  Franklin University  
Columbus, Ohio  
EDU DISC  6,440

A file with student and alumni information was accidentally placed on a publicly accessible web server. The information included names, Social Security numbers, term and class information, email addresses and Franklin University ID numbers. The file was removed from the web server.

January 7, 2008  Central Piedmont Community College  
Charlotte, North Carolina  
EDU INSD  3,437

An employee reported unauthorized credit card charges. An investigation revealed that a part-time employee had used the employee’s password and accessed personal information.

January 7, 2008  CMP Advanced Mechanical Solutions  
Binghampton, New York  
BSO DISC  202

The personal information of employees was placed on a shared Company drive. The files were accessible to all employees who had a computer between August 2007 and November 2007. The breach occurred when payroll files were transferred to human resources and a copy of the data files was inadvertently left on a shared drive.

January 6, 2008  U-Care Thrift Store  
Mesa, Arizona  
BSR PHYS  30

Employee records with Social Security numbers, dates of birth and driver’s license photos were found in an alley.

January 5, 2008  New Mexico State University  
Las Cruces, New Mexico  
EDU PORT Unknown

A computer hard drive containing the names and Social Security numbers of current and former NMSU employees is missing from the Pan American Center.

January 5, 2008  Commerce Bank, Citizens Bank, NewConcept Inc.  
Philadelphia, Pennsylvania  
BSF INSD Unknown

Employees of several organizations were found to be involved in a fraud ring. Using customer information, the criminals attempted to defraud Commerce Bank and Citizens Bank. People in Philadelphia, the Eastern District of Pennsylvania, New Jersey, the Eastern District of New York and elsewhere were affected. The fraud ring was in effect between March of 2007 and May 15 of 2007.

January 5, 2008  University of Texas Austin  
Austin, Texas  
EDU DISC  13

A privacy group discovered a file with the names, Social Security numbers, test scores, assignment scores and grades of 13 people online. It appears that the file was accidentally placed there by a professor who taught Biology 331. The discovery was made on November 3 of 2007 and the University took the file offline within hours of notification.

January 4, 2008  Health Net  
Mountain View, California  
MED PORT  5,000

Additional locations: Connecticut.
Thousands of Health Net employees in Connecticut and other states have been notified that their names and Social Security numbers were on a laptop computer that was stolen more than a month ago from a company vendor. The laptop had information on about 5,000 employees companywide and an undisclosed number of health-care providers outside the Northeast.

Information Source: Dataloss DB
January 4, 2008 Florida Department of Children and Families
Orange, Florida

GOV PORT 1,200

Additional locations: Seminole and Osceola, FL

Social Security numbers, birth dates and other information about day-care workers in Orange, Seminole and Osceola counties were among the data on five laptop computers that were stolen from the DCF office near Orlando.

Information Source: Dataloss DB
January 4, 2008 Maryland Department of Assessments and Taxation
Baltimore, Maryland

GOV DISC 900

The Maryland Department of Assessments and Taxation Web site may have exposed Social Security numbers online because the application system did not have a necessary security certificate to encrypt the information before it was sent out over the Internet. Roughly 900 people used the system.

Information Source: Dataloss DB
January 4, 2008 Mariner Health Care, Windham Brannon, SavaSeniorCare Administrative Services, LLC
Atlanta, Georgia

BSF PORT 80,124

Cash and several laptops were stolen from Windham’s Atlanta office on the evening of December 31, 2007. Windham provides audit services for Mariner’s and SaveSeniorCare’s 401(k) benefit plans. Current and former employees may have had their names, Social Security numbers, addresses, dates of birth, salary information and 401(l) account information.

Information Source: Dataloss DB
January 3, 2008 Robotics Industries Association
Ann Arbor, Michigan

BSO HACK Unknown

A hacker accessed the administration site for Robotics Online gaining access to individual orders that contained credit card information. Seven residents of NH were affected, but national totals were not indicated.

Information Source: Media
January 3, 2008 Dorothy Hains Elementary School
Augusta, Georgia

EDU STAT Unknown

The library door was kicked in and the circulation computer was stolen, something the principal desperately wants back because it has the Social Security numbers of students and teachers on it.

Information Source: Dataloss DB
January 2, 2008 Workers Compensation Fund
Salt Lake City, Utah

BSO PORT 2,800

Officials with one of Utah’s largest insurance companies are searching for a stolen laptop containing Social Security numbers and other personal information for about 2,800 people and 1,400 companies. The computer was taken from a car parked in the home garage of an auditor for the Workers Compensation Fund.

Information Source: Dataloss DB
January 2, 2008 Centocor, Inc.
Horsham, Pennsylvania

BSR PORT Unknown

In early October, Centocor was notified by its IT vendor that one or two computers could not be located. Centocor’s vendor investigated and reported that several more computers could not be found on November 29. Centocor believes that a former, contracted employee of the vendor removed the computers from the Horsham facilities. One of the laptops probably contained a file with information intended for management of National Faculty and Rounds on the Road Speakers programs. Names, cities and states, Social Security numbers and tax ID numbers of speaker consultants may have been exposed.
A laptop computer containing personal information on Minnesotans licensed by the state Commerce Department was stolen from one of its Pennsylvania vendors.

Someone broke into several county offices over Christmas and stole laptop computers that county officials now believe may have contained Social Security numbers and other personal information for every registered voter in Davidson County.

UPDATE (1/19/08): Metro Police confirmed late Thursday they have recovered the hard drive from the laptop computer, containing names and complete Social Security numbers for 337,000 registered voters, that was stolen from the Election Commission in December.

A military laptop computer is missing and it contains personal information including Social Security numbers, birth dates, addresses, and telephone numbers of active and retired Air Force members. The laptop belonged to an Air Force band member at Bolling Air Force Base, he reported it missing from his home.

Computer equipment and a licensing computer were stolen during an office burglary that occurred sometime around December 15. Some agent appointment forms were on the licensing computer. Names, Social Security numbers, addresses and other personal client information may have been exposed.

At least six central Ohioans are now under investigation by the U.S. Secret Service for hacking into a government Web site and stealing Social Security numbers to create false credit accounts. More than 270 people nationwide might have been victimized by a security lapse in the Franklin County Municipal Court Web site. Someone was randomly feeding Social Security numbers into a clerk’s site, which contained personal information for thousands of people charged with misdemeanors, some guilty of only a speeding ticket. Once a number was hit on, the name, address, age and other information could be used to obtain credit cards and open bank accounts.

UPDATE (1/21/2011): Two people were sentenced to two and a half years in federal prison. Each man was charged with bank fraud, conspiracy to commit bank fraud and aggravated identity theft.

On December 1, a company laptop was stolen from an employee’s car while it was parked at home. The information included employee names, Social Security numbers, email addresses, ID numbers and salary information. Employees of Wendy's International, Wendy's Restaurants of Canada and The New Bakery were affected.

Data tapes containing Social Security numbers, phone numbers and addresses for up to 800 current and former employees.
Data tapes containing Social Security numbers, phone numbers and addresses for up to 800 current and former employees of the state Dormitory Authority are missing.

**Information Source:** Dataloss DB

**December 20, 2007**

**Greenville County School District**

Greenville, South Carolina

EDU HACK Unknown

The district notified employees last week that its computers had been compromised and that employees’ personal information was taken, including their names, home phone numbers and Social Security numbers.

**Information Source:** Dataloss DB

**December 20, 2007**

**Robotic Industries Association**

Ann Arbor, Michigan

BSR HACK 1,500

Sensitive customer information was accessed by a hacker on or around December 10. The hacker gained access to the administration site by using a password-cracking program or guessing the password. The hacker then had access to customer orders and credit card information.

**Information Source:** Dataloss DB

**December 20, 2007**

**Watertown Public Schools**

Watertown, Massachusetts

EDU PORT 400

A laptop owned by Watertown was stolen from the vehicle of the Director of Personnel of Watertown Public Schools on December 18. There is a possibility that the laptop contained employee information. Employee names, Social Security numbers, addresses and other payroll information may have been exposed.

**Information Source:** Dataloss DB

**December 20, 2007**

**Jackson National Life Insurance Company, INVEST Financial Corporation**

Lansing, Michigan

BSF HACK Unknown

Jackson discovered a breach that allowed access to client information through the Internet-based trading program Streetscape. The incident involved the unauthorized use of a password. Client INVEST accounts and balances, names, Social Security numbers, tax ID numbers, addresses and dates of birth were accessed.

**Information Source:** Dataloss DB

**December 19, 2007**

**Vitale, Caturano and Company**

Boston, Massachusetts

BSF PORT 8,000

On December 14, an accountant’s laptop was stolen from his or her car while it was parked in a garage onsite. A file containing 8,000 to 9,000 names, deferred income account balances and Social Security numbers of members of the International Brotherhood of Electrical Workers Local 103 benefit plan was stored on the laptop.

**Information Source:** Dataloss DB

**December 18, 2007**

**Brownsville School District**

Brownsville, Pennsylvania

EDU PHYS Unknown

Forms with employee personal information littered the fence of a Brownsville school district warehouse. Information on litter contained confidential letters with names, bank account numbers, and Social Security numbers. The forms may be more than ten years old, but they each contain information that’s still valuable.

**Information Source:** Media

**December 18, 2007**

**Pennsylvania Department of Aging**

Harrisburg, Pennsylvania

GOV PORT 21,000

A state Department of Aging-owned laptop computer containing personal information on senior citizens was stolen from a Johnstown home. The information included names, addresses, Social Security numbers and some medical information.

**Information Source:** Dataloss DB

**December 17, 2007**

**West Penn Allegheny Health System**

Pittsburgh, Pennsylvania

MED PORT 42,000

649
The names, Social Security numbers, phone numbers, addresses and patient care information of 42,000 patients were all on a laptop computer stolen from a nurse’s home. Only home care and hospice patients could be impacted, not patients at the hospitals.

**Information Source:** Dataloss DB
**December 14, 2007**
**Deloitte & Touche**
**New York, New York**
**BSO**  **PORT**  **Unknown**

A laptop containing the personal information of an undisclosed number of Deloitte & Touche partners, principals and employees was stolen while in possession of a contractor responsible for scanning the accounting firm’s pension fund documents. The computer contained confidential data, including names, Social Security numbers, birth dates, and other personnel information, such as hire and termination dates.

**Information Source:** Dataloss DB
**December 14, 2007**
**Deloitte & Touche, IKON Office Solutions**
**New York, New York**
**BSF**  **PORT**  **22,634**

A laptop was stolen from a contractor working on scanning Deloitte's pension fund documents. The laptop contained names, Social Security numbers, dates of birth, start and end dates and other personnel information of Deloitte partners, principals and other employees. The laptop was stolen sometime around Thanksgiving. Deloitte no longer works with the service provider.

**Information Source:** Dataloss DB
**December 10, 2007**
**Cameron County**
**Brownsville, Texas**
**GOV**  **UNKN**  **Unknown**

An employee released an e-mail with a list of all county officials and employees. It reportedly contained names, Social Security numbers, and salaries.

**Information Source:** Dataloss DB
**December 10, 2007**
**Sutter Lakeside Hospital**
**Lakeport, California**
**MED**  **PORT**  **45,000**

A laptop computer containing personal and medical information of approximately 45,000 former patients, employees and physicians has been stolen from the residence of a contractor.

**Information Source:** Dataloss DB
**December 10, 2007**
**Iowa Department of Natural Resources**
**Des Moines, Iowa**
**GOV**  **PORT**  **7,000**

A contractor working for the DNR revealed that a computer jump drive containing the names and Social Security numbers for 7000 people is missing. The contractor believes the jump drive fell off of his desk and into a garbage can.

**Information Source:** Dataloss DB
**December 10, 2007**
**Peerless Industries Inc., C I Host Chicago Datacenter**
**Chicago, Illinois**
**BSR**  **STAT**  **Unknown**

C I Host experienced a burglary on October 2. Peerless’s web-servers had been housed there and were stolen during the incident. Customer names, addresses, email addresses, telephone numbers, and encrypted credit card numbers were on one or more of the stolen web-servers. Affected customers were notified during the first half of November.

**Information Source:** Dataloss DB
Detailed, personally identifiable medical records of thousands of Colorado residents were viewable on a publicly accessible Internet site for an uncertain period of time. The data included details of patients' visits to emergency rooms - what ailments they complained of, diagnoses, treatments, and medical histories, along with the patients’ names, occupations, addresses, phone numbers, insurance providers, and in some cases, Social Security numbers. The company is trying to determine the exact number of patients affected, but Beck says the number looks to be fewer than 5,000.

Information Source: Dataloss DB
December 7, 2007

Colorado Board of Dental Examiners
Lone Tree, Colorado

More than a hundred Colorado dentists and their patients could be at risk for identity theft after a car containing a bag of sensitive information was stolen. Authorities found the car a few days later at an apartment complex where one of the alleged thieves lived. Inside the unit, police discovered a massive amount of personal information from previous crimes. Social Security numbers, dates of birth, credit card numbers, pin numbers to those credit cards, and photo IDs of the individuals they stole credit cards from were all in the bag.

Information Source: Dataloss DB
December 6, 2007

S&K Famous Brands, Inc.
Richmond, Virginia

On October 24, S&K was notified of a suspicious email addressed to customers. It was determined that the email had been sent from a fictitious S&K email address and was a phishing attempt. The email contained a real or fictitious S&K order number and the last four digits of the credit card number used by the customer to whom it was addressed. The email requested that the customer provide a credit card identification number. The online store was disconnected and remote access to S&K’s network was disabled within 30 minutes of the discovery. Customers of S&K Menswear may have had their names, addresses, credit card numbers and expiration dates may have been accessed.

Information Source: Dataloss DB
December 6, 2007

Oak Ridge National Laboratory
Oak Ridge, Tennessee

Hackers may have infiltrated a non-classified database containing names, Social Security numbers and birth dates of every lab visitor between 1990 and 2004. The assault was in the form of phony e-mails containing attachments, which when opened allowed hackers to penetrate the lab’s computer security. The lab has sent letters to about 12,000 potential victims.

Information Source: Dataloss DB
December 5, 2007

Memorial Blood Centers
Duluth, Minnesota

Hot Line (888) 333-1491 Contacts: Memorial Blood Centers Laura Kaplan, (651) 332-7220 lkaplan@mbc.org or Jim McCartney, (952) 346-6688

A laptop computer holding donor information was stolen. About 268,000 donor records on this laptop computer contain a donor name in combination with the donor’s Social Security number.

Information Source: Dataloss DB
December 5, 2007

Forrester Research
Cambridge, Massachusetts

Thieves stole a laptop from the home of a Forrester Research employee, potentially exposing the names, addresses and Social Security numbers of an undisclosed number of current and former employees and directors.

Information Source: Dataloss DB
December 4, 2007

Indianapolis Power and Light
Indianapolis, Indiana

(317) 261-4845

The private information of thousands of customers was inadvertently posted online for up to four years. Data included names, addresses and Social Security numbers.

Information
Social Security numbers of about 1,400 prospective law school applicants may have been compromised when a school Web site was accessed illegally.

Other organizations: Community Blood Bank, Ohio Masonic Home

A laptop was stolen from a Battelle & Battelle LLC employee’s vehicle. The laptop contained information on an audit of the Community Blood Center's 401K plan as well as information on the employees of Springfield-based Ohio Masonic Home. The stolen laptop needs multiple levels of authentication in order to access the sensitive data, according to a representative of Battelle. Masonic Home officials report 600 of its employees were affected.

The state of Massachusetts is warning 150,000 members of its Prescription Advantage insurance program that their personal information may have been snatched by an identity thief. Local authorities arrested a lone identity thief who had been using information taken from the program in an attempted identity theft scheme. Although the thief used information from just a small number of participants in the scheme, state data-breach laws require that the 150,000 people who could have possibly been affected by the breach be contacted.

An employee who had authorized access to personal information was arrested and charged with stealing personal information and identity theft. The employee took client names, Social Security numbers, dates of birth, addresses and bank account information.

Six boxes were left unattended in a public hallway for more than six hours. The files contained personal information of current and former employees and were placed there by human resources. Names, addresses and social security numbers could have easily been stolen. The files also contained embarrassing information, including disciplinary actions, results from a drug test, a sexual harassment case even someone’s criminal record from another state.

An electronic folder that resided on a share drive at OCD was accessed by authorized users of the Johnson & Johnson computer system in North America for approximately six months. The file should have only been accessed by authorized human resources personnel and included current and former employee Social Security numbers, addresses, phone numbers, pre-employment screening information, compensation information and other employment data. The information in the folder dates back to January of 2002.

Those who suspect their Social Security numbers were posted can search their names on the Web site www.ssnbreach.org.
More than 400 former UF students might have been put at risk for identity theft after their Social Security numbers were posted on UF’s Computing & Networking Services Web site. A news release from the Liberty Coalition, a group that works to preserve the privacy of individuals, said 14 files on the Web site contained sensitive information of 534 former UF students, including 415 Social Security numbers.

Information
Source: Dataloss DB

November 21, 2007
United Healthcare (UnitedHealthcare)
New York, New York

UnitedHealthcare is headquartered in Minneapolis, Minnesota.

United Healthcare posted the Social Security numbers of doctors at Columbia University’s faculty practice on a public Web site. United posted the taxpayer identification numbers, some of which were Social Security numbers, alongside the names of 993 providers at Columbia who participate in the insurer’s network. The list was supposed to be accessible to Columbia employees during the current open enrollment period.

Information
Source: Media

November 20, 2007
Beth Israel Deaconess Medical Center, Affiliated Physicians Group (APG)
Foxborough, Massachusetts

On October 20, a briefcase was stolen from the vehicle of a physician. The briefcase contained patient encounter forms with names, addresses, Social Security numbers, telephone numbers and insurance information.

Information
Source: Dataloss DB

November 19, 2007
General Cable Corporation
Marshall, Texas

An employee used the wrong email distribution list and sent an email to several unauthorized employees on November 1. The email included names and Social Security numbers of current and former employees, as well as third-party vendors. At least 19 Massachusetts residents and four residents of other states were affected, but the total number of affected individuals nationwide was not revealed.

Information
Source: Dataloss DB

November 16, 2007
A.J. Falciani Realty Company
Vineland, New Jersey

Computers containing the personal information of between 500 to 1,000 clients of A.J. Falciani Realty Company were taken in a burglary. Many of the stolen computers stored the names, addresses, Social Security numbers, dates of birth, telephone numbers and other information on the company’s clients.

Information
Source: Dataloss DB

November 16, 2007
University of Wisconsin, Whitewater
Whitewater, Wisconsin

Officials were notified by one individual about his ability to access an online search feature for the school’s website. The search feature could be used to see student names and Social Security numbers along with some other limited student information. Access to the feature was promptly disabled upon notification of the problem.

Information
Source: Media

November 16, 2007
U.S. Department of Veteran Affairs
Washington, District Of Columbia

Investigation from a man’s home uncovered a computer that held about 1.8 million Social Security numbers from the U.S. Department of Veteran Affairs, where he had been employed as an auditor. Veterans Affairs’ officials have said only 185,000 numbers are at risk because many were repeated in the file.

Information
Source: Dataloss DB

November 16, 2007
Wake Technical Community College
Raleigh, North Carolina

A flash drive that contained student names and Social Security numbers was lost and recovered. The flash drive was discovered missing on October 18 and was recovered within a month. The College stopped using Social Security numbers as student IDs shortly after this breach.
November 15, 2007
Roudebush Veteran’s Administration Medical Center
Indianapolis, Indiana

Two personal computers and a laptop computer were allegedly stolen from an unsecured room. One of the stolen computers contained the names, Social Security numbers and dates of service of approximately 12,000 veterans.

UPDATE (3/19/08): A 50 year old Indianapolis man was arrested Monday on one count of Class D felony theft after investigators identified him from surveillance video. A probable cause affidavit, a sworn police statement filed in support of the charge, identifies him as a former patient at the facility. The man has been charged in the disappearance of hospital computer equipment that contained the records of nearly 12,000 patients.

November 14, 2007
Harvard University
Cambridge, Massachusetts

Folders containing information about students from the University’s Division of Continuing Education were lost. The folders were from the previous year and included names, Social Security numbers, Harvard ID numbers, dates of birth, addresses, email addresses and phone numbers. Some of the folders contained additional information about the students and their dependents, spouses or parents. The information did not include credit card numbers. The University speculates that the folders were placed in a file cabinet that was later recycled.

November 13, 2007
Commerce Bancorp
Philadelphia, Pennsylvania

A Commerce Bancorp Inc. employee gave out personal information on an unspecified number of the Cherry Hill bank’s customers. The Bank discovered the breach through an internal investigation and sent letters to affected customers. The bank does not know if the information included account numbers and Social Security numbers. It is unclear if this incident is related to or the same as the January 5 insider breach that involved a Commerce Bank employee.

November 13, 2007
Youth Women’s Christian Association (YWCA)
New York, New York

Staff discovered that a computer had been stolen from the office sometime around October 1. It contained the names and Social Security numbers of active participants in the YWCA Retirement Fund. Individuals who participated between January 1, 2002 and September 28 were affected.

November 12, 2007
The Horace Mann Companies
Springfield, Illinois

A Horace agent’s laptop was stolen on October 31. It contained names, addresses, phone numbers and Social Security numbers. A security breach letter from Horace claims that no business files were lost or compromised.

November 11, 2007
Oracle Corporation, Lodestar
Suwanee, Georgia

A computer that contained employee and contractor information was misplaced during a move. Employees and contractors of Lodestar may have had their names, Social Security numbers, addresses, earning information and expense information exposed.

November 11, 2007
State of Nevada
Carson City, Nevada

The Nevada State Personnel Director said that hundreds of CDs containing payroll information about state employees had been lost. Thirteen thousand CDs had been sent to 80 agencies over the last three years and 470 were missing as of November. The Personnel Director plans to implement a new system to decrease data loss.

Information Source: Dataloss DB
Records from this breach used in our total: 1,886

Information Source: Dataloss DB
Records from this breach used in our total: 12,000

Information Source: Dataloss DB
Records from this breach used in our total: 56

Information Source: Dataloss DB
Records from this breach used in our total: 0

Information Source: Dataloss DB
Records from this breach used in our total: 13,000

Information Source: Dataloss DB
Records from this breach used in our total: 209

Information Source: Dataloss DB
Records from this breach used in our total: 132
UConn was notified of a security breach by an outside party on the network of Convio, Inc., a vendor used by The University of Connecticut Foundation, Inc. for processing online gift transactions and communicating by e-mail. This breach affected 92 of Convio’s clients nationwide, including the UConn Foundation. User names and passwords for Convio account preferences were compromised in this breach.

A paramedic left a computer on the back bumper of an ambulance and then drove away. The laptop contains names, addresses, phone numbers and Social Security numbers of approximately 28,000 people who have been cared for by the Cabarrus County EMS over the last four years.

A hard drive was discovered missing from a computer in the employee fitness center on August 28. Technicians had been working on a computer during the previous day and may have misplaced its hard drive. The hard drive contained full names, Social Security numbers, dates of birth, genders, addresses, telephone numbers, emergency contact information, physician addresses and fitness center membership information of current and former employees.

Around five hundred credit or debit card numbers were obtained via unknown means. Around one hundred were used to make approximately $3000 in contributions to Ron Paul’s presidential campaign. It is possible that the identity thieves were testing the cards to see if they were valid.

A laptop with customers’ personal information including names, addresses, Social Security numbers and bank account numbers was stolen from Butte Community Bank.

The personal information, including the names, ages and Social Security numbers of families enrolled in the state’s ALL Kids health care coverage program, were accidentally sent to the wrong families last week. 1,554 affected families were alerted that some of their confidential information might have been released.

KimsCrafts’ on-line ordering system experienced a security breach or security breaches between August 13 and October 1. Customers who placed orders anytime on or after June 25, 2001 may have had their names, addresses and credit card numbers accessed. It is not clear whether the breach occurred because of an unauthorized user or because of an employee or contractor mistake.
Montana State University
Bozeman, Montana

November 2, 2007

MSU learned that an employee’s laptop computer had been stolen somewhere off-campus. It contained the Social Security numbers of 216 students and employees who lived in on-campus housing from 1998 to 2007.

An independent security watchdog group informed MSU that an Excel spreadsheet with the names and Social Security numbers of 42 people, most of them hired in the summer of 2006, was publicly accessible on MSU’s Web site.

While investigating that breach, MSU data-security staff found another Excel spreadsheet accidentally posted on the MSU Web site since 2002. It contained the Social Security numbers of 13 people who got travel vouchers from the computer science department in the College of Engineering.

City University of New York
New York, New York

November 1, 2007

A broken laptop containing personal information was taken from the School’s financial aid office.

MeadWestvaco
Glen Allen, Virginia

November 1, 2007

An employee accidentally posted an electronic file in a location that was accessible to most or all people with access to MeadWestvaco’s internal computer network. The file was accessible for approximately 10 days. It contained names, Social Security numbers and home addresses of employees. At least 652 North Carolina residents were affected, but the total number of affected individuals nationwide was not reported.

University of Nevada, Reno
Reno, Nevada

October 30, 2007

A University of Nevada, Reno administrative employee has lost a flash drive that contained the names and Social Security numbers of 16,000 current and former students.

Hartford Financial Services Group
Hartford, Connecticut

October 30, 2007

Three backup tapes that contained personal information of 230,000 customers, including 9,200 Ohioans, mainly of the company’s property lines, were misplaced.
Someone broke into a locked office building, several computers with flat screen monitors were stolen. One of those computers had patient information on about 75,000 people. This information included names, addresses, Social Security number, even medical information.

### Information Source:
Dataloss DB

**Pathology Group**
Memphis, Tennessee

**October 30, 2007**

Employees' names, Social Security numbers and other information were on a laptop computer that was stolen.

### Information Source:
Dataloss DB

**United States Postal Service**
Oahu, Hawaii

**October 29, 2007**

Two men found a box in a dumpster. The cell phone business recently moved and threw away documents that contained personal information from customers. The information contained driver's license numbers, Social Security number, bank account numbers, credit card numbers, work and home addresses.

### Information Source:
Media

**ABC Phones, ACC Communications**
Greenville, North Carolina

**October 29, 2007**

A former Horace agent's computer was lost during shipping sometime around September 27. The computer contained names, Social Security numbers, addresses, phone numbers, driver's license numbers, bank account numbers and credit card numbers.

### Information Source:
Dataloss DB

**The Horace Mann Companies**
Springfield, Illinois

**October 29, 2007**

Personal information of alumni was available on the page of the School's website through a Google Internet search. The information included names, Social Security numbers, dates of birth, addresses and telephone numbers. The information was immediately removed from the website after the mid-October discovery.

### Information Source:
Dataloss DB

**New England School of Law**
Boston, Massachusetts

**October 29, 2007**

Cyberspace criminals gained systems entry despite multiple security layers and accessed some credit card transactions. The retailer of posters, prints and framed art alerted customers that hackers had gotten into the website to access credit card accounts.

### Information Source:
Dataloss DB

**Art.com**
Lockbourne, Ohio

**October 28, 2007**

The breach occurred on a server located in Delaware. The location listed is the headquarters of Scarborough & Tweed.

### Information Source:
Dataloss DB

**Scarborough & Tweed**
Pleasantville, New York

**October 26, 2007**

A microfilm containing the personal information of alumni were missing. Names, previous addresses, phone numbers, birth dates and Social Security numbers was on the missing microfilm.

### Information Source:
Dataloss DB

**University of Akron**
Akron, Ohio

**October 25, 2007**

Records from this breach used in our total: 75,000

Records from this breach used in our total: 3,000

Records from this breach used in our total: 0

Records from this breach used in our total: 737

Records from this breach used in our total: 5,098

Records from this breach used in our total: 0

Records from this breach used in our total: 570

Records from this breach used in our total: 1,200
Unauthorized third parties attempted to or succeeded in accessing customer account during May. It appears that the third parties used techniques to gather access customer accounts through customer care telephone lines as opposed to Virgin's website. It was determined that people were calling customer service and claiming to be a customer or relative of a customer, and obtaining account information. Third parties may have also called customer service and guessed common surnames and common passwords or secret answers in order to access customer accounts. After accessing an account via customer care telephone lines, the third parties may have transferred account balances and/or airtime minutes, converted account balances to Virgin merchandise, purchased Virgin airtime or merchandise with credit or debit cards linked to the account, changed account login or contact information, or deactivated the account.

Massachusetts restaurants were targeted by an individual or individuals seeking to illegally obtain credit card data. The data that was compromised included credit card numbers, expiration date and name associated with the card.

West Virginia officials are alerting 200,000 past and current members of three health insurance programs that a computer tape containing full names, addresses, phone numbers, Social Security numbers and marital status was lost last week while being shipped via United Parcel Service.

A Sarasota resident was fishing in a trash container for boxes when he found 400 documents. These documents included membership forms and employment applications with names, addresses, credit card numbers and Social Security numbers.

An unauthorized person reportedly gained access to a computer system and confidential files, including Social Security numbers, birth date information and addresses for some 11,000 alumni and current DSC employees who graduated or worked at DSC from 1986 to 2005.

Two publicly accessible documents that contained the records of nearly 500 recipients of the federal Perkins Loan, along with each recipient's address, date of birth, Social Security number, legal name and loan amount, were accessible on the Bates network.

A laptop that may have contained names, Social Security numbers and addresses was lost during a move. The research department of the AAP misplaced a file cabinet and a laptop during the process of moving offices.
Information
Source: Dataloss DB

La Jolla, California

BSR PORT Unknown

A data storage tape containing backup data relating to pharmacy transactions was stolen during a store burglary. It contained customer names, prescription information and insurance plan membership information. Some membership numbers were or contained Social Security numbers.

Information
Source: Dataloss DB

October 19, 2007, Blockbuster Inc.
Lantana, Florida

BSR PORT Unknown

A computer was stolen from a Blockbuster office during a September 5 burglary. Customer names, addresses, telephone numbers, Blockbuster account numbers, driver’s license numbers, credit card numbers and credit card types, and email addresses were on the computer’s hard drive.

Information
Source: Dataloss DB

October 18, 2007, University of Cincinnati
Cincinnati, Ohio

EDU PORT 7,000

The personal information of thousands of University of Cincinnati students and graduates has been stolen. A flash drive was taken from a UC employee last month. It contained the Social Security numbers and other data for more than 7,000 people.

Information
Source: Dataloss DB

October 18, 2007, First Banks Inc, iWire Inc
Jericho, New York

BSF HACK 5,234

iWire’s Payroll Passport/IC Settlement database was breached on September 29. A database of cardholder account records was accessed. It contained Social Security numbers.

Information
Source: Dataloss DB

October 17, 2007, Home Depot
Boston, Massachusetts

BSR PORT 10,000

A laptop computer containing about 10,000 employees’ personal data was stolen from a regional manager’s car. The computer, which was password protected, didn’t contain any customer information. The laptop contained names, home addresses and Social Security numbers of certain Home Depot employees.

Information
Source: Dataloss DB

October 17, 2007, Louisiana Office of Student Financial Assistance, Iron Mountain
Baton Rouge, Louisiana

EDU PORT Unknown

http://www.osfa.state.la.us/notice.htm

Sensitive data for virtually all Louisiana college applicants and their parents over the past nine years were in a case lost last month during a move. The data included Social Security numbers for applicants and their parents. The bank account information for START account holders also was involved.

Information
Source: Dataloss DB

October 16, 2007, Administaff Inc.
Houston, Texas

BSO PORT 159,000

Current and former workers personal data may be compromised because of a stolen laptop. The data wasn’t encrypted when it was stored on the portable computer, which is password-protected. Data stored on the laptop included names, addresses and Social Security numbers for most employees paid by Administaff in 2006.

Information
Source: Dataloss DB

October 15, 2007, Transportation Security Administration

GOV PORT 3,930

659
Two laptop computers with detailed personal information about commercial drivers across the country who transport hazardous materials are missing and considered stolen. The laptops contained the names, addresses, birthdays, commercial driver's license numbers and, in some cases, Social Security numbers of 3,930 people.

Information Source: Dataloss DB

October 13, 2007, Montana State University
Bozeman, Montana
EDU HACK 1,400
(406) 994-6550, http://eu.montana.edu/security/
An unknown hacker remotely accessed a computer server that housed records containing credit card numbers and Social Security numbers of students who enrolled online for MSU Extended University courses during the last two years. The data in question was encrypted, and there is no evidence that personal information was stolen.

Information Source: Dataloss DB

October 12, 2007, King County Transportation Department
Seattle, Washington
GOV PORT 1,400
A laptop computer containing personal information about current and former employees has been stolen. Workers' names, addresses and Social Security numbers were on the password-protected laptop, which was stolen during a Sept. 28 home burglary. The information was not encrypted.

Information Source: Dataloss DB

October 12, 2007, Track Data Securities Corp.
New York, New York
BSF HACK 276
Track Data learned that the security of its computer system was compromised. Customer names, Social Security numbers, addresses and credit card numbers may have been illegally accessed. At least 276 New Hampshire residents were affected, but the total number of affected customers nationwide was not reported.

Information Source: Dataloss DB

October 12, 2007, LPL Financial
San Diego, California
BSF HACK 40
Unauthorized individuals accessed LPL's trading and operation system data by obtaining passwords of eight financial advisors. LPL discovered the breach on July 17 and immediately informed law enforcement officials. It appears that the purchases were made to increase the volume of trading and affect prices of certain stocks. The trades were rejected once it was determined that they were fraudulent. Client names, Social Security numbers, dates of birth, addresses, phone numbers and account numbers may have been exposed.

Information Source: Dataloss DB

October 10, 2007, Wheels Inc., Pfizer
Des Plaines, Illinois
BSO DISC 1,800 + 23 Not included in Total because it is not clear if SSNs were exposed.
The spouses and domestic partners of about 1,800 Pfizer employees, including 23 from Connecticut, learned late last month about a data breach at Wheels Inc., which provides cars to the company, mostly for use by its sales force. The breach at Wheels, first reported by the Pharmalot Web site, released onto the Internet names, addresses, birth dates and driver's license numbers, but not Social Security numbers, according to the company.

Information Source: Dataloss DB

October 10, 2007, Commerce Bank
Wichita, Kansas
BSF HACK 20
A hacker gained access to a database with about 3,000 customer records and accessed data belonging to 20 of them. The bank is contacting those who may have been affected. The hacking was quickly detected and stopped, according to Commerce Bank, which then notified law enforcement.

Information Source: Dataloss DB
Personal information on anyone who worked or volunteered for the Pembroke schools in the last four years was accessible via the Internet because of a weakness in the district's computer system. The information included names, birth dates and Social Security numbers.

Information Source:
Dataloss DB

A laptop computer was stolen from a former teaching assistant. The theft of the computer, which occurred last month in a break-in of the instructor's home, contained class records such as attendance, test scores, and grades of students who took his philosophy courses at the UI between 2002 and 2006. Social Security numbers were also present in 100 of the records.

Information Source:
Dataloss DB

Two laptops were stolen from the office of a computer science professor. Both of the computers were believed to have contained significant personal identifying data, such as Social Security numbers.

Information Source:
Dataloss DB

A laptop computer and other personal belongings were stolen from one of Semtech's vendors. The computer was not stolen from a Semtech facility, but may have contained computerized data relating to Semtech employees. Semtech declined to provide further details of the incident, such as what personal employee data may have been put at risk, when the theft happened or how long it took the company to inform its workers of the potential breach.

Information Source:
Dataloss DB

A laptop was stolen from an employee during travel. The information on the laptop included names, tax ID numbers, Social Security numbers and other personal information of NFP's vendors.

Information Source:
Dataloss DB

Social Security numbers of about 450,000 licensed professionals were inadvertently released. The information was mailed last month to agencies that submitted a public records request for the names and addresses of professionals licensed by the division. The division mailed 28 computer disks to 23 agencies that use the information as a marketing or promotional tool. The disks would normally contain only the names and addresses of individuals licensed through the Division of Professional Licensure and the Division of Health Professions Licensure. However, the disks also included Social Security numbers.

Information Source:
Dataloss DB

A laptop was stolen from the car of a claims representative. It contained the names, Social Security numbers and driver's license numbers of clients.
October 2, 2007  The Nature Conservancy  Arlington, Virginia  

Additional locations: Little Rock, Fayetteville, Arkadelphia, Batesville and Ponca, (Arkansas)

A hacker illegally gained access to a computer of The Nature Conservancy containing personal information on current and former employees and their dependents. The stolen information included the names, home addresses, Social Security numbers and birth dates. It also included direct deposit bank account numbers for employees who were on the payroll between 2000 and 2004, as well as the Social Security numbers of those employees’ dependents. When employees accessed a particular Web site, the site planted a program on the employees’ computers that copied the contents of the hard drives and sent the information to the hacker.

October 2, 2007  Athens Regional Health Services  Athens, Georgia  

A computer missing from a Regional First Care clinic in Watkinsville held the personal information of more than 1,400 people, according to Athens Regional Health Services. Workers first noticed on Sept. 24 that the computer was missing. The computer held Social Security numbers for 85 people, some health information for 545 people and the name, address and/or telephone numbers of 811 people. No credit card or other financial information was stored on the computer, which was a backup server for the Watkinsville clinic.

October 1, 2007  PFPC Inc., AFBA  Alexandria, Virginia  

On July 17, a laptop was stolen from the vehicle of a contractor working on an information technology project. A file on the laptop contained AFBA 5 Star Fund shareholder information. Names, Social Security numbers and addresses were exposed. At least 60 Maine residents were affected, but the total number of affected individuals nationwide was not revealed.

September 28, 2007  Gap Inc.  San Francisco, California  

A laptop containing the personal information of certain job applicants was recently stolen from the offices of an experienced third-party vendor that manages job applicant data for Gap Inc. Personal data for approximately 800,000 people who applied online or by phone for store positions at one of Gap Inc.’s brands between July 2006 and June 2007 was contained on the stolen laptop. Social Security numbers were included in the information on the laptop.

UPDATE (5/28/10): A man whose Social Security number and other personal information were compromised by a company that processed his job application for The Gap Inc. has no legal claims against the company because no actual damage resulted from the privacy breach (a laptop stolen from Vangent), ruled the Ninth Circuit Court of Appeals. Ruiz v. Gap, Inc. 09-15971 (9th Circ. May 28, 2010), http://www.ca9.uscourts.gov/datastore/memoranda/2010/05/28/09-15971.pdf.

September 28, 2007  Pfizer  New York, New York  

An employee wrongfully arranged to have copies made of confidential information in electronic format and did not return the information upon termination. The information included names and Social Security numbers of current and former Pfizer associates. The incident occurred on July 17 and was discovered on August 18. The company said it would notify affected individuals by October 15.

September 28, 2007  Wal-Mart Stores Inc.  Bentonville, Arkansas  

UPDATE (5/28/10): A man whose Social Security number and other personal information were compromised by a company that processed his job application for The Gap Inc. has no legal claims against the company because no actual damage resulted from the privacy breach (a laptop stolen from Vangent), ruled the Ninth Circuit Court of Appeals. Ruiz v. Gap, Inc. 09-15971 (9th Circ. May 28, 2010), http://www.ca9.uscourts.gov/datastore/memoranda/2010/05/28/09-15971.pdf.
A Wal-Mart associate took confidential information relating to a group of associates. The former associate was not authorized to retain the information after ending his employment with Wal-Mart. Associate names, Social Security numbers, Wal-Mart job codes and compensation information were exposed. The incident occurred on August 15.

Information
Source: Dataloss DB
September 27, 2007 Kelley Drye and Warren LLP Washington, District Of Columbia

A laptop was stolen from an external pension auditor on September 12. It contained information related to Kelley's Retirement Savings Plan. This information included names, Social Security numbers, dates of birth, addresses, and/or date of employment.

Information
Source: Dataloss DB
September 25, 2007 Merlin Information Services Kalispell, Montana

The login information of a legitimate customer was compromised and an unauthorized individual may have accessed names, Social Security numbers and addresses of certain persons.

Information
Source: Dataloss DB
September 24, 2007 Utah Department of Workforce Services American Fork, Utah

A laptop computer containing a spreadsheet with the Social Security numbers and other personal information of about 2,000 people was reported stolen.

Information
Source: Dataloss DB
September 24, 2007 Fidelity National Information Services, Fidelity National Financial Jacksonville, Florida

A laptop was stolen from an employee on August 28. The laptop contained payroll information such as name, Social Security number, address, email address and date of birth. At least 74 Maine and 37 New Hampshire residents were affected, but the total number of individuals affected nationwide was not revealed.

Information
Source: Dataloss DB
September 21, 2007 City of Columbus, Ohio Columbus, Ohio

For Info: The Columbus Dispatch, http://www.dispatch.com

The city of Columbus is offering identity-theft protection services to more than 3,000 people whose Social Security numbers were on three computers stolen from a warehouse. The theft affected people who had signed up for the city’s Mobile Tool Library, which lends power tools, lawn mowers and supplies.

Information
Source: Dataloss DB
September 21, 2007 Citigroup, ABN Amro Mortgage Group Norridge, Illinois

Three spreadsheets containing 5,200 Social Security numbers and other personal details about customers were inadvertently leaked over an online file-sharing network by a former employee. Tiversa, a company that monitors P2P networks, found Excel spreadsheets from the desktop of a financial analyst at ABN Amro Mortgage Group running LimeWire. Although Tiversa found over 10,000 files, deduplication revealed only 5,208 unique Social Security numbers, along with names and what type of mortgage each customer had.

Information
Source: Media

A backup tape was stolen in Ohio in June and contained data removed by Accenture from the state's Core-CT computer system, which performs all of the state's payroll, personnel, purchasing, accounting and inventory functions. The backup tape contained state agency bank account numbers, bank names and types of accounts, as well as the names and Social Security numbers of over 663 state employees.
Security numbers of 58 of Connecticut taxpayers. Connecticut officials today revealed plans to file a civil complaint against IT consulting giant Accenture Ltd. related to this security breach involving stolen records tied to state agency bank accounts worth millions of dollars.

**Information Source**
**September 19, 2007**
**Kansas University**
**Lawrence, Kansas**

A number of documents containing Kansas University student, faculty and staff personal information were recovered from the recycling and trash in the Mathematics Department at Kansas University. The information included student exams, student change of grade forms, class rosters, copies of health insurance cards, copies of immigration forms as well as a copy of a Social Security card.

**Information Source**
**September 19, 2007**
**University of Michigan School of Nursing**
**Ann Arbor, Michigan**

Backup tapes containing patient information like Social Security numbers, patient names and addresses were stolen from the School of Nursing two weeks ago.

**Information Source**
**September 14, 2007**
**TD Ameritrade Holding Corp.**
**Omaha, Nebraska**

One of TD Ameritrade’s databases was hacked and contact information for its more than 6.3 million customers was stolen. A spokeswoman for the Omaha-based company said more sensitive information in the same database, including Social Security numbers and account numbers, does not appear to have been taken. “We were able to conclude that while Social Security numbers are stored in this particular database, your SSN were not retrieved.” The company said names, email addresses, phone numbers, and home addresses were taken in the data breach. Company customers received unwanted spam because of this breach.

**UPDATE** (4/28/09): TD Ameritrade sent a mass email on September 14, 2007 to its customers admitting SSNs had been compromised: “[W]e recently discovered and eliminated unauthorized code from our systems. This code allowed certain client information stored in one of our databases … to be retrieved by an external source [and] Social Security Numbers are stored in this particular database.”

**UPDATE** (10/27/09): TD Ameritrade was nearing a settlement in the case of more than six million stolen records when the judge, who previously seemed to agree with the proposal, rejected it today. The federal judge handling the case has decided the proposed settlement provides no discernible benefit to the victims and he rejected the proposed settlement.

**UPDATE** (11/16/10): Pending approval by a U.S. District Judge, TD Ameritrade will offer between $0 and $2,500 to customers who were affected by the breach. Customers who received spam, or were victims of criminal identity theft because a criminal who was arrested posed as them, will get $0 unless they were also victims of account-fraud-based identity theft. This settlement will cost between $2,500,000 and $6,500,000.

**http://www.citizen.org/litigation/forms/cases/getlinkforcase.cfm?cID=499**

**http://www.bargaineering.com/articles/td-ameritrade-discovers-database-breach.html**

**Information Source**
**September 14, 2007**
**Tennessee Tech University**
**Cookeville, Tennessee**

Some 3,100 current or past students who owe the university money were notified today that some of their personal data may have been compromised. A technical problem in the way student bills are printed resulted in the chance that some student social security numbers and personal identification numbers may have been sent to another student’s address.

**Information Source**
**September 14, 2007**
**Cornell University**
**Ithaca, New York**

A desktop computer was stolen from the East wing of Ives Hall in the School of Industrial and Labor Relations. It contained the names, Social Security numbers and dates of birth of some individuals.
The Voxant online ecommerce store server was hacked using what appeared to be a typical phishing scheme. The server is separate from the primary business at www.voxant.com. The affected server was immediately taken offline and removed the offending phishing pages. Encrypted credit card numbers could have been accessed during the incident. Although the credit card numbers were encrypted, the encryption key was not well protected. The database up through June 19-20 could have been affected, representing approximately 4,500 US customers.

To sign up for the free ID theft protection you must call AmeriChoice at (800) 690-1606.

Activity from a third party was detected on the website. It is likely that the third party used customer Social Security numbers, dates of birth and annuity contract numbers to access the website. The third party may have been able to reset customer PINs and access customer accounts with this information.

Somebody either lost or stole a computer potentially containing the credit card information of anyone who has shopped at the Greensburg store since it first opened more than five years ago. Gander Mountain said credit card information for 112,000 customers of its Greensburg store might have been compromised. That includes 10,000 records with names, card numbers and expiration dates.

The university is warning those who were students in the fall of 2004 that information about them was inadvertently posted on the Internet. The information was in a document that contained the names and Social Security numbers of students in the Animal Sciences 102 class. The page was no longer in use but was on a computer server connected to the Internet. The document was found recently through an internal search and reported to the chief information security officer at Purdue.
A laptop was stolen from a Larson Allen employee. It contained a spreadsheet with the personal information of FirstHealth’s employees. The information included the names, Social Security numbers, dates of birth, addresses and employment information of people on payroll during August.

Information Source: Dataloss DB

September 9, 2007  De Anza College  Cupertino, California

EDU PORT 4,375

(408) 864-8292

Thousands of former students might be at risk for identity fraud after an instructor’s laptop computer, containing students’ personal information, was stolen last month. The computer contained the students’ names, addresses, grades and in many cases Social Security numbers.

Information Source: Dataloss DB

September 9, 2007  McKesson Specialty, AstraZeneca  Scottsdale, Arizona

MED STAT 68,779

(866) 554-6366

McKesson Health-care services company, is alerting thousands of its patients that their personal information is at risk after two of its computers were stolen from an office.

Information Source: Dataloss DB

September 6, 2007  University of South Carolina  Columbia, South Carolina

EDU DISC 1,482

A number of files containing Social Security numbers, test scores and course grades were exposed online. It appears the person responsible for the breach may not have known enough about computers to realize the information could be accessed outside the university system.

Information Source: Dataloss DB

September 5, 2007  Affiliated Computer Services (ACS), Kraft Foods  Northfield, Illinois

BSR PORT 1446

A computer tape with the names and Social Security numbers of current and former Kraft employees was lost by ACS. ACS administers Kraft’s prescription drug benefits program. ACS believes it accidentally destroyed the tape. Kraft reported the number of affected residents in North Carolina, New Hampshire, Maine and New York, but the total number nationwide was not reported and is likely to exceed 1446.

Information Source: Dataloss DB

September 4, 2007  Pfizer  New York, New York

BSO INSD 34,000

(866) 274-3891

A security breach may have caused employees’ names, Social Security numbers, addresses, dates of birth, phone numbers, bank account numbers, credit card information, signatures and other personal information to be publicly exposed. The breach occurred late last year when a Pfizer employee removed copies of confidential information from a Pfizer computer system without the company’s knowledge or approval. Pfizer didn’t become aware of the breach until July 10.

Information Source: Dataloss DB

September 4, 2007  Brevard Public Schools  Viera, Florida

EDU UNKN 61

A missing piece of luggage belonging to a state auditor contains the personal information of 61 Brevard Public Schools employees and had district personnel scrambling before the holiday weekend began to notify people that their names and Social Security numbers might be compromised.

UPDATE (9/21/07): Melbourne International Airport police arrested a 44-year-old defense subcontractor from California on charges of stealing luggage. He is in the Brevard County jail, facing at least two charges of grand theft.

Information Source: Dataloss DB

September 4, 2007  Brevard Public Schools  Viera, Florida

EDU UNKN 61
Media

September 1, 2007  
Johns Hopkins Hospital  
Baltimore, Maryland  

A desktop computer containing the personal information of 5,783 Johns Hopkins Hospital patients was stolen. The computer included patients' names, Social Security numbers, birth dates and medical histories.

Information Source:  
Dataloss DB  

A desktop computer containing the personal information of 5,783 Johns Hopkins Hospital patients was stolen. The computer included patients' names, Social Security numbers, birth dates and medical histories.

Information Source:  
Dataloss DB  

August 31, 2007  
Option One Mortgage  
Irvine, California  

A computer server that contained customer service information was hacked. People who visited the customer service website between August 9 and 14 may have had their names, Social Security numbers, addresses, phone numbers, loan information and payment histories exposed. The hacker was able to change the website so that a virus was installed on the computers of visitors.

Information Source:  
Dataloss DB  

August 31, 2007  
Option One Mortgage  
Irvine, California  

A computer server that contained customer service information was hacked. People who visited the customer service website between August 9 and 14 may have had their names, Social Security numbers, addresses, phone numbers, loan information and payment histories exposed. The hacker was able to change the website so that a virus was installed on the computers of visitors.

Information Source:  
Dataloss DB  

A desktop computer containing the personal information of 5,783 Johns Hopkins Hospital patients was stolen. The computer included patients' names, Social Security numbers, birth dates and medical histories.

Information Source:  
Dataloss DB  

August 31, 2007  
AW Direct Inc.  
Berlin, Connecticut  

An unauthorized person accessed AW Direct's website. Customer order information that included full names, addresses and credit card information was exposed.

Information Source:  
Dataloss DB  

A desktop computer containing the personal information of 5,783 Johns Hopkins Hospital patients was stolen. The computer included patients' names, Social Security numbers, birth dates and medical histories.

Information Source:  
Dataloss DB  

August 31, 2007  
Voxant  
Reston, Virginia  

A hacker accessed the website and obtained personal information of customers.

Information Source:  
Dataloss DB  

August 30, 2007  
Maryland Department of the Environment  
Annapolis, Maryland  

A laptop computer containing personal information on people with state licenses has been stolen from a vehicle. It contains four databases that include personal information related to licenses issued by four state boards.

Information Source:  
Dataloss DB  

August 30, 2007  
Maryland Department of the Environment  
Annapolis, Maryland  

A laptop computer containing personal information on people with state licenses has been stolen from a vehicle. It contains four databases that include personal information related to licenses issued by four state boards.

Information Source:  
Dataloss DB  

August 30, 2007  
AT&T  
San Antonio, Texas  

A laptop containing unencrypted personal data on current and former employees of the former AT&T Corp. was stolen recently from the car of an employee of a professional services firm doing work for the company. That theft prompted the company to notify an unspecified number of individuals about the potential compromise of their Social Security numbers, names and other personal details.

Information Source:  
Media  

August 28, 2007  
Connecticut Department of Revenue Services  
Hartford, Connecticut  

A computer laptop with the names and Social Security numbers of more than 100,000 Connecticut taxpayers has been stolen. The Department of Revenue Services intends to launch a web page soon that residents can search to determine whether their personal information was stored on the laptop.

UPDATE (9/14/07): More than 2 dozen state laptops have gone missing since July 2006.

UPDATE (10/19/07): A supervisor at the state Department of Revenue Services was suspended without pay. His computer was stolen from his car in August at a hotel in New York. Police say it was possible the vehicle was not locked because there were no signs of a break-in.

Information Source:  
Dataloss DB  

5,247 Not added

667
An e-mail sent Aug. 24 to about 700 University of Illinois engineering students contained a spreadsheet listing personal information, including addresses and grade point averages, of thousands of students. The spreadsheet attached to the mass mail did not contain Social Security numbers or the students’ university identification numbers. But, the person who sent the mass e-mail attached a spreadsheet containing information on all 5,247 students in the College of Engineering. The spreadsheet included each student’s name, e-mail address, major, gender, race and ethnicity, class, date admitted, spring 2007 grade point average, cumulative GPA, plus local address and phone number.

Information
Source: Media

August 26, 2007 American Ex-Prisoners of War, Texas

Personal records including addresses and Social Security numbers of more than 35,000 veterans and their families were stolen this month from the offices of a POW support organization in Texas. Digital and paper records included information on the group’s entire membership, including addresses, dates of birth, Social Security numbers and VA claims data.

Information
Source: Dataloss DB

August 23, 2007 New York City Financial Information Services Agency

A laptop loaded with financial information on as many as 280,000 city retirees was stolen from a consultant who took the computer to a restaurant.

Information
Source: Dataloss DB

August 23, 2007 Loomis Chaffee School

Valuable computer equipment, including two large storage devices were stolen during a night time burglary from the locked IT facility on campus. The stolen storage devices contained information about some recent graduates of the school, including their names, Social Security numbers, and contact information from their days as students at the school.

Information
Source: Dataloss DB

August 23, 2007 Monster.com

Monster announced that the details of some 1.6 million job seekers had been stolen. Fewer than 5,000 of those 1.6 million users affected are based outside the United States. The information stolen was limited to names, addresses, phone numbers and email addresses, and no other details including bank account numbers were uploaded.

UPDATE (8/29/07): Hackers have stolen the names, e-mail addresses and telephone numbers of about 146,000 subscribers to USAJOBS.gov. The hackers accessed the information from the resume database run by Monster.com, which provides the technology for USAJOBS.gov. Monster Worldwide told OPM that no Social Security numbers were compromised.

Information
Source: Media

August 22, 2007 California Public Employees’ Retirement System (CalPERS)

Roughly 445,000 retirees in California received brochures announcing an upcoming election to fill a rare vacancy on the board of the California Public Employees’ Retirement System. All or a portion of each person’s Social Security number appeared without hyphens on the address panel.
Five laptops were stolen from Printpack's corporate headquarters during a nighttime burglary on or around August 16. One laptop was taken from the finance department and had human resources information from current and former employees. Names, Social Security numbers, dates of birth, marital status, addresses and other information may have been exposed.

Boxes of documents containing personal information were supposed to be shredded but instead turned up last week in an off-base trash bin. Police do not believe anyone had access to the information other than the person who found the records. An investigation is under way to determine precisely what information they held and why they appeared off base.

Every barber and cosmetologist licensed in the state of West Virginia since 1986 could now potentially be a victim of identity theft. Someone broke into the second floor office of the Board of Barbers and Cosmetologists and stole a safe. The director of the agency says the safe contains the personal information of thousands of hair dressers.

A laptop computer has been stolen from an office in the Student Recreation Center that contained some student and employee names and Social Security numbers.

Four external computer hard drives used to back up information were discovered missing from a locked information technology workroom. The hard drives contained personal information about Celgene's current and former employees. Names, Social Security numbers, addresses, phone numbers, dates of birth, bank and financial accounts, compensation information and some driver's license numbers were on the hard drives.

A laptop was stolen from the car of an employee while it was in a parking lot on August 9. The laptop contained full names and Social Security numbers of employees. It is not clear if all 5,530 of Applera's employees were affected by the incident. At least 24 New Hampshire residents were affected.

A laptop belonging to an HP director was lost during a business trip to Atlanta, GA. The breach occurred in late July and involved the names, Social Security numbers, addresses, dates of birth, citizenship status and compensation information of Mercury Interactive employees. Mercury Interactive was acquired by HP in November of 2006.
An MS Excel spreadsheet containing names and Social Security numbers of graduate students at the University was posted within the University's website on or around April 17, 2007. Specifically, the spreadsheet contained the credit hour and tuition information associated with "inter-college" graduate programs. In addition to the credit hour and tuition information that were visible at the top of the spreadsheet, the bottom of the report also included the names and Social Security numbers of students. A staff member recognized the mistake on July 27.

**Information Source:** Dataloss DB

**August 16, 2007**
**Utica Title and Escrow**
**Bixby, Oklahoma**

Boxes belonging to Utica Title and Escrow had been stored at a storage unit in Bixby. When Utica quit paying rent the storage company went through the legal process to be able to sell everything left behind. No one wanted to buy the boxes of paper so the boxes were thrown out. The boxes contained private information, including Social Security numbers, bank accounts and pay stubs.

**Information Source:** Media

**August 16, 2007**
**Nationwide Mutual Insurance**
**Woodbury, New York**

A laptop was stolen from the car of a claims representative. It contained the names, Social Security numbers and driver's license numbers of clients.

**Information Source:** Dataloss DB

**August 15, 2007**
**Idaho Army National Guard**
**Boise, Idaho**

http://www.idahoarmyguard.org/, or call the Idaho National Guard Joint Operations Center

A small computer drive containing Social Security numbers and other personal information about every Army National Guard soldier in Idaho has been stolen.

**Information Source:** Dataloss DB

**August 15, 2007**
**Greater Detroit Hospital**
**Detroit, Michigan**

It's a repeat of a problem that emerged late last year at the Greater Detroit Hospital where metal thieves stripped everything from copper piping to windows, exposing rows of abandoned patient files. Neighbors said there are hundreds of boxes of patient files and payroll records inside, full of credit card and Social Security numbers.

**Information Source:** Media

**August 15, 2007**
**Sky Lakes Medical Center, Verus Inc.**
**Klamath Falls, Oregon**

The company that maintained the hospital's online bill payment system, transferred patient information from one server to another to perform maintenance but didn't take security measures, leaving information such as names, addresses and Social Security numbers exposed.

**Information Source:** Dataloss DB

**August 13, 2007**
**Pfizer, Axia Ltd.**
**New York, New York**

(866) 274-3891

Axia Ltd. had notified Pfizer on June 14 of an incident in which two Pfizer laptops were stolen from a locked car. The laptops, which disappeared May 31 in Boston, included the names and Social Security numbers of health-care professionals who were providing or considering providing contract services for Pfizer, according to the letter.

**Information Source:** Dataloss DB

**August 11, 2007**
**Providence Alaska Medical Center**
**Anhorage, Alaska**

**Information Source:** Dataloss DB
A laptop computer that contains the personal information of patients is missing. On the laptop there may be names, medical record numbers, dates of birth, patient diagnoses, Social Security numbers and addresses.

Information
Source: Dataloss DB

August 10, 2007 Loyola University
Chicago, Illinois

A computer with the Social Security numbers of 58 hundred students was discarded before its hard drive was erased, forcing the school to warn students about potential identity theft.

Information
Source: Dataloss DB

August 10, 2007 Legacy Health System
Portland, Oregon

(503) 445-9533

A primary care physician practice has discovered the theft of $13,000 in cash and personal data for patients. Patient receipts, credit card transaction slips and checks are also missing, in addition to Social Security numbers and dates of birth for patients. The investigation indicated it was a dishonest insider.

Information
Source: Dataloss DB

August 9, 2007 Citigroup
Stamford, Connecticut

A laptop was stolen from a third party vendor during an office burglary. The information on the laptop may have included customer names, Social Security numbers, addresses, telephone numbers and email addresses. The information was related to student loans, but did not include financial account information.

Information
Source: Dataloss DB

August 9, 2007 Penson Worldwide
Dallas, Texas

A person or persons breached Penson's computer network security systems on July 30. User logins, passwords, email addresses, security questions and answers were compromised.

Information
Source: Dataloss DB

August 8, 2007 Yale University
New Haven, Connecticut

Social Security numbers for over 10,000 current and former students, faculty and staff were compromised last month following the theft of two University computers.

Information
Source: Dataloss DB

August 7, 2007 Electronic Data Systems
Montgomery, Alabama

A former employee was arrested this week for allegedly trafficking in stolen identities she received through her work with the company. She obtained the names and identifying information of 498 Alabama Medicaid recipients and subsequently sold 50 of those identities.

Information
Source: Dataloss DB

August 7, 2007 Merrill Lynch
Hopewell, New Jersey

A computer device apparently was stolen containing sensitive personal information, including Social Security numbers, about some 33,000 employees.
August 7, 2007  Blue Cross Blue Shield North Carolina  Durham, North Carolina  BSF DISC  2,940

Letters were accidentally mailed with subscriber Social Security numbers visible through envelope windows.

Information Source: Dataloss DB  records from this breach used in our total: 2,940

August 6, 2007  Verisign  Mountain View, California  BSO PORT Unknown

A laptop containing extensive personal information on an undisclosed number of VeriSign employees was stolen from an employee's car. The information included names, addresses, Social Security numbers, dates of birth, telephone numbers, and salary records.

Information Source: Dataloss DB  records from this breach used in our total: 0

August 4, 2007  Kellogg Community Federal Credit Union  Battle Creek, Michigan  BSF STAT Unknown

A computer containing personal information on an undisclosed number members was stolen. A file containing some members' names, addresses, telephone numbers, birth dates, Social Security numbers and account numbers was on the computer's hard drive.

Information Source: Dataloss DB  records from this breach used in our total: 0

August 3, 2007  WorkCare Orem  Pleasant Grove, Utah  MED PHYS Unknown

A truck driver found medical documents containing personal information in his truck and on the ground while he picked up a load at a garbage transfer station. The documents contained names, addresses, telephone numbers, Social Security numbers and birth dates.

Information Source: Media  records from this breach used in our total: 0

August 3, 2007  Wabash Valley Correctional Facility  Indianapolis, Indiana  GOV DISC Unknown

A database containing Social Security numbers, dates of birth and names of people employed at the facility between 1997 and 2002 was unintentionally moved from a secure private drive that was accessible only by the human resources department to a shared directory that could be accessed by other employees here.

Information Source: Dataloss DB  records from this breach used in our total: 0

August 2, 2007  E.On - U.S. (energy services)  Louisville, Kentucky  BSO PORT Unknown

A laptop with names, Social Security numbers and birth dates of most E.On U.S. employees and some retirees was stolen last month.

Information Source: Dataloss DB  records from this breach used in our total: 0

August 2, 2007  University of Toledo  Toledo, Ohio  EDU STAT Unknown

(419) 530-4836, (419) 530-3661, (419) 530-1472

Two computers were stolen with hard drives containing student and staff Social Security numbers, names, and grade change information.

Information Source: Dataloss DB  records from this breach used in our total: 0

August 1, 2007  Lifetime Fitness  Dallas, Texas  GOV PHYS Unknown

Staff had discarded customer records in easily accessible trash cans behind Dallas businesses. Information that was discarded contained names, addresses, Social Security numbers, driver's license numbers and credit card information, as well as the date of birth of several children. Lifetime Fitness is based in Minnesota.
July 31, 2007  Textron
Providence, Rhode Island  BSF  PORT  500 (No SSNs or financial information reported)

An employee’s laptop was stolen. It contained employee information. At least 475 New Hampshire and 25 Maine residents were affected, but the total number of affected individuals was not revealed.

July 28, 2007  Yuba County Health and Human Services
Yuba County, California  MED  PORT  70,000

A laptop stolen from a building contained personally identifiable information of individuals whose cases were opened before May 2001. The laptop was being used as a backup system for the county’s computer system. The data include Social Security numbers, birth dates, driver’s license numbers and other private information.

July 27, 2007  City of Virginia Beach, Flexible Benefits Administrators
Virginia Beach, Virginia  GOV  INSD  2,000

A former employee allegedly stole Virginia Beach city and school district employees’ personal information and used it to commit prescription fraud. Police discovered a list of names and Social Security numbers at the employee’s home.

(917) 351-8763

City Harvest is currently investigating a potential improper access of systems that contained credit card information of their donors.

July 27, 2007  City Harvest
New York, New York  NGO  HACK  12,000

July 27, 2007  American Education Services, Vista Financial Inc
Harrisburg, Pennsylvania  BSF  PORT  5,000

Personal information was on a laptop stolen in a burglary at a subcontractor’s headquarters. The information, which was not encrypted, included names, addresses, phone numbers, e-mail addresses and Social Security numbers.

July 26, 2007  United States Marine Corps, Penn State University
Harrisburg, Pennsylvania  EDU  DISC  10,554

Data belonging to 10,554 Marines was “improperly posted” by Penn State University, according to the Marine Corps. Names and Social Security numbers of Marines could be found via Google search engine. Penn State University was under a research contract with the Marine Corps.

July 25, 2007  Hidalgo County Commissioner’s Office
Hidalgo County, Texas  GOV  DISC  25

The private medical information, including Social Security numbers and treatment details of people who sought medical assistance from the county was posted on the Hidalgo County Website.

Levington, Kentucky  GOV  PORT  2,718
The location listed is an ACS office. The location of the breach was not reported.

The luggage of an employee of ACS was stolen during airline travel. The bag contained a hard drive that may have included names, addresses, Social Security numbers and dates of birth. The information was obtained from the State of Delaware Court System.

**Information Source:** Dataloss DB

**July 24, 2007**  
**St. Vincent Hospital, Verus, Inc.**  
**Indianapolis, Indiana**  
**MED DISC 51,000**

Saint Vincent used subcontractor Verus Inc. to set up an online bill payment for patients. For a “brief” period of time, personal information was left unprotected and available online. The security lapse compromised names, addresses and Social Security numbers.

**Information Source:** Dataloss DB

**July 23, 2007**  
**Fox News**  
**Los Angeles, California**  
**BSO DISC 1.5 million**

Sensitive information was exposed on the Fox News web server. The security hole allowed hackers to access login information, names, phone numbers, and email addresses.

**Information Source:** Media

**July 21, 2007**  
**University of Michigan**  
**Ann Arbor, Michigan**  
**EDU HACK 5,500**

University databases were hacked. Names, addresses, Social Security numbers, birth dates, and in some cases, the school districts where former students were teaching were exposed.

**Information Source:** Dataloss DB

**July 20, 2007**  
**Science Applications International Corp. (SAIC)**  
**San Diego, California**  
**BSO DISC 867,000**


The Pentagon contractor may have compromised personal information. Information such as names, addresses, birth dates, Social Security numbers and health information about military personnel and their relatives were exposed when the data were not encrypted prior to being transmitted online.

**UPDATE (5/05/2012):** Though 580,000 households were reported, a total of 867,000 people may have been affected.

**Information Source:** Dataloss DB

**July 19, 2007**  
**Cricket Communications**  
**Omaha, Nebraska**  
**BSO PHYS 300**

Documents stolen from store result in loss of 300 credit card numbers.

**Information Source:** Dataloss DB

**July 19, 2007**  
**Jackson Local Schools**  
**Massillon, Ohio**  
**EDU DISC 1,800**

The Social Security numbers of present and former Jackson Local Schools’ employees were at risk of public access on a county maintained Web site.

**Information Source:** Dataloss DB

**July 18, 2007**  
**Purdue University**  
**West Lafayette, Indiana**  
**EDU DISC 50**
Files which were no longer in use were discovered on a computer server connected to the Internet. The files contained names and Social Security numbers of students who were enrolled in an industrial engineering course in spring 2002 or fall 2004.

**Information Source:** Dataloss DB  
**July 18, 2007**  
**Connecticut General Assembly Transportation Committee, L.G. Defelice**  
**Hartford, Connecticut**  
**GOV**  
**DISC**  
**300**  
Social Security numbers of former employees of defunct L.G. Defelice Inc. were posted on CT transportation committee website.

**Information Source:** Dataloss DB  
**July 17, 2007**  
**Western Union**  
**Greenwood Village, Colorado**  
**BSF**  
**HACK**  
**20,000**  
Credit card information and names were hacked from a database. The thieves got names, addresses, phone numbers and complete credit-card information.

**Information Source:** Dataloss DB  
**July 17, 2007**  
**Louisiana Board of Regents**  
**Baton Rouge, Louisiana**  
**GOV**  
**DISC**  
**80,000**  
Records of students and staff including Social Security numbers, names, and addresses exposed on web. In all, more than 80,000 names and Social Security numbers were accessible for perhaps as long as two years on an internal Internet site.

**Information Source:** Dataloss DB  
**July 17, 2007**  
**Kingston Technology Co.**  
**Fountain Valley, California**  
**BSO**  
**HACK**  
**27,000**  
A security breach may have compromised the names, addresses and credit card details of online customers. Kingston Technology is a computer memory vendor. The breach may have gone undetected for nearly 2 years.

**Information Source:** Dataloss DB  
**July 16, 2007**  
**Transportation Security Administration (TSA)**  
**Arlington, Virginia**  
**GOV**  
**PORT**  
**100,000**  
Authorities realized in May a storage device was missing from TSA headquarters. The drive contained historical payroll data, Social Security numbers, dates of birth, addresses, time and leave datas, bank account, routing information, and details about financial allotments and deductions.

**Information Source:** Media  
**July 16, 2007**  
**Intergraph Corporation**  
**Huntsville, Alabama**  
**BSR**  
**HACK**  
**Unknown**  
Confidential information about some transactions was accessed without authority by an unknown person or persons via the Internet. The information may have included name, address, and credit or debit card number and expiration date, in addition to shipping address and in some cases, a separate credit card address.

**Information Source:** Dataloss DB  
**July 15, 2007**  
**Westminster College**  
**Salt Lake City, Utah**  
**EDU**  
**DISC**  
**100**  
Names of students, former and current were printed in two files along with each student’s Social Security number. The files were on a student Web server used by Westminster students.

**Information Source:** Media  
**July 15, 2007**  
**City of Encinitas**  
**GOV**  
**DISC**  
**1,200**  
675
July 13, 2007  Encinitas, California  GOV  DISC  1,200

(760) 633-2788
Credit card or checking account information and addresses of people who had enrolled in Encinitas' youth recreation programs was inadvertently posted on the city's Web site.

Information Source: Dataloss DB

July 13, 2007  Metropolitan St. Louis Sewer District  St. Louis, Missouri  GOV  INSD  1,600

A employee had downloaded Social Security numbers of current or former district employees to a home computer. The Social Security numbers were part of a computer file the district uses to make sure workers get the proper pay.

Information Source: Dataloss DB

July 11, 2007  South County Hospital  South Kingstown, Rhode Island  MED  PHYS  79

Paperwork containing personal details from customers was left in a briefcase inside a car that was stolen. That batch of paperwork contained details including names, addresses, Social Security numbers, phone numbers and a summary of hospital accounts.

Information Source: Dataloss DB

July 11, 2007  Texas A&M University  Corpus Christi, Texas  EDU  PHYS  49

College of Business officials are investigating a faculty member for the misplacement of a business law class roster containing the names and Social Security numbers of students.

Information Source: Media

July 11, 2007  Disney Movie Club, Alta Resources, McNeil-PPC Inc  Neenah, Wisconsin  BSO  INSD  Unknown

A contract employee stole an unknown number of credit card numbers. Credit-card information was sold by an employee of a Disney contractor to a federal agent as part of an undercover sting operation.

Information Source: Dataloss DB

July 9, 2007  Girl Scouts Mile Hi  Denver, Colorado  NGO  PORT  Unknown

Tapes stolen from a car held personal information from a membership database, including names, addresses, phone numbers. A very limited number of credit card numbers and Social Security numbers were included in the stolen data from the camp and event registration database.

Information Source: Media

July 7, 2007  Cuyahoga County Dept. of Development  Cleveland, Ohio  GOV  PORT  3,000

Names and Social Security numbers on memory stick stolen in carjacking.

Information Source: Dataloss DB

July 5, 2007  Highland University  Las Vegas, New Mexico  EDU  UNKN  420

A building on the campus had been broken into, and the affected offices might have contained such personal information as Social Security numbers, credit card and bank account information.

Information Source: Dataloss DB

July 3, 2007  Fidelity National Information Services/Certegy Check Services Inc.  BSO  INSD  8,500,000

676
A worker at one of the company's subsidiaries (Certegy Check Services, Inc.) stole customer records containing credit card, bank account and other personal information.

**UPDATE (8/27/07):** The company first estimated that about 2.3 million records were affected but quickly boosted that number to 8.5 million in filings with the U.S. Securities and Exchange Commission. A California law firm has filed a class-action suit charging Fidelity National Information Services (FIS) and one of its subsidiaries with negligence in connection with a data breach.

**UPDATE (11/23/07):** A former database analyst at Certegy Check Services Inc., has agreed to enter a guilty plea to federal fraud and conspiracy charges in connection with the theft of data.

**UPDATE (7/7/08):** A new settlement provides that all class members whose personal or financial information was stolen can get compensated up to $20,000 if they were not reimbursed for certain identity theft losses caused by the data theft.

A worker at one of the company's subsidiaries (Certegy Check Services, Inc.) stole customer records containing credit card, bank account and other personal information.

**UPDATE (8/27/07):** The company first estimated that about 2.3 million records were affected but quickly boosted that number to 8.5 million in filings with the U.S. Securities and Exchange Commission. A California law firm has filed a class-action suit charging Fidelity National Information Services (FIS) and one of its subsidiaries with negligence in connection with a data breach.

**UPDATE (11/23/07):** A former database analyst at Certegy Check Services Inc., has agreed to enter a guilty plea to federal fraud and conspiracy charges in connection with the theft of data.

**UPDATE (7/7/08):** A new settlement provides that all class members whose personal or financial information was stolen can get compensated up to $20,000 if they were not reimbursed for certain identity theft losses caused by the data theft.


**UPDATE (4/26/10):** As part of a class action settlement in U.S. District Court in Tampa, consumers were given the opportunity to elect credit monitoring for one year or bank account monitoring for two years and were able to seek reimbursement of certain out-of-pocket costs incurred or identity theft expenses. Consumers also were able to request credit monitoring at the company’s expense immediately after the thefts were announced. The settlement with the Attorney General’s office ensures that Certegy will maintain a comprehensive information-security program. This program will assess internal and external risks to consumers’ personal information, implement safeguards to protect that consumer information, and will regularly monitor and test the effectiveness of those safeguards. Certegy and its related entities also agree to adhere to payment card industry data security standards as those standards continue to evolve. As part of the settlement, Certegy is donating $125,000 to the Attorney General’s Seniors vs. Crime Program for educational, investigative and crime prevention programs for the benefit of senior citizens and the community and will pay $850,000 for the state’s investigative costs and attorney’s fees related to the case.

**Information Source:** Dataloss DB

**June 29, 2007**

**Harrison County Schools**
**Charleston, West Virginia**

Several computers that contained the personal information, including Social Security numbers, of several Harrison County school employees were stolen. Workers Comp claims between January of 2001 and February of 2007 are at risk.

**Information Source:** Dataloss DB

**June 27, 2007**

**Milwaukee PC**
**Milwaukee, Wisconsin**

(414) 258-2275

Credit card information for 65,000 was possibly compromised. A service center noticed a file in their server and was concerned that file could contain customers' credit card numbers and personal information.

**Information Source:** Dataloss DB

**June 27, 2007**

**Bowling Green State University**
**Bowling Green, Ohio**

Lost storage device contained Social Security numbers, and names of 199 former students.

**Information Source:** Dataloss DB

**June 27, 2007**

**University of California, Davis**
**Davis, California**

deansoffice@vetmed.ucdavis.edu

Computer-security safeguards were breached. Compromised information included the applicants' names, birth dates and, in most cases, Social Security numbers.

**Information Source:** Dataloss DB

**June 25, 2007**

**Fresno County**
**Fresno, California**

(559) 453-6450

A disk containing information pertaining to thousands of home health-care workers -- including their names, addresses and Social Security numbers -- was lost when it was shipped to a software vendor's office in San Jose, CA.

**Information**
A former employee had the names, Social Security numbers, dates of birth and addresses of about 127 members. The employee is believed to have participated in fraudulent activity and may have accessed approximately 17,000 members' information during the final 2 1/2 years of his or her employment.

Pharmacy documents were found behind a closed Winn-Dixie grocery store, containing telephone numbers, Social Security numbers and addresses of thousands of individuals. Apparently when the grocery store/pharmacy closed, employees put bundles of documents outside to be picked up. However, they were never retrieved.

Information such as account numbers, Social Security numbers, names and addresses may have been stored on a stolen laptop computer during a car theft in Dallas.

Personal information including Social Security numbers of pilots and other employees at American Airlines, including the chief executive, was exposed on a company Web site.

A parent says his son should never have received bills in the mail for a pre-employment drug screening visit. Additionally, he received information about 17 others who were also tested, including Social Security numbers.

Investigation by The Smoking Gun Web site said that by changing a few characters on the web page URL it was possible to see the subscriber's name, email address, password, phone number, mailing address and credit card number.

A local newspaper employee gained unauthorized access to the Shamokin Area School District's computer database. It is the same system that stores students' personal information, including Social Security numbers. That newspaper employee brought the security flaw to the attention of school officials.

A professor vacationing off the coast of Africa took data with him on a small computer storage device which was lost or stolen. It is thought to contains SSNs and dates of birth for students enrolled in the spring, summer and fall semesters of 2006.
June 15, 2007 Ohio state workers Columbus, Ohio

GOV PORT 1,000,000

(888) 644-6648(taped-message), (877) 742-5622 (Ohio Consumers' Counsel) or (800) 267-4474

A backup computer storage device with the names and Social Security numbers of every state worker was stolen out of a state intern's car. The tape, which was stolen in June, contains personally identifiable information of nearly 84,000 current and former Ohio state employees and more than 47,000 state taxpayers.

UPDATE (6/20/07) : The storage device also had the names and Social Security numbers of 225,000 taxpayers.

UPDATE (6/22/07) : Previous news stories reported smaller amounts, but the most recent news story shows 500,000.

UPDATE (7/12/07) The State of Ohio increased the data theft estimation to one million.

June 14, 2007 Division of Workforce Services Salt Lake City, Utah

GOV UNKN 20,000

(801) 281-1267

Children's Social Security numbers are believed to have been compromised by identity thieves.

June 14, 2007 Hamburger Hamlet Restaurant Los Angeles, California

BSO INSD 40

Former waitress made off with the credit or debit card numbers of at least half a dozen patrons - and possibly as many as 40. Already, about $16,300 in unauthorized charges have been linked to the scam.

June 14, 2007 Georgia Tech University Atlanta, Georgia

EDU DISC

An electronic file containing the personal information of current and former Georgia Tech students was exposed briefly.

June 14, 2007 Lynchburg City Lynchburg, Virginia

GOV DISC

Personal information of Lynchburg city employees and retirees was accidentally posted on the city's website among that information employee's prescription medications.

June 11, 2007 Pfizer New York, New York

BSO DISC 17,000

866-274-3891

Installation of certain file sharing software on a Pfizer laptop, exposed files containing names, Social Security numbers, addresses and bonus information of present and former Pfizer colleagues. Investigation revealed that certain files containing data were accessed and copied.
A flash drive containing confidential information was stolen. Social Security numbers of current and former students were on the flash drive, stolen from the English department.

Information
Source: Dataloss DB
June 11, 2007
Grand Valley State University
Allendale, Michigan
EDU PORT 3,000

Jann Joseph (616) 331-2110

A flash drive containing confidential information was stolen. Social Security numbers of current and former students were on the flash drive, stolen from the English department.

Information
Source: Dataloss DB
June 9, 2007
Concord Hospital, Verus Inc.
Concord, New Hampshire
MED DISC 9,297

Contact mhanna@cmonitor.com for more information.

Patient names, addresses, dates of birth and Social Security numbers were exposed on the internet for a period of time. A subcontractor names Verus that handles Concord's online billing was responsible for the breach.

UPDATE (6/20/07): The Washington-based company that managed Concord's online billing system was fired. Hospital officials now are asking for an audit to verify that Verus Incorporated has removed all of its patient information from its servers.

Information
Source: Dataloss DB
June 9, 2007
Verus Inc., Concord Hospital
Concord, New Hampshire
MED DISC 9,297

Patient names, addresses, Social Security numbers and dates of birth were unprotected on the Internet. A subcontractor named Verus that handles Concord's online billing was responsible for the breach.

Information
Source: Dataloss DB
June 8, 2007
University of Virginia
Charlottesville, Virginia
EDU HACK 5,735

http://www.virginia.edu/uvatoday/newsRelease.php?id=2217, identity-assistance@virginia.edu, (866) 621-5948

A breach in one of the computer applications resulted in exposure of sensitive information belonging to current and former U.Va. faculty members. The information included names, Social Security numbers and dates of birth. The investigation has revealed that on 54 separate days between May 20, 2005, and April 19, 2007, hackers tapped into the records of 5,735 faculty members.

Information
Source: Dataloss DB
June 8, 2007
University of Iowa
Iowa City, Iowa
EDU HACK 1,100

Social Security numbers of faculty, students and prospective students were stored on the Web database program that was compromised.

Information
Source: Dataloss DB
June 6, 2007
Cedarburg High School
Cedarburg, Wisconsin
EDU DISC Unknown

Students obtained names, addresses and Social Security numbers and might have accessed personal bank account information of current and former district employees.

Information
Source: Dataloss DB
June 6, 2007
Dearfield Medical Building
Greenwich, Connecticut
MED PHYS Unknown

A box was discovered at inside a trash bin in May and contains information about lab tests and insurance approvals as well as other medical issues, documents are not medical charts, but do contain patient names and contact information.
June 5, 2007  vFinance Investments Inc.  
Boca Raton, Florida  

A database that contained customer information was accessed through the [www.vfinance.com](http://www.vfinance.com) website by an unauthorized person. The goal of the attack seems to have been to deface the website.

**Information Source:**  Dataloss DB

June 4, 2007  Stevens Hospital  
Edmonds, Washington  

(425) 673-3745

Personal information including names, addresses, and Social Security numbers were exposed online due to a lapse in the data security procedures by a subcontractor. An Internet search engine was able to access the information while the subcontractor’s laptop was unsecured.

**Information Source:**  Dataloss DB

June 4, 2007  GFK NOP LLC  
New York, New York  

An employee’s laptop was stolen from her car on May 29. A payroll-related Excel file that contained the names, Social Security numbers, dates of birth, state of residence and base rate of pay for employees.

**Information Source:**  Dataloss DB

June 3, 2007  Gadsden State Community College  
College Gadsden, Alabama  

Students who took an Art Appreciation class at the Ayers Campus between 2005 and 2006 had their names, grades and Social Security numbers scattered across a local business’ driveway.

**Information Source:**  Dataloss DB

June 1, 2007  Fresno County, Refined Technologies Inc., DHL  
Fresno, California  

A missing computer disk contains names, addresses and Social Security numbers. The County sent it by courier to a software vendor’s office in San Jose to determine workers’ eligibility for health care benefits. The software company, Refined Technologies Inc., said they never received the disk. The courier service, DHL, told County officials that the file was delivered May 10, though the County didn’t require anyone to sign for the delivery.

**Information Source:**  Dataloss DB

June 1, 2007  Jax Federal Credit Union  
Jacksonville, Florida  

Social Security numbers and account numbers of clients were accidentally posted on the Internet, then indexed by Google. JFCU was transmitting information to a printer for a preapproved auto loan mailing when the information was picked up by Google from the printer’s Web site. JFCU normally transmits information on an encrypted disk delivered by courier, but when the printer couldn’t open the disk, the information was sent again, but wasn’t encrypted and included Social Security numbers and account numbers.

**Information Source:**  Dataloss DB

June 1, 2007  Northwestern University  
Evanston, Illinois  

c-loebbaka@northwestern.edu

Files containing personal information of students and applicants were available online.

**Information Source:**  Dataloss DB

June 1, 2007  JAX Federal Credit Union  
Jacksonville, Florida  

Auto loan mailing list information that was being transmitted to a printer was picked up by Google through the printer’s
website. Social Security numbers and account numbers were exposed. The information was supposed to be encrypted.

Information Source: Dataloss DB
May 31, 2007  Priority One Credit Union  South Pasadena, California

Priority One Credit Union sent out election ballots to members with Social Security numbers and account numbers printed on the outside of the envelopes.

Information Source: Dataloss DB
May 30, 2007  OfficeTeam  Manchester, New Hampshire

A staffing professional from OfficeTeam sent an email to individuals. The email included the email addresses and Social Security numbers of all the recipients of the email. At least 237 New Hampshire residents were affected by the incident, but the total number of individuals affected nationwide was not reported.

Information Source: Dataloss DB
May 29, 2007  Mytreo.net  Sunnyvale, California

The location listed is the headquarters of Palm Inc. Mytreo.com is a division of Palm.

Mytreo.net store customers may have had their personal information compromised. An individual may have viewed names, Social Security numbers, addresses and encrypted credit card information. The criminal had not been caught at the time of the report, and their method for accessing customer information was not revealed.

Information Source: Dataloss DB
May 26, 2007  Cover Tennessee  Nashville, Tennessee

A computer error at the Cover Tennessee health insurance program caused small business owners who chose not to print out their forms from the Web site to have their personal information including Social Security numbers added to the next user’s printout request.

Information Source: Dataloss DB
May 25, 2007  North Carolina Department of Transportation  Raleigh, North Carolina


A computer server used to back up employee identification badge records that included the names and Social Security numbers of NCDOT employees, contractors and other state employees was compromised.

Information Source: Dataloss DB
May 25, 2007  Booker T. Washington Community Center  Auburn, New York

A laptop computer with personal information of individuals who applied for Family Health Plus or Child Health Plus state health insurance program benefits was recovered when a woman tried to sell it at a pawn shop.

Information Source: Media
May 24, 2007  Beacon Medical Services  Aurora, Colorado

Private medical and financial information including patient records from at least 10 Colorado clinics and hospitals, and one hospital in Peoria, Illinois that should have been only accessible through VPN access were inadvertently available on the Internet.
May 24, 2007  Home Depot
Atlanta, Georgia  BSR  PORT  204

A consultant’s laptop was stolen. It contained the names and Social Security numbers of Home Depot associates.

Information
Source:  Dataloss DB

May 23, 2007  Mountain Xpress (Greenline Media Inc.)
Asheville, North Carolina  BSO  HACK  6,540

Someone launched a dictionary attack on the email server. The hacker obtained a user name and password that allowed access to an internal database that stored credit card numbers.

Information
Source:  Dataloss DB

May 23, 2007  Waco Independent School District
Waco, Texas  EDU  HACK  17,400

Two high school seniors recently hacked into the district’s computer network potentially compromising the personal information including Social Security numbers of students and employees.

Information
Source:  Dataloss DB

May 23, 2007  Check into Cash
Champaign, Illinois  BSF  PHYS  Unknown

Consumer loan documents and related reports were found in a trash bin behind the shopping center where Check into Cash is located. Documents contained Social Security numbers, addresses, copies of driver’s licenses and other personal information of the company’s customers.

Information
Source:  Dataloss DB

May 22, 2007  University of Pittsburgh Medical Center
Pittsburgh, Pennsylvania  MED  DISC  6,000

UPMC mailed a fundraising letter to 6,000 former patients on May 7. The donor response cards inadvertently included each individual’s SSN in the tracking code, visible through the envelope window.

Information
Source:  Dataloss DB

May 22, 2007  University of Colorado, Boulder
Boulder, Colorado  EDU  HACK  45,000

Hotline: (303) 492-1655

A hacker launched a worm that attacked a University computer server used by the College of Arts and Sciences. Information for 45,000 students enrolled at UC-B from 2002 to the present was exposed, including SSNs. The breach was discovered May 12. Apparently anti-virus software had not been properly configured.

Information
Source:  Dataloss DB

May 21, 2007  Columbia Bank
Fair Lawn, New Jersey  BSF  HACK  Unknown

Columbia Bank notified its online banking customers of a hacking incident. Names and SSNs were accessed, but account numbers and passwords were not.

Information
Source:  Dataloss DB

May 20, 2007  Northwestern University
Chicago, Illinois  EDU  PORT  Unknown

A laptop belonging to the financial aid office was stolen. It contained SSNs and other information of some alumni.

Information
Source:  Dataloss DB

May 19, 2007  Texas Commission on Law Enforcement Standards and Education
  GOV  PORT  230,000
A laptop computer was stolen from the state agency that licenses police officers. It contained information on every licensed peace officer in Texas, including SSNs, driver’s license numbers, and birth dates.

**Information**

**Source:** Dataloss DB

**May 19, 2007**

**Illinois Dept. of Financial and Professional Regulation**

Chicago, Illinois

GOV HACK 300,000

For information about breach [www.idfpr.com](http://www.idfpr.com)

A computer server in the office of the Illinois Dept. of Financial and Professional Regulation was breached earlier this year. SSNs, tax numbers, and addresses of banking and real estate licensees and applicants were exposed. The hacking incident was discovered May 3.

**Information**

**Source:** Dataloss DB

**May 19, 2007**

**Stony Brook University**

Stony Brook, New York

EDU DISC 90,000

[http://www.stonybrook.edu/sb/disclosure/](http://www.stonybrook.edu/sb/disclosure/), Call Center, (866) 645-5830 (available until July 15, 2007)

SSNs and university ID numbers of faculty, staff, students, alumni, and other community members were visible via the Google search engine after they were posted to a Health Sciences Library Web server April 11. It was discovered and removed 2 weeks later.

**Information**

**Source:** Dataloss DB

**May 18, 2007**

**Alcatel-Lucent**

Murray Hill, New Jersey

BSO PORT Unknown

The telecom and networking equipment maker notified employees that a computer disk containing personal information was lost in transit to Aon Corp., another vendor. It contained names, addresses, SSNs, birth dates, and salary information of current and former employees.

**Information**

**Source:** Dataloss DB

**May 18, 2007**

**Yuma Elementary School District No. 1**

Yuma, Arizona

EDU PHYS 91

SSNs of 91 substitute teachers were stolen May 7 when a district employee’s car was broken into and a brief case was taken containing payroll reports. The reports did not include bank account information.

**Information**

**Source:** Dataloss DB

**May 18, 2007**

**Indianapolis Public Schools**

Indianapolis, Indiana

EDU DISC 7,500 (No SSNs or financial information reported)

A local newspaper reporter discovered that sensitive personal information was accessible online, including employee performance reviews, student grade books, student special education needs, and essays.

**Information**

**Source:** Dataloss DB

**May 17, 2007**

**Georgia Division of Public Health**

Atlanta, Georgia

GOV HACK 140,000

The GA Dept. of Human Resources notified parents of infants born between 4/1/06 and 3/16/07 that paper records containing parents’ SSNs and medical histories -- but not names or addresses -- were discarded without shredding.

**Information**

**Source:** Dataloss DB

**May 15, 2007**

**IBM**

Armonk, New York

BSO PORT 2226

An unnamed IBM vendor lost computer tapes containing information on IBM employees -- mostly ex-workers -- including
SSNs, dates of birth, and addresses. They went missing in transit from a contractor's vehicle. At least 1468 New Hampshire and 758 Maine residents were affected, but the total number of affected individuals nationwide was not revealed.

**Information Source:** Dataloss DB

**Community College of Southern Nevada**  
**North Las Vegas, Nevada**  
**EDU Hack**  
**197,000**

A virus attacked a computer server and could have allowed a hacker to access students' personal information including names, Social Security numbers and dates of birth, but the school is not certain whether anything was actually stolen from the school's computer system.

**Information Source:** Dataloss DB

**Goshen College**  
**Goshen, Indiana**  
**EDU Hack**  
**7,300**

A hacker accessed a college computer that contained the names, addresses, birth dates, Social Security numbers and phone numbers of students and information on some parents with the suspected motivation of using the system to send spam e-mails.

**Information Source:** Dataloss DB

**University of California, Irvine Medical Center**  
**Irvine, California**  
**MED Phys**  
**287**

About 1,600 file boxes stored in an off-site university warehouse were discovered missing. Some of the files included patients' names, addresses, Social Security numbers and medical record numbers.

**Information Source:** Media

**Highland Hospital (Rochester, NY)**  
**Rochester, New York**  
**MED Port**  
**13,000**

Two laptop computers, one containing patient information including Social Security numbers, were stolen from a business office. The computers were sold on eBay, and the one containing personal information was recovered.

**Information Source:** Dataloss DB

**Student Loan Funding Resources, The Art Institute of California**  
**San Diego, California**  
**BSF Hack**  
**Unknown**

A breach on the Student Loan Funding's eCounselor website may have exposed names and Social Security numbers.

**Information Source:** Dataloss DB

**University of Missouri**  
**Columbia, Missouri**  
**EDU Hack**  
**22,396**

(866) 241-5619

A hacker accessed a computer database containing the names and Social Security numbers of employees of any campus within the University system in 2004 who were also current or former students of the Columbia campus.

**Information Source:** Dataloss DB

**EZCORP, EZPAWN**  
**San Antonio, Texas**  
**BSF Phys**  
**Unknown**

Several EZPAWN stores in the San Antonio area exposed customers' personal information by discarding business records in easily accessible trash cans behind stores. The Texas Attorney General decided to take legal action against EZCORP Inc. and its subsidiary EZPAWN. Customer records included promissory notes and bank statements that contained names, addresses, Social Security numbers, driver's license numbers and checking account information.

**Information Source:** Dataloss DB
May 8, 2007  Jones Beauty College  
Dallas, Texas  
EDU   PHYS   Unknown

The Texas Attorney General filed an enforcement action against the College in March. Student financial aid forms with Social Security numbers and other personal information had been improperly discarded.

Information Source: 
Media

May 8, 2007  Carus Publishing Company  
Petersborough, New Hampshire  
BSO   HACK   Unknown

Hackers obtained access to customer information located on the Company’s website. The breach occurred sometime between April and May. Customer names, addresses, credit card numbers and types of credit cards were downloaded by the hackers.

Information Source: 
Dataloss DB

May 7, 2007  Indiana Department of Administration  
Indianapolis, Indiana  
GOV   DISC   Unknown

An employee uploaded a list of certified women and minority business enterprises to the department’s Web site and inadvertently included their tax identification numbers, which for some businesses and sole proprietorships is the owner’s Social Security number. Reports indicate that the number of people affected was no more than a couple hundred.

Information Source: 
Dataloss DB

May 7, 2007  Private Tax Practice  
Southold, New York  
BSF   PORT   60

A laptop with client information was stolen on April 27. Tax return files were on the laptop, though it was encrypted. Client information also included names, addresses and Social Security numbers.

Information Source: 
Dataloss DB

May 7, 2007  Arteis  
Palo Alto, California  
BSO   HACK   Unknown

The location listed is Hewlett-Packard Company’s headquarters. Hewlett-Packard acquired Arteis in May of 2007.

In January, Arteis discovered that an unauthorized person had accessed certain files. Customer names, addresses and credit card numbers may have been exposed.

Information Source: 
Dataloss DB

May 7, 2007  Transportation Security Administration (TSA)  
Crystal City, Virginia  
GOV   PORT   100,000

A computer hard drive containing payroll data from January 2002 to August 2005 including employee names, Social Security numbers, birth dates, bank account and routing information of current and former workers including airport security officers and federal air marshals was stolen.

UPDATE (5/14/07) The American Federation of Government Employees is suing the TSA for the loss of the hard drive. It calls the breach a violation of the Privacy Act.

Information Source: 
Dataloss DB

May 3, 2007  Maryland Department of Natural Resources  
Annapolis, Maryland  
GOV   PORT   1,433

Personal information of current and retired employees including names and Social Security numbers was downloaded to a thumb drive by an employee who wanted to work at home but was lost en route.

Information Source: 
Dataloss DB

May 3, 2007  Louisiana State University, E.J. Ourso College of Business  
Baton Rouge, Louisiana  
EDU   PORT   750

A laptop stolen from a faculty member’s home contained personally identifiable information including may have included students’ Social Security numbers, full names and grades of University students.
May 3, 2007

**Montgomery College**
Conroe, Texas

A new employee posted the personal information of all graduating seniors including names, addresses and Social Security numbers on a computer drive that is publicly accessible on all campus computers.

May 1, 2007

**Healing Hands Chiropractic**
Sterling, Colorado

Hundreds of medical records containing the personal information of chiropractic patients including Social Security numbers, birth dates, addresses and, in some cases, credit card information were thrown into a dumpster “due to lack of office space.”

May 1, 2007

**JP Morgan**
New York, New York

Documents containing personal financial data of customers including names, addresses and Social Security numbers were found in garbage bags outside five branch offices in New York.

May 1, 2007

**Maine State Lottery Commission**
Hallowell, Maine

Documents containing personal information such as names, Social Security numbers, references to workers compensation claim records, psychiatric and other medical records, and police background checks were found in a dumpster.

May 1, 2007

**Champaign Police Officers**
Champaign, Illinois

The names and Social Security numbers of Champaign police officers were left on a computer donated to charity.

May 1, 2007

**JP Morgan**
Chicago, Illinois

A computer tape containing personal information of wealthy bank clients and some employees was delivered to a secure off-site facility for storage but was later reported missing.

April 30, 2007

**Home Depot**
Atlanta, Georgia

A laptop was stolen on March 23. Home Depot associates may have had their Social Security number and amount of Home Depot incentive program bonus exposed. Names and addresses were not on the laptop. Employees were notified on April 30.

April 29, 2007

**University of New Mexico**
Alburquerque, New Mexico

3,000 not included in total below because SSNs were apparently not compromised)
Employees’ personal information including names, e-mail and home addresses, UNM ID numbers and net pay for a pay period for staff, faculty and a few graduate students may have been stored on a laptop computer stolen from the San Francisco office of an outside consultant working on UNM’s human resource and payroll systems.

**Information Source:** Dataloss DB

**April 28, 2007**

**Couriers on Demand**  
Dallas, Texas  
BSO  DISC  Hundreds

Personal information of job applicants was accidentally published to the Internet.

**Information Source:** Dataloss DB

**April 27, 2007**

**Google Ads**  
Mountain View, California  
BSO  HACK  Unknown

Top sponsored Google ads linked to 20 popular search terms were found to install a malware program on users’ computers to capture personal information and access online accounts for 100 different banks.

**Information Source:** Media

**April 27, 2007**

**Caterpillar, Inc., SBA Inc.**  
Peoria, Illinois  
BSO  PORT  Unknown

A laptop computer containing personal data of employees including Social Security numbers, banking information and addresses was stolen from a benefits consultant that works with the company.

**Information Source:** Dataloss DB

**April 27, 2007**

**Commonwealth Business Media**  
Newark, New Jersey  
BSO  DISC  145

An employee accidentally attached a spreadsheet to an email that was sent to other employees. The spreadsheet had the names, Social Security numbers and other personnel information of each of the people it was emailed to.

**Information Source:** Dataloss DB

**April 26, 2007**

**Ceridian Corp.**  
Minneapolis, Minnesota  
BSO  DISC  150

A former employee had data containing the personal information of employees including ID and bank-account data and then, accidentally posted it on a personal Web site.

**Information Source:** Dataloss DB

**April 25, 2007**

**Neiman Marcus Group**  
Dallas, Texas  
BSR  STAT  160,000

http://phx.corporate-ir.net/phoenix.zhtml?c=118113&p=irol-recentdata, (800) 456-7019

Computer equipment was stolen containing files with sensitive information including name, address, Social Security number, date of birth, period of employment and salary information of retailer Neiman Marcus Group’s current and former employees and their spouses.

**Information Source:** Dataloss DB

**April 24, 2007**

**Purdue University**  
West Lafayette, Indiana  
EDU  DISC  175

(866) 307-8513

Personal information including names and Social Security numbers of students who were enrolled in a freshman engineering honors course was on a computer server connected to the Internet that had been indexed by Internet search engines and consequently was available to individuals searching the Web.

**Information Source:** Dataloss DB

**April 24, 2007**

**Baltimore County Department of Health**  
GOV  PORT  6,000

688
April 24, 2007 Baltimore, Maryland

A laptop containing personal information including names, date of birth, Social Security numbers, telephone numbers and emergency contact information of patients who were seen at the clinic between Jan. 1, 2004 and April 12 was stolen.

Information Source: Dataloss DB


Social Security numbers of Disaster Assistance Employees were printed on the outside address labels of reappointment letters

Information Source: Dataloss DB

April 21, 2007 Albertsons (Save Mart Supermarkets) Alameda, California

Credit and debit card numbers were stolen using bogus checkout-line card readers resulting in card numbers processed at those terminals being captured and some to be misused.

Information Source: Dataloss DB

April 20, 2007 Los Alamos National Laboratory Alburquerque, New Mexico

The names and Social Security numbers of lab workers were posted on a Web site run by a subcontractor working on a security system.

Information Source: Dataloss DB

April 20, 2007 U.S. Agriculture Department Washington, District Of Columbia

The Social Security numbers of people who received loans or other financial assistance from two Agriculture Department programs were disclosed since 1996 in a publicly available database posted on the Internet. Originally, the US Department of Agriculture estimated that the personal information of as many as 150,000 people may be affected, then reduced the number 38,700.

Information Source: Dataloss DB

April 19, 2007 New Mexico State University Las Cruces, New Mexico

The names and Social Security numbers of students who registered online to attend their commencement ceremonies from 2003 to 2005 were accidentally posted on the school’s Web site when an automated program moved what was supposed to be a private file into a public section of the Web site.

Information Source: Dataloss DB

April 19, 2007 Honeywell International Morristown, New Jersey

A laptop was stolen from a Honeywell HR employee. It contained the names and Social Security numbers of employees. At least 20 New York residents were affected, but the total number of people affected nationwide was not revealed.

Information Source: Dataloss DB

April 19, 2007 Valve Software Bellevue, Washington

A hacker accessed customer information that was stored on the website. Thousands of customers had their information exposed, and the hacker posted some customer credit card information. The hacker claims to have gained access by utilizing login details that were easily found by browsing. Valve asset information was also exposed.
A hacker accessed the names, Social Security numbers, employee ID numbers and birth dates of 14,000 current and former staff members.

A computer file server containing names, contact information, and Social Security numbers for study subjects and potential study subjects related to research on causes and cures for different types of cancer was stolen from a locked UCSF office. For some individuals, the files also included personal health information.

The names, Social Security numbers and grades of 3,500 former chemistry students were on class rosters housed on two laptop computers stolen from a professor's home in late February.

The Attorney General of Texas filed a complaint against CVS Pharmacy for illegally disposing of personal information including active debit and credit card numbers, complete with expiration dates and medical prescription forms with customer's name, address, date of birth, issuing physician and the types of medication prescribed. The information was found in a dumpster behind a store that apparently was being vacated.

A laptop containing personal information of current, former and retired employees including names, addresses, dates of birth and Social Security numbers was stolen when an employee was a victim of a recent break-in. A limited number of people were affected.

Personal information including names, Social Security numbers, and radiology images of patients were previously included in two medical symposium presentations that were posted on UPMC's Web site. Though the presentation was later removed in 2005, the presentations were apparently inadvertently re-posted on the site and only recently removed again.

30 boxes of Fulton County voter registration cards that contain names, addresses and Social Security numbers were found in a trash bin.
A laptop computer that contained personal information of members who had loans with the credit union was stolen from Protiviti, a consultant employed by Bellco Credit Union conducting due diligence to prepare a possible acquisition bid.

An organization responsible for managing Broward County’s child welfare system believes a dishonest former employee stole a laptop from the agency’s office. It contains personal information of adoptive and foster-care parents including financial and credit data, Social Security numbers, driver’s license data and passport numbers.

Names and Social Security numbers of scholarship winners were inadvertently posted and publicly available on the university’s web site.

Two emails were sent to a group of Company employees. They contained an attachment with the names, Social Security numbers, addresses, dates of birth, job titles and pay rates of all employees. Some of the email recipients had authorization to view the information, but most did not.

A computer disk containing personal information including addresses, birthdates, dates of eligibility, full names, Medicaid or children’s health care recipient identification numbers, and Social Security numbers went missing from a private vendor, Affiliated Computer Services (ACS), contracted to handle health care claims for the state.

The location listed is the headquarters of TurboTax’s developer Intuit Consumer Tax Group.

Using TurboTax online to access previous returns, a Nebraska woman was able to access tax returns for other Turbo Tax customers in different parts of the country. The returns contained personal information needed to e-file including bank account numbers with routing digits and Social Security numbers.
A locked shipping case of backup tapes containing personal information including names, Social Security numbers, drivers' license numbers, and bank account numbers went missing while in transit with UPS.

Information
Source: Dataloss DB

April 6, 2007  Chicago Public Schools
Chicago, Illinois
EDU  PORT
April 6, 2007
(773) 553-1142
Two laptop computers contain the names and Social Security numbers of current and former employees was stolen from Chicago Public Schools headquarters.

Information
Source: Dataloss DB

April 5, 2007  DCH Health Systems
Tuscaloosa, Alabama
MED  PORT
April 5, 2007
An encrypted disc and hardcopy documents containing retirement benefit information including Social Security numbers and other personal information were lost. Tracking data indicates the package was delivered to the addressee’s building, but the intended recipient never received the package.

Information
Source: Dataloss DB

April 5, 2007  Security Title Agency
Phoenix, Arizona
BSF  HACK
April 5, 2007
Hackers "defaced" the company's Web site and may have accessed customer information which is stored on the same server as the site.

Information
Source: Media

April 5, 2007  Thomson Elite
Los Angeles, California
BSF  STAT
April 5, 2007
Eleven computers were stolen during a March 25 office burglary. One of the computers contained a file of travel and expense information of certain individuals. Credit card information and Social Security numbers may have been exposed.

Information
Source: Dataloss DB

April 4, 2007  University of California, San Francisco (UCSF)
San Francisco, California
EDU  HACK
April 4, 2007
(415) 353-8100, jsecurity@ucsf.edu
An unauthorized party may have accessed the personal information including names, Social Security numbers, and bank account numbers of students, faculty, and staff associated with UCSF or UCSF Medical Center over the past two years by compromising the security of a campus server.

Information
Source: Dataloss DB

April 4, 2007  Guilford Technical Community College
Greensboro, North Carolina
EDU  PHYS
April 4, 2007
550 (No SSNs or financial information reported)
A surplus file cabinet that was temporarily stored in a warehouse area prior to an auction held sensitive paper documents. Anyone entering the warehouse could have viewed or taken the files.

Information
Source: Dataloss DB

April 3, 2007  Commerce Banc Insurance Services (CBIS)
Cherry Hill, New Jersey
BSF  PORT
April 3, 2007
A CBIS vendor had a laptop stolen. CBIS employees may have had their names, Social Security numbers, and possibly health information exposed.
A laptop was stolen from an employee on or around January 10. People who had previously traveled on the company aircraft had their information exposed.

An investigation revealed that an employee was selling customer financial information. The employee’s work computer was searched and several spreadsheets with customer names, addresses, credit card numbers and bank account numbers were found.

A laptop was stolen from an employee’s vehicle in a parking lot on March 24. It contained names, Social Security numbers and loan data.

Three laptops containing personal information including about 130,500 Social Security numbers — most without names, 12,000 individuals' names and addresses, and more than 101,000 child support case numbers were apparently stolen from the department’s office.

Three laptops were reported missing that may contain Sailors’ names, rates and ratings, Social Security numbers, and college course information. The compromise could impact Sailors and former Sailors homeported on San Diego ships from January 2003 to October 2005 and who were enrolled in the Navy College Program for Afloat College Education.

A computer disk containing students' Social Security numbers, names, birth dates, addresses and other personal information was stolen from a professor’s office. The stolen information belonged to over 400 students enrolled in the TRIO Student Support Services program, which offers financial and personal counseling and other assistance.

A software configuration problem caused personnel information stored on a Curb employee’s home computer to be accessible through the Internet. Employees may have had their names, Social Security numbers, addresses and telephone numbers exposed.

A laptop was stolen from an employee’s vehicle in a parking lot on March 24. It contained names, Social Security numbers and loan data.

Three laptops containing personal information including about 130,500 Social Security numbers — most without names, 12,000 individuals' names and addresses, and more than 101,000 child support case numbers were apparently stolen from the department’s office.

Three laptops were reported missing that may contain Sailors’ names, rates and ratings, Social Security numbers, and college course information. The compromise could impact Sailors and former Sailors homeported on San Diego ships from January 2003 to October 2005 and who were enrolled in the Navy College Program for Afloat College Education.

A computer disk containing students' Social Security numbers, names, birth dates, addresses and other personal information was stolen from a professor’s office. The stolen information belonged to over 400 students enrolled in the TRIO Student Support Services program, which offers financial and personal counseling and other assistance.

A software configuration problem caused personnel information stored on a Curb employee’s home computer to be accessible through the Internet. Employees may have had their names, Social Security numbers, addresses and telephone numbers exposed.

A laptop was stolen from Exponent's office. Multiple organizations were affected because Exponent provides human resources services for various companies. Employee names, Social Security numbers and addresses may have been on the laptop.

Information Source: Dataloss DB  
March 30, 2007  New York State Office of the State Comptroller  Albany, New York  
GOV DISC 47

A retiree discovered a web page with a list of retirees who had requested a copy of their 1099R tax form. Names, Social Security numbers, phone numbers and retirement numbers were on the page. The entire web page and the "tax calculator" feature which the retiree had used to find the information were removed from the website when the Office became aware of the incident.

Information Source: Dataloss DB  
March 29, 2007  RadioShack  Portland, Texas  
BSR PHYS Unknown

20 boxes of discarded records including sales receipts with names, addresses, Social Security numbers, credit card information, and personal information of store employees spanning from 2001 to 2005 were found in a dumpster.

UPDATE (04/03/07): The Texas Attorney General’s Office filed an action against the Radio Shack store for violating the state’s violating the 2005 Identity Theft Enforcement and Protection Act.

Information Source: Dataloss DB  
March 29, 2007  Experian, Vallarta Auto Sales  Las Vegas, Nevada  
BSR UNKN Unknown

An unauthorized person gained access to Vallarta's Experian account and may have obtained consumer information. Affected individuals may have had their names, Social Security numbers, dates of birth and addresses exposed. Fourteen New York residents were affected, but the total number of people affected nationwide was not reported.

Information Source: Dataloss DB  
March 28, 2007  City of New York Department of Environmental Protection  Flushing, New York  
GOV INSD 2,108

An employee was discovered to have accessed customer names and Social Security numbers. The employee was terminated. The employee's length of employment and any fraudulent activity related to the breach was not reported.

Information Source: Dataloss DB  
March 27, 2007  St. Mary Parish Schools  Centerville, Louisiana  
EDU DISC 380

Personal information including Social Security numbers of St. Mary Parish public school employees was available on the Internet when a Yahoo!Web crawler infiltrated the server of the school's technology department.

Information Source: Dataloss DB  
March 26, 2007  Fort Monroe  Fort Monroe, Virginia  
GOV PORT 16,000

A laptop computer containing the names, Social Security numbers and payroll information for as many as 16,000 civilian employees was stolen from an employee's personal vehicle. Bank account and bank routing information were not included. People who work at the U.S. Army Training and Doctrine Command were affected.

Information Source: Dataloss DB
March 26, 2007  United Subcontractors Inc.
Edina, Minnesota

The theft occurred in New Jersey.

Three jump drives and a laptop were stolen from the trunk of a rental car. The names, Social Security numbers, and dates of birth of employees may have been exposed.

Information Source: Dataloss DB

March 23, 2007  Group Health Cooperative Health Care System
Seattle, Washington


Two laptops containing names, addresses, Social Security numbers and Group Health ID numbers of local patients and employees have been reported missing.

Information Source: Dataloss DB

March 23, 2007  Swedish Urology Group
Seattle, Washington

Three computer hard drives with personal files on hundreds of patients, doctors, and staff were stolen.

Information Source: Dataloss DB

March 23, 2007  New York Institute of Technology
Old Westbury, New York

A file with the names, Social Security numbers, addresses, dates of birth, degree types and majors of former NYIT students was posted on NYIT's website. The information was not accessible via the NYIT website, but could be found through an Internet search.

Information Source: Dataloss DB

March 23, 2007  Homeland Funding Solutions Inc.
Cranston, Rhode Island

Two laptops and 13 desktop computers were stolen from the main office of Homeland Funding Solutions, Inc. over the weekend of March 17. Loan information that had been sent via email may have been on the hard drives of the stolen computers.

Information Source: Dataloss DB

March 20, 2007  Tax Service Plus
Santa Rosa, California

Thieves stole the company's backup computer, which contained financial data on thousands of tax returns dating back three years.

Information Source: Dataloss DB

March 20, 2007  Sungard
Malvern, Pennsylvania

A laptop was stolen from an employee's car. It contained the names and Social Security numbers of employees. Around 1,700 employees had their bank transfer ABA number and account number exposed, and about 100 had their credit card number exposed.

Information Source: Dataloss DB

March 19, 2007  Science Applications International Corp. (SAIC)
Boise, Idaho

Barrels filled with thousands of sensitive documents including printed copies of e-mail and performance evaluations along with documents marked “internal use only – not for public release” and “for official use only” were found on the curb outside of SAIC's local office.
March 19, 2007  Pitney Bowes  Stamford, Connecticut  

An employee's laptop was stolen from her home on or around March 2. The laptop may have contained employee names and Social Security numbers.

March 19, 2007  Electronic Data Systems Corp. (EDS)  Sacramento, California  

An EDS employee working on a project involving processing workers' compensation related medical bills for Fireman's Fund had his laptop stolen from his car on January 19. Names and Social Security numbers were exposed.

March 16, 2007  Springfield City Schools, Ohio State Auditor  Springfield, Ohio  

A laptop containing personal information of current and former employees of Springfield City Schools including their names and Social Security numbers was stolen from a state auditor employee's vehicle while parked at home in a garage.


A laptop was stolen from a Henry Schein agent during a trade show in Chicago, IL. The laptop may have contained the names and Social Security numbers of people who had a leasing or loan transaction with Choice Health Leasing were affected.

March 16, 2007  Laser Pros International Corp  Rhinelander, Wisconsin  

Someone gained access to transaction data from the Laser Pros website. Customer names, addresses, email addresses, credit card numbers and security codes for credit cards may have been accessed. Some customers reported fraudulent charges. The total number of credit cards accessed was 434, though customers may have had multiple credit cards.

March 14, 2007  WellPoint’s Empire Blue Cross and Blue Shield unit in NY  Indianapolis, Indiana  

An unencrypted disc containing patient's names, Social Security numbers, health plan identification numbers and description of medical services back to 2003 was lost en route to a subcontractor.

UPDATE (3/14/07): The subcontractor reported that the CD that was reported missing on Feb. 9 has been found.

March 13, 2007  U.S. Department of Agriculture (USDA)  Washington, District Of Columbia  

A total of 95 USDA computers were lost or stolen between Oct. 1, 2005, and May 31, 2006. Some may have contained personal information such as names, addresses, Social Security numbers and payment information. Two-thirds of the computers contained unencrypted data.
The January 13 theft of a laptop exposed personal information of current and former practitioner teachers. The laptop was stolen from an office. It contained names, Social Security numbers, addresses and telephone numbers. Seven New York residents were affected, but the number of affected employees nationwide was not revealed.

**Information Source:** Dataloss DB

March 12, 2007  **Dai Nippon**, New York, New York  
BSO  INSD  Unknown

The incident occurred outside of the U.S. and the companies affected were not disclosed.

A former contract worker of a Japanese commercial printing company stole nearly 9 million pieces of private data on customers from 43 clients, including U.S. companies. The stolen data includes confidential information such as names, addresses and credit card numbers intended for use in direct mailing and other printing services. Customers of U.S.-based American Home Assurance Co. and Toyota Motor were affected.

**Information Source:** Dataloss DB

March 10, 2007  **University of Idaho**, Moscow, Idaho  
EDU  DISC  2,700

888-900-3783

A data file posted to the school’s Web site contained personal information including names, birthdates and Social Security numbers of University employees.

**Information Source:** Dataloss DB

March 9, 2007  **California National Guard**, Sacramento, California  
GOV  PORT  1,300

A computer hard drive containing Social Security numbers, home addresses, birth dates and other identifying information of California National Guard troops deployed to the U.S.-Mexico border was stolen.

**Information Source:** Dataloss DB

March 7, 2007  **Los Rios Community College**, Sacramento, California  
EDU  DISC  2,000

Student information including Social Security numbers were accessible on the Internet after the school used actual data to test a new online application process in October.

**Information Source:** Dataloss DB

March 7, 2007  **U.S. Census Bureau**, Washington, District Of Columbia  
GOV  DISC  302 households


Personal information of 302 households including names, addresses, phone numbers, birth dates and family income ranges were posted on a public Internet site multiple times over a five-month period from October 2006 to Feb. 15, 2007 when Census employees working from home tested new software records.

**Information Source:** Dataloss DB

March 7, 2007  **Right Media Inc.**, New York, New York  
BSO  HACK  34

An unauthorized person or persons accessed the computer system. Customer names, Social Security numbers, email addresses, addresses and employee ID numbers may have been accessed.

**Information Source:** Dataloss DB

March 7, 2007  **North Carolina Department of Correction**, Raleigh, North Carolina  
GOV  PHYS  16 (No SSNs or financial information}
Paper documents with sensitive information were thrown into the trash and may have been recovered by an inmate working as a janitor.

Information Source: Dataloss DB
March 7, 2007  Eastern Suffolk BOCES Patchogue, New York

A file server in the Eastern Suffolk BOCES computer area was hacked. Data from the Free and Reduced Lunch Database was compromised. The names of parents and children, Social Security numbers, addresses, home and work phone numbers, salary information and income information that were related to the program may have been accessed.

Information Source: Dataloss DB
March 3, 2007  Metropolitan State College of Denver Denver, Colorado

http://www.mscd.edu/securityalert/, 866-737-6622

A faculty member's laptop computer that contained the names and Social Security numbers of former students was stolen from its docking station on campus.

Information Source: Dataloss DB
March 3, 2007  Johnny's Selected Seeds Winslow, Maine

Hacker accessed credit card account information of online customers. About 20 credit cards have been used fraudulently.

Information Source: Dataloss DB
March 2, 2007  California Department of Health Services Sacramento, California


Benefit notification letters containing names addresses, Medicare Part D plan names and premium payment amounts of some individuals enrolled in the California AIDS Drug Assistance Program (ADAP) were erroneously mailed to another enrollee.

Information Source: Media
March 1, 2007  Westerly Hospital Westerly, Rhode Island

Patient names, Social Security numbers, contact information as well as insurance information were posted on a publicly-accessible Web site.

Information Source: Dataloss DB
February 28, 2007  Gulf Coast Medical Center Tallahassee, Florida

Patient information including names and Social Security numbers were compromised when a computer went missing in February in Tallahassee, FL. A very similar and previously uncovered breach happened in November of 2006.

Information Source: Dataloss DB
February 28, 2007  Gulf Coast Medical Center Nashville, Tennessee

Patient information including names and Social Security numbers were compromised when a computer went missing in November 2006 from Nashville, TN. This breach drew media attention when an additional 8,000 patients' information was compromised during a February 2007 breach in Tallahassee, FL.
Subscriber user-IDs and passwords were compromised. Unauthorized individuals may have accessed names, Social Security numbers, addresses and other information related to employment credit reports. At least 11 New York residents were affected by this breach, but the total number of affected individuals nationwide was not revealed.

**Information Source:** Dataloss DB

**February 27, 2007**
**CBCInnovis Inc., Hudiburg Chevrolet**
**Midwest City, Oklahoma**

BSR UNKN 138

An unauthorized person gained access to Hudiburg Chevrolet's CBCInnovis account. The person or persons would have been able to obtain customer names, Social Security numbers, addresses and credit information.

**Information Source:** Dataloss DB

**February 23, 2007**
**Rabun Apparel Inc., former subsidiary of Fruit of the Loom**
**Rabun Gap, Georgia**

BSR DISC 1,006

Names and Social Security numbers of former employees were accessible on the Internet from Jan. 15 until Feb. 20.

**Information Source:** Dataloss DB

**February 23, 2007**
**ADC Telecommunications Inc., Flex Compensation**
**St. Louis Park, Minnesota**

BSR PORT 63,400

A laptop was stolen from ADC’s benefits administrator. Current and former employee names, Social Security numbers, bank account numbers, dates of birth, addresses and other private information were on the laptop. It is not clear if employees from other companies that use Flex Compensation for benefits administration are among the 63,400 affected individuals.

**Information Source:** Dataloss DB

**February 22, 2007**
**Speedmark**
**Woodlands, Texas**

BSO STAT 35,000

Thieves stole several computers, one of which contained a database with personally identifying information including names, addresses, e-mail accounts, and Social Security numbers of Speedmark’s mystery shopper employees and contractors.

**Information Source:** Dataloss DB

**February 21, 2007**
**Georgia Institute of Technology**
**Atlanta, Georgia**

EDU HACK 3,000

404-894-2499, hr@gatech.edu

Personal information of former employees mostly in the School of Electrical and Computer Engineering including name, address, Social Security number, other sensitive information, and about 400 state purchasing card numbers, were compromised by unauthorized access to a Georgia Tech computer account.

**Information Source:** Dataloss DB

**February 21, 2007**
**Fidelity Investments, Dairy Farmers of America**

BSF PORT 69

A Fidelity laptop used by a former Fidelity employee was discarded and recovered by a non-affiliated person. The employee had taken the laptop home after believing it had been decommissioned from business use by Fidelity. Participants and beneficiaries of participants in the Dairy Farmers of America Defined Benefit plan had their names and Social Security numbers exposed. At least 69 New York residents were affected by the breach, but the total number of affected individuals nationwide was not revealed.

**Information Source:** Dataloss DB

**February 20, 2007**
**Back and Joint Institute of Texas**
**San Antonio, Texas**

MED PHYS Unknown
Twenty boxes containing Social Security numbers, photocopies of driver’s license numbers, addresses, phone numbers and private medical history of chiropractic patients were found in a dumpster.

**Information Source:**
Dataloss DB

February 20, 2007

**Credit Suisse**
New York, New York

BSF DISC 3,000

Documents with confidential details of loan applicants were mistakenly posted online. The documents are routinely posted online without personal information. Applicant names, Social Security numbers, addresses, monthly incomes and credit scores were exposed. The exposure first occurred on March 15, 2006.

**Information Source:**
Dataloss DB

February 19, 2007

**Seton Healthcare Network**
North Austin, Texas

MED PORT 7,800

A laptop with uninsured patients’ names, birth dates and Social Security numbers was stolen last week from the Seton hospital system. The uninsured patients had gone to Seton emergency rooms and city health clinics since July 1, 2005.

**Information Source:**
Dataloss DB

February 19, 2007

**Clarksville-Montgomery County middle and high schools**
Clarksville, Tennessee

EDU DISC 633

Staff and faculty Social Security numbers, used as employee identification numbers, were embedded in file photos by the company that took yearbook pictures and inadvertently placed in a search engine on school system’s Web site.

**Information Source:**
Dataloss DB

February 19, 2007

**Stop & Shop Supermarkets**
Quincy, Massachusetts

BSR CARD Unknown

Additional locations: Southern Massachusetts and Rhode Island. (877) 366-2668

Credit and debit card account information including PIN numbers was stolen by high-tech thieves who apparently broke into checkout-line card readers and PIN pads and tampered with them.

**Information Source:**
Dataloss DB

February 19, 2007

**Social Security Administration (SSA)**
Milwaukee, Wisconsin

GOV PHYS 13

Files of disability applicants containing Social Security numbers, addresses, phone numbers of family members, dates of birth, work history, and detailed medical information were lost/stolen when a telecommuting employee abandoned them in a locked filing cabinet at home after a threat of domestic violence. Several of the files were mailed back to the local SSA office. Others were found in a dumpster months later. Four were never recovered.

**Information Source:**
Media

February 17, 2007

**Albany Medical Center**
Albany, New York

MED PORT 12,000

(A Unknown number of SSNs)

A laptop was stolen from the Employee Health Services center. It contained software used to track information required for N95 fit testing at Albany Med. Staff names and Social Security numbers were also exposed. Anyone who had N95 fit testing at Albany Med between January 2005 and February 2007 may have had their personal information exposed.

**Information Source:**
Dataloss DB

February 16, 2007

**Brunswick Corp.**
Lake Forrest, Illinois

BSR HACK 5,100

An unauthorized person obtained access to employee information stored on Brunswick’s computer systems. Names, Social Security numbers and addresses may have been exposed during the April incident.

**Information Source:**
Dataloss DB

February 16, 2007
Names, grades, and SSNs were posted on an unprotected Web site after summer session in 1999. CCSF stopped using SSNs as students IDs in 2002.

Information Source: Dataloss DB records from this breach used in our total: 11,000

February 15, 2007  The Professional Education Institute Burr Ridge, Illinois  EDU DISC 34

Customer information was accidentally exposed online because of a data encryption lapse. The Social Security numbers and dates of birth of some customers were viewable on the Millionaire Elite Website. Two New Hampshire, three Maine and 29 New York residents were affected by the breach. The total number of individuals affected nationwide was not revealed.

Information Source: Dataloss DB records from this breach used in our total: 34

February 14, 2007  Kaiser Medical Center Oakland, California  MED PORT 22,000 patients, but apparently only 500 records contained SSNs

(866) 529-0779

A doctor’s laptop was stolen from the Medical Center containing medical information of 22,000 patients. But only 500 records contained SSNs.

Information Source: Dataloss DB records from this breach used in our total: 500

February 14, 2007  Iowa Department of Education Des Moines, Iowa  GOV HACK 600

Up to 600 files of G.E.D. recipients were viewed when the online database was hacked. Files included names, addresses, birthdates, and SSNs of G.E.D. graduates from 1965 to 2002.

Information Source: Dataloss DB records from this breach used in our total: 600

February 14, 2007  Connecticut Office of the State Comptroller Hartford, Connecticut  GOV DISC 1,753

Personal information of state employees including names and Social Security numbers was inadvertently posted on the Internet in a spreadsheet of vendors used by the state.

Information Source: Dataloss DB records from this breach used in our total: 1,753

February 10, 2007  State of Indiana Official Website www.IN.gov Indianapolis, Indiana  GOV HACK 76,600

(888) 438-8397, Email: securityconcerns @www.IN.gov

A hacker gained access to the State Web site and obtained credit card numbers of individuals who had used the site’s online services and gained access to Social Security numbers for 71,000 healthcare workers and 5,600 individuals and businesses.

UPDATE (3/22/07): Investigators have identified a teen they believe hacked into the IN.gov as a prank.

Information Source: Dataloss DB records from this breach used in our total: 76,600

February 9, 2007  East Carolina University Greenville, North Carolina  EDU DISC 65,000 students, alumni, and staff members

http://www.ecu.edu/incident/, 877-328-6660

A programming error resulted in personal information of 65,000 individuals being exposed on the University’s Web site.
The data has since been removed. Included were names, addresses, SSNs, and in some cases credit card numbers.

**Information Source:** Dataloss DB  
**February 9, 2007**  
**Radford University, Waldron School of Health and Human Services**  
**Radford, Virginia**  
**EDU**  
**HACK**  
**2,400 children**

A computer security breach exposed the personal information, including SSNs, of children enrolled in the FAMIS program, Family Access to Medical Insurance Security.

**Information Source:** Dataloss DB  
**February 9, 2007**  
**General Electric**  
**Louisville, Kentucky**  
**BSR**  
**PORT**  
**80**

A GE service technician's laptop was stolen. It contained customer names and credit card numbers.

**Information Source:** Dataloss DB  
**February 8, 2007**  
**Piper Jaffrey**  
**Minneapolis, Minnesota**  
**BSF**  
**DISC**  
**More than 1,000 employees**

W-2s sent to current and former employees in January included employees’ Social Security numbers on the outside of the envelope. Though the numbers were not identified as Social Security numbers, they followed the standard XXX-XX-XXXX format. Executives indicated the mishap was an error by a third-party vendor.

**Information Source:** Dataloss DB  
**February 8, 2007**  
**St. Mary’s Hospital**  
**Leonardtown, Maryland**  
**MED**  
**PORT**  
**130,000**

A laptop was stolen in December that contained names, SSNs, and birthdates for many of the Hospital’s patients.

**Information Source:** Dataloss DB  
**February 8, 2007**  
**Fresenius Medical Care Holdings Inc., Fresenius Medical Care North America (FMCNA)**  
**Waltham, Massachusetts**  
**MED**  
**PORT**  
**10 (No SSNs or financial information reported)**

A laptop was stolen from the locked car of an employee on December 13 while it was parked outside of a restaurant. The laptop contained patient names, dates of birth, dates of service and insurance information.

**Information Source:** Dataloss DB  
**February 8, 2007**  
**LexisNexis**  
**Boca Raton, Florida**  
**BSO**  
**INSD**  
**220**

LexisNexis sent out notification letters of two separate incidents. A law enforcement customer noticed that an account was used in an unauthorized way. Searches that revealed names, Social Security numbers and driver’s license numbers may have been performed by an unauthorized user or without proper reason. The second incident involves a government agency employee who may have used his account in an unauthorized manner to view names, Social Security numbers, addresses and driver’s license numbers. Over 220 New York residents were affected by the breaches, but the total number of affected customers nationwide was not revealed.

**Information Source:** Dataloss DB  
**February 8, 2007**  
**District Council 37 Health and Security Plan of New York City**  
**New York, New York**  
**GOV**  
**PORT**  
**31,500**

A CD containing prescription drug data was discovered missing from the organization’s files. People who had their prescription drugs filled through DC 37’s prescription drug benefits plan may have had their names and Social Security numbers exposed. Prescription information from between February 13 and February 22 of 2006 (the previous year) was also exposed.
An employee accidentally posted SSNs of 72 students, professors, and staff on UNL's public Web site where they remained for 2 years. They have since been removed.

Information Source: Dataloss DB

Johns Hopkins University and Johns Hopkins Hospital
Baltimore, Maryland

Johns Hopkins reported the disappearance of 9 backup computer tapes containing personal information of employees and patients. Eight of the tapes contained payroll information on 52,000 past and present employees, including SSNs and in some cases bank account numbers. The 9th tape contained less sensitive information about 83,000 hospital patients.

Information Source: Dataloss DB

Central Connecticut State University
New Britain, Connecticut

Social Security numbers of about 750 CCSU students were exposed in the name and address window on envelopes mailed to them. The envelopes were not folded correctly. They contained IRS 1098T forms.

Information Source: Dataloss DB

A laptop computer and documents were stolen from a state tax auditor's apartment. While the laptop had security features and had little personal information on it, the documents contained personal information for people who were employed by 13 Capital Region businesses.

Information Source: Dataloss DB

Thousands of files from the defunct bill collection company containing medical records, phone bills and Social Security numbers were found in a trash bin.

Information Source: Dataloss DB

A hacker gained access to a customer database. Customers who made transactions with merchants that Merchant America provides payment processing services to may have had their names, bank account numbers and driver's license numbers exposed.

Information Source: Dataloss DB

The computer and hard drive of a tax preparation company were stolen. Data included names, bank account numbers, routing numbers, birthdates, SSNs, and addresses.

Information Source: Dataloss DB

Massachusetts Department of Industrial Accidents
Boston, Massachusetts

Information Source: Dataloss DB
A former state contractor allegedly accessed a workers' compensation data file and stole personal information, including SSNs. The thief used the data to commit identity theft on at least 3 individuals.

**Information Source:**
Dataloss DB

**February 2, 2007**
**Indian Consulate via Haight Ashbury Neighborhood Council recycling center**
**San Francisco, California**

Visa applications and other sensitive documents were accessible for more than a month in an open yard of a recycling center. Information included applicants' names, addresses, phone numbers, birthdates, professions, employers, passport numbers, and photos. A sampling of documents indicated that the paperwork included everyone who applied in the Western states from 2002-2005. Applicants were current and former executives of major Bay Area companies that have operations in India.

**Information Source:**
Dataloss DB

**February 2, 2007**
**Wisconsin Assembly**
**Madison, Wisconsin**

A document containing personal information of Wisconsin Assembly members was stolen from a legislative employee's car while she was exercising at a local gym. It contained names, addresses, and SSNs.

**Information Source:**
Dataloss DB

**February 2, 2007**
**University of Missouri, Research Board Grant Application System**
**Columbia, Missouri**

A hacker broke into a UM computer server mid-January and might have accessed personal information, including SSNs, of 1,220 researchers on 4 campuses. The passwords of 2,579 individuals might also have been exposed.

**Information Source:**
Dataloss DB

**February 2, 2007**
**New York Department of State**
**Albany, New York**

The agency's Web site posted commercial loan documents that mistakenly contained SSNs. The forms are posted to let lenders know the current financial status of loan recipients.

**Information Source:**
Dataloss DB

**February 2, 2007**
**U.S. Department of Veterans Affairs, VA Medical Center**
**Birmingham, Alabama**

An employee reported a portable hard drive stolen or missing that might contain personal information about veterans including Social Security numbers.

**UPDATE (2/10/07):** VA increases number of affected veterans to 535,000, included in the total below.

**UPDATE (2/12/07):** VA reported that billing information for 1.3 million doctors was also exposed, including names and Medicare billing codes, not included in the total below.

**UPDATE (3/19/07):** The VA's Security Operations Center has referred 250 incidents since July 2006 to its inspector general, which has led to 46 separate investigations.

**UPDATE (6/18/07):** More than $20 million to respond to its latest data breach, the breach potentially puts the identities of nearly a million physicians and VA patients.

**Information Source:**
Dataloss DB

**January 29, 2007**
**Mendoza College of Business, Notre Dame University**
**Notre Dame, Indiana**

A file of individuals who took the GMAT test (Graduate Management Admissions Test) was mistakenly left on a computer

**Information Source:**
Dataloss DB
that was decommissioned. The computer was later reactivated and plugged into the Internet. Its files were available through a file-sharing program. Data included names, scores, SSNs and demographic information from 2001.

**Information Source:** Media

**January 29, 2007**  
**Vermont Agency of Human Services**  
**Waterbury, Vermont**

GOV  
HACK  
70,000

Customers of New England Federal Credit Union, Central Vermont Public Service Employees Credit Union, First Brandon National Bank, Federal Family Credit Union, Granite Hills Credit Union, Merchants Bank, Northfield Savings Bank, Opportunities Credit Union and the Vermont State Employees Credit Union were affected.

A state computer that contained the names, Social Security numbers and bank account information was hacked into. Some of the information came from noncustodial parents who owed back child support while most of the people affected were customers of New England Federal Credit Union with no history of owing child support. The information is from 2004 and 2005 credit union members.

**Information Source:** Dataloss DB

**January 29, 2007**  
**Public Storage Inc.**  
**Glendale, California**

BSO  
HACK  
Unknown

Someone gained unauthorized access to electronic company personnel files. The files included Social Security numbers, dates of birth, home addresses and other active employee information.

**Information Source:** Dataloss DB

**January 28, 2007**  
**Salina Regional Health Center**  
**Salina, Kansas**

MED  
PORT  
1,100

A laptop was stolen from a Hospital office. It contained names, Social Security numbers and medical histories of patients. Only patients treated by the laptop user are at risk for identity theft.

**Information Source:** Dataloss DB

**January 28, 2007**  
**New York Academy of Medicine**  
**New York, New York**

EDU  
STAT  
7,460 (0 complete SSNs)

A computer was stolen during an office burglary in October 28. The last four digits of research participants’ Social Security numbers, full names and dates of birth were on a database on the computer. Some participants also had their addresses and laboratory data exposed.

**Information Source:** Dataloss DB

**January 26, 2007**  
**Indiana Department of Transportation (INDOT)**  
**Indianapolis, Indiana**

GOV  
DISC  
4,000

The names and SSNs of INDOT employees were inadvertently posted on an internal network computer drive sometime between Sept. 6 and Dec. 4, 2006.

**Information Source:** Dataloss DB

**January 26, 2007**  
**Vanguard University**  
**Costa Mesa, California**

EDU  
STAT  
5,105 financial aid applicants

(800) 920-7312

On Jan. 16, 2 computers were discovered stolen from the financial aid office. Data included names, SSNs, dates of birth, phone numbers, driver’s license numbers, and lists of assets. Affected financial aid applicants from 2005-2006 and 2006-2007 school years.

**Information Source:** Dataloss DB

**January 26, 2007**  
**WellPoint’s Anthem Blue Cross Blue Shield**  
**Richmond, Virginia**

MED  
PORT  
50,000

(800) 284-9779
Cassette tapes containing customer information were stolen from a lock box held by one of its vendors. Data included names and SSNs.

Information Source: Dataloss DB

January 26, 2007 Chase Bank and the former Bank One, now merged Shreveport, Louisiana

A Bossier woman bought a used desk from a furniture store. She discovered a 165-page spread sheet in a drawer that included names and SSNs of bank employees. The document was returned to the bank.

Information Source: Media


A desktop computer was stolen from the Student Life office containing membership rosters -- including SSNs, birthdates, and addresses -- of the University's 23 fraternities and sororities. A hard drive and memory from 2 other computers were also stolen.

Information Source: Dataloss DB

January 26, 2007 The Bombay Company Fort Worth, Texas

A laptop that contained customer names, credit card types, last four digits of credit card numbers and phone numbers was stolen. Information about purchase amounts and dates was also on the laptop.

Information Source: Dataloss DB

January 26, 2007 UPS Capital Business Credit, U.S. Farm Credit Administration (FCA) Windsor, Connecticut

An FCA employee's laptop and USB memory drive were lost on November 3. UPS credit loans were being reviewed by FCA. Taxpayer identification numbers, Social Security numbers and loan information may have been exposed.

Information Source: Dataloss DB

January 25, 2007 Clay High School Oregon, Ohio

A former high school student obtained sensitive staff and student information through an apparent security breach. The data was copied onto an iPod and included names, birth dates, SSNs, addresses, and phone numbers.

Information Source: Dataloss DB

January 25, 2007 Ohio Board of Nursing Columbus, Ohio

The agency's Website posted names and SSNs of newly licensed nurses twice in the past two months. The Social Security numbers were supposed to have been removed before posting.

Information Source: Dataloss DB

January 25, 2007 Wahiawa Women, Infants and Children program (WIC) Honolulu, Hawaii


A WIC employee apparently stole the personal information of agency clients, including SSNs, and committed identity theft on at least 3 families and perhaps 2 more. The Health Director said the agency will no longer use SSNs in its data base.
January 25, 2007

**Visiting Nurse Service of New York (VNSNY)**
**New York, New York**

A tablet computer was stolen from a registered nurse. Patient Social Security numbers, names, addresses and telephone numbers were on the tablet. VNSNY warned patients that people might use the information and tablet to pose as VNSNY employees.

January 24, 2007

**Cornell University**
**Detroit, Michigan**

An employee laptop was lost after being checked as baggage at Detroit Metropolitan International Airport. It contained names, Social Security numbers and credit card numbers of some people.

January 23, 2007

**Rutgers-Newark University, Political Science Department**
**Newark, New Jersey**

An associate professor’s laptop was stolen, containing names and SSNs of 200 students. Rutgers no longer uses SSNs as student IDs, but student IDs from past years are still SSNs.

January 23, 2007

**Xerox**
**Wilsonville, Oregon**

A laptop was stolen from a human resources manager’s car. Some of the employees affected by the incident experienced credit problems before being informed that the theft had put them at risk. One employee had multiple cell phone accounts taken out in his name a month and a half after the theft.

January 22, 2007

**U.S. Department of Veterans Affairs**
**Seattle, Washington**

Folders of veterans’ personal information were stolen from a locked car in Bremerton, WA. News stories are not clear on the type of information contained in the folders.

January 22, 2007

**Chicago Board of Election**
**Chicago, Illinois**

About 100 computer discs (CDs) with 1.3 million Chicago voters’ SSNs were mistakenly distributed to aldermen and ward committeemen. The CDs also contain birth dates and addresses.

January 22, 2007

**Sprint Nextel**
**Charlotte, North Carolina**

A laptop computer was stolen from an employee’s home during a late November burglary. Information from customers nationwide was stored on the hard drive. Customers’ names, addresses, Sprint Nextel account numbers and access codes, credit card numbers and phone numbers may have been exposed.

January 20, 2007

**Greenville South Carolina County School District**
**Greenville, South Carolina**

Boxes of personnel records were inadvertently left unsecured during renovations. Ten boxes held the names and Social Security numbers of teachers employed by the district between 1972 and 1990. Other boxes contained personnel records.
through 1998. District officials secured the boxes after receiving an anonymous call about the mistake.

Information Source: Dataloss DB

**January 19, 2007**

**U.S. Internal Revenue Service via City of Kansas City**

*Kansas City, Missouri*  

GOV PORT Unknown

26 IRS computer tapes containing taxpayer information were reported missing after they were delivered to City Hall. They potentially contain taxpayers' names, SSNs, bank account numbers, or employer information. The 26 tapes were the entire shipment received by the City last August. The disappearance was noticed late December 2006.

Information Source: Dataloss DB

**January 19, 2007**

**First Advantage SafeRent, Inc., Z II Investment Group, LLC**

*Philadelphia, Pennsylvania*  

BSF INSD 18

A company named Z II Investment Group, LLC had a number of unauthorized credit reports performed. The unauthorized reports contained name, address, Social Security number, date of birth, and partial credit card number.

Information Source: Dataloss DB

**January 18, 2007**

**KB Home**

*Charleston, South Carolina*  

BSO STAT 2,700

A computer was stolen from one of the home builder's offices. It likely contained names, addresses, and SSNs of people who had visited the sales office for Foxbank Plantation in Berkeley County near Charleston.

Information Source: Dataloss DB

**January 18, 2007**

**Private Medical Practice**

*Cheektowaga, New York*  

MED STAT 10,600

The December 15 office burglary of three computers may have exposed patient information. Names, Social Security numbers, addresses, dates of birth, phone numbers, insurance companies and insurance ID numbers were on the computers.

Information Source: Dataloss DB

**January 17, 2007**

**TJ stores (TJX), including TJMaxx, Marshalls, Winners, HomeSense, AJWright, KMmaxx, and possibly Bob's Stores in U.S. & Puerto Rico -- Winners and HomeGoods stores in Canada -- and possibly TKMaxx stores in UK and Ireland**

Framingham, Massachusetts  

BSR HACK 100,000,000


The TJX Companies Inc. experienced an unauthorized intrusion into its computer systems that process and store customer transactions including credit card, debit card, check, and merchandise return transactions. It discovered the intrusion mid-December 2006. Transaction data from 2003 as well as mid-May through December 2006 may have been accessed. According to its Web site, TJX is the leading off-price retailer of apparel and home fashions in the U.S. and worldwide.

Note on our total: included in this breach are 45,700,000 credit and debit card account numbers; 455,000 merchandise return records containing customer names and driver’s license numbers; recovery of about 200,000 stolen credit card account numbers; records then indicated an additional 48 million people have been affected. Totals were estimated at 94 million but now seem to have affected over 100 million accounts.

**UPDATE** (2/22/2007): TJX said that while it first thought the intrusion took place from May 2006 to January 2007, it now thinks its computer system was also hacked in July 2005 and on various subsequent dates that year.

**UPDATE** (3/21/2007): Information stolen from TJX’s systems was being used fraudulently in November 2006 in an $8 million gift card scheme, one month before TJX officials said they learned of the breach, according to Florida law enforcement officials.

**UPDATE** (3/29/2007): The company reported in its SEC filing that 45.7 million credit and debit card numbers were hacked, along with 455,000 merchandise return records containing customers’ driver’s license numbers; Military ID numbers or Social Security numbers.

**UPDATE** (4/22/2007): Initially, TJX said the break-in started seven months before it was discovered. Then, on Feb. 18, the company noted the perpetrators had access to data for 17 months, and apparently began in July 2005.

**UPDATE** (04/26/2007): Three states’ banking associations (MA, CT, and ME) filed a class action lawsuit against TJX to recover the costs of damages totaling tens of millions of dollars incurred for replacing customers’ debit and credit cards.

**UPDATE** (05/04/2007): An article in the *WSI* notes that because TJX had an outdated wireless security encryption system,
had failed to install firewalls and data encryption on computers using the wireless network, and had not properly install another layer of security software it had bought, thieves were able to access data streaming between hand-held price-checking devices, cash registers and the store's computers. 21 U.S. and Canadian lawsuits seek damages from the retailer for reissuing compromised cards.

UPDATE (07/10/2007): U.S. Secret Service agents found TJX customers' credit card numbers in the hands of Eastern European cyber thieves who created high-quality counterfeit credit cards. Victims are from the U.S., Europe, Asia and Canada, among other places. Several Cuban nationals in Florida were arrested with more than 200,000 credit card account numbers.

UPDATE (08/31/2007): The U.S. Secret Service Agency earlier this week said it has arrested and indicted four members of an organized fraud ring in South Florida, charging each of them with aggravated identity theft, counterfeit credit-card trafficking, and conspiracy.

UPDATE (09/21/2007): A ring leader in the TJX Cos.-linked credit card fraud, was sentenced to five years in prison and has been ordered to pay nearly $600,000 in restitution for damages resulting from stolen financial information.

UPDATE (09/25/2007): TJX announced the terms of a settlement for customers affected by the breach -- with strings attached. Credit monitoring will be offered to about 455,000 of the 46 million affected. TJX will reimburse customers who had to replace driver’s licenses as a result of the breach if they submit documentation for the time and money spent on replacing licenses. The company will give a $30 store voucher to those customers who submit documentation about their lost time and money. And TJX will hold a special 3-day sale with a 15% discount sometime in 2008. The settlement still needs to be approved by the court.

UPDATE (10/23/2007): Court filings in a case brought by banks against TJX say the number of accounts affected by the thefts topped 94 million.

UPDATE (10/23/2007): The total number of records increased from 167 million to 215 million. Recent court filings in a case brought by banks against TJX say the number of accounts affected by the thefts topped 94 million, up considerably from 45.7 million credit and debit card account numbers initially thought to be compromised. Breach costs have been estimated at $216 million.

UPDATE (11/30/2007): Fifth Third Bancorp, the Ohio bank that was fined $880,000 by Visa for its role in the customer data security breach at TJX Cos., the largest ever, also paid fines and compensation totaling $1.4 million following the loss of data from BJ's Wholesale Club Inc.

UPDATE (12/05/2007): An InternetNews.com article estimates TJX expenses at $500 million to $1 billion. In a settlement with VISA USA, TJX will pay a maximum of $40.9 million to fund an alternative recovery payments program for customers affected by the breach. At least 19 lawsuits have been filed, and there are investigations underway by the Federal Trade Commission and 37 state Attorneys General.

UPDATE (12/18/2007): TJX has settled the lawsuit for an undisclosed amount. Although both sides said the settlement total would remain confidential, TJX said the costs were covered by a $107 million reserve that it set aside against its second-quarter earnings. TJX also has said that $107 million would cover the costs of another breach agreement: a Nov. 30 deal with Visa Inc. to help pay a maximum $40.9 million to help pay the network's card-issuing banks recover expenses to replace customers' Visa cards.

UPDATE (2/10/2008): Notices are going out to millions of customers who may have had credit card information compromised in a data breach. The notices contain information about eligibility for compensation such as vouchers and credit monitoring to be provided under a proposed settlement.

UPDATE (4/2/2008): TJX Cos. reached a settlement with MasterCard Inc. in which it will pay up to $24 million to banks and other institutions to cover fraud losses stemming from a massive data breach disclosed last year. They also struck a similar deal with rival card network Visa in which it agreed to pay up to $40.9 million. As in that deal, TJX said the costs of its MasterCard settlement are included in the $256 million the company has set aside to pay for computer work and other costs associated with the breach.

UPDATE (5/14/2008): The TJX Companies, Inc. today announced that it completed its previously announced settlement with MasterCard International Incorporated and its issuers. Financial institutions representing 99.5% of eligible MasterCard accounts worldwide claimed to have been affected by the unauthorized computer intrusion(s) at TJX accepted the alternative recovery offer under TJX's previously announced Settlement Agreement with MasterCard.

UPDATE (8/5/2008): Eleven perpetrators allegedly involved in the hacking of nine major U.S. retailers have been charged with numerous crimes, including conspiracy, computer intrusion, fraud and identity theft. This is the largest hacking and identity theft case ever prosecuted by the U.S. Department of Justice. An indictment was returned on Aug. 5, 2008. Conspirators obtained the credit and debit card numbers by wardriving and hacking into the wireless computer networks of major retailers -- including TJX Companies, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, Sports Authority, Forever 21 and DSW. The indictments are the result of a three-year undercover investigation conducted out of the San Diego Field Office of the U.S. Secret Service.

UPDATE (8/30/2008): TrustCo BankCorp NY sued TJX in August 2008 to recoup costs it incurred from reissuing an estimated 4,000 customer MasterCard debit cards after hackers accessed the TJX computer network. The bank stated its cost for the breach was up to $20 per affected account, explaining that it suffered losses from administrative expenses and lost interest and transaction fees. Later in the month, TJX in turn claimed that Trustco failed to implement policies or procedures that would have enabled the bank to avoid canceling and replacing customer debit cards.

UPDATE (9/22/2008): One of the 11 people arrested last month in connection with the massive data theft at TJX Companies Inc., BJ Wholesale Clubs Inc. and several other retailers pleaded guilty yesterday to four felony counts, including wire and credit card fraud and aggravated identity theft. Many of the Internet attacks that he facilitated were SQL injection attacks, according to court documents. The stolen data was sold to cyber criminals in Eastern Europe and the U.S. or used to make fraudulent credit and debit cards.

UPDATE (6/26/2009): TJX has agreed to pay $9.75 million to 41 states and to implement and maintain a comprehensive...
Information security program, designed to safeguard consumer data and address any weaknesses in TJX's systems in place at the time of the breach. Of the $9.75 million monetary payment under the settlement, $5.5 million is to be dedicated to data protection and consumer protection efforts by the states, and $1.75 million is to reimburse the costs and fees of the investigation. Further, $2.5 million of the settlement will fund a Data Security Trust Fund to be used by the state Attorneys General to advance enforcement efforts and policy development in the field of data security and protecting consumers' personal information.

**UPDATE (7/28/2009):** Pennsylvania and 40 other states reached a $9.75 million settlement.

**UPDATE (9/4/2009):** TJX settles for $525K with four banks. As part of the settlement with AmeriFirst Bank, Trustco Bank, HarborOne Credit Union and SELCO Community Credit Union, the Framingham, Mass.-based retailer paid $525,000. The money primarily will be used to cover the banks' expenses in pursuing the legal action.

**UPDATE (12/15/2009):** A Miami hacker who had already pleaded guilty to computer fraud and identity theft for breaches at retailers T.J. Maxx, OfficeMax, and many other merchants, pleaded guilty on Tuesday to similar charges related to breaches at Heartland Payment Systems, 7-Eleven, Hannaford Brothers supermarkets, and two other companies. Albert Gonzalez, 28, reiterated terms of a plea agreement in U.S. District Court in Boston. A week earlier, co-conspirator Stephen Watt of New York, appeared in that same court and was ordered to serve two years in prison and pay $171.5 million in restitution for developing a sniffing program used to grab payment card data in the breach at the TJX companies between 2003 and 2008.

**UPDATE (3/17/2010):** Humza Zaman, a co-conspirator in the hack of TJX and other companies, was sentenced in Boston to 46 months in prison and fined $75,000 for his role in the conspiracy. The sentence matches what prosecutors were seeking. Zaman was charged with laundering between $600,000 and $800,000 for hacker Albert Gonzalez, who is currently awaiting sentencing on charges that he and others hacked into TJX, Office Max, Heartland Payment Systems and numerous other companies to steal data on more than 100 million credit and debit card accounts. Zaman pleaded guilty in April to one count of conspiracy. His sentence includes three years of supervised release with the condition that Zaman must disclose his conviction to any future employer. Upon release, Zaman will not be barred from using computers. Zaman is the second conspirator in the TJX case to be charged. Former Morgan Stanley coder, Stephen Watt, was sentenced in December to two years in prison for his role in the TJX case, which involved supplying Gonzalez with a sniffer program used to siphon card data from the TJX network.

**UPDATE (3/29/2010):** A 28-year-old college dropout who became the world's biggest credit card hacker on Thursday was sentenced to 20 years in prison for stealing millions of credit union and bank account records from T.J. Maxx, Office Max, Dave & Buster's, Barnes & Noble and a string of other companies - even as he was working as a $75,000-a-year underground informant for the U.S. government in identity theft cases. But that's not the end of it, as Albert Gonzalez is scheduled to be sentenced again to additional years behind bars for additional data thefts at Heartland Payment Systems, Hannaford Bros. supermarkets and 7-Eleven convenience stores. The theft of credit card data cost financial institutions, insurers and cardholders an estimated $200 million, according to law enforcement. JC Penney and Wet Seal were both officially added to the list of retail victims of Albert Gonzalez on Friday (March 26) when U.S. District Court judge Douglas P. Woodlock refused to continue their cloak of secrecy and removed the seal from their names. StorefrontBacktalk had reported last August that $17 billion JC Penney chain was one of Gonzalez's victims, even though JC Penney's media representatives were denying it. But the $561 million chain Wet Seal, which has 504 stores in 47 states, Washington, D.C. and Puerto Rico, had kept their identity secret. No more and that's the way Woodlock wanted it.

**UPDATE (4/16/2010):** Damon Patrick Toey, the 'trusted subordinate' of TJX hacker Albert Gonzalez, was sentenced in Boston to 5 more years in prison. He also received a $100,000 fine and three years. supervised release, according to the Justice Department.

**UPDATE (7/8/2010):** TJX has settled another lawsuit. The Louisiana Municipal Police Employees' Retirement System, a shareholder of TJX stock, settled with TJX for $595,000 in legal fees and enhanced oversight of customer files.

**UPDATE (4/8/2011):** Albert Gonzalez is appealing his conviction for his role in a large data breach by claiming that his actions were authorized by the Secret Service. The government acknowledged that Gonzalez was a key undercover Secret Service informant at the time of the breaches. In a 25-page petition, Gonzalez faulted one of his attorney's for failing to prepare a "Public Authority" defense, which would have argued that he committed crimes with the approval of government authorities.

Information Source: DataLoss DB

**January 17, 2007**  
**Rincon del Diablo Municipal Water District**  
**Escondido, California**  
GOV  STAT  500

Additional locations: unincorporated neighborhoods outside the city, and parts of San Marcos and San Diego, CA. (760) 745-5522

Two computers were stolen from the district office. One included names and credit card numbers of customers.

Information Source: DataLoss DB

**January 16, 2007**  
**University of New Mexico**  
**Albuquerque, New Mexico**  
EDU  STAT  Unknown

At least 3 computers and 4 monitors were stolen from the associate provost's office overnight between Jan. 2 and 3. They may have included faculty members' names and SSNs.

Information Source: DataLoss DB

**January 17, 2007**  
**Rincon del Diablo Municipal Water District**  
**Escondido, California**  
GOV  STAT  500

Additional locations: unincorporated neighborhoods outside the city, and parts of San Marcos and San Diego, CA. (760) 745-5522

Two computers were stolen from the district office. One included names and credit card numbers of customers.

Information Source: DataLoss DB

**January 16, 2007**  
**University of New Mexico**  
**Albuquerque, New Mexico**  
EDU  STAT  Unknown

At least 3 computers and 4 monitors were stolen from the associate provost's office overnight between Jan. 2 and 3. They may have included faculty members' names and SSNs.
January 13, 2007  North Carolina Department of Revenue  Raleigh, North Carolina  

A laptop computer containing taxpayer data was stolen from the car of a NC Dept. of Revenue employee in mid-December. The files included names, SSNs or federal employer ID numbers, and tax debt owed to the state.

Information Source:  Dataloss DB  

January 12, 2007  MoneyGram International  Minneapolis, Minnesota  

MoneyGram, a payment service provider, reported that a company server was unlawfully accessed over the Internet last month. It contained information on about 79,000 bill payment customers, including names, addresses, phone numbers, and in some cases, bank account numbers.

Information Source:  Media  

January 11, 2007  University of Idaho  Moscow, Idaho  

Over Thanksgiving weekend, 3 desktop computers were stolen from the Advancement Services office containing personal information of alumni, donors, employees, and students. 331,000 individuals may have been exposed, with as many as 70,000 records containing SSNs, names and addresses.

Information Source:  Dataloss DB  


A former employee of an affiliated company accessed customer records and was eventually discovered to be part of a credit card fraud investigation. The records found included names, addresses, Social Security numbers and dates of birth.

Information Source:  Dataloss DB  

January 10, 2007  University of Arizona  Tucson, Arizona  

Breaches occurred in November and December 2006 that affected services with UA Student Unions, University Library, and UA Procurement and Contracting Services. Some services were shut down for several days.

Information Source:  Dataloss DB  

January 10, 2007  Advent Software Inc.  San Francisco, California  

A laptop was stolen from the office on or around November 20. It contained employee Social Security numbers and addresses. Employees were notified in December. At least 21 New Hampshire residents were affected, but the total number of affected individuals nationwide was not revealed.

Information Source:  Dataloss DB  

January 10, 2007  New Hope Church  Durham, North Carolina  

Current and former employee information was on a stolen laptop. The laptop was taken from the church offices during a December 31 burglary. Names, Social Security numbers, addresses and payroll information was on the stolen laptop.

Information Source:  Dataloss DB  

January 9, 2007  Towers Perrin  New York, New York  

30,000 taxpayers
Around 18,000 past and present employees, presumably of Altria, and 6,300 employees of Philip Morris were affected.

Five laptops were stolen from Towers Perrin, allegedly by a former employee. The theft occurred Nov. 27, 2006. The computers contain names, SSNs, and other pension-related information, presumably of several companies, although news reports are not clear. Companies named include Altria (unknown number, possibly 18,000 employees) and Philip Morris (6,300 employees).

UPDATE (1/11/07): NY police arrested a junior-level administrative employee of the company in the theft of the laptops.


Information Source: Dataloss DB

January 9, 2007 Mercer Health and Benefits

A laptop computer was stolen from a vehicle.

Information Source: Dataloss DB

January 5, 2007 Dr. Baceski’s office, internal medicine
Somerset, Pennsylvania

A hard drive was stolen containing personal information on hundreds of patients.

Information Source: Media

January 4, 2007 Selma, North Carolina, Water Treatment Plant
Johnston County, North Carolina

A laptop stolen from the water treatment facility holds the names and SSNs of Selma volunteer firefighters.

Information Source: Dataloss DB

January 3, 2007 Academic Magnet High School
North Charleston, South Carolina

A recent burglary makes it the third time that computers were stolen during campus burglaries. Two other incidents occurred in November. Student information was on the laptop stolen in the recent burglary. School officials felt that risk of identity theft was extremely low because the information was password protected and encrypted.

Information Source: Dataloss DB

January 2, 2007 Notre Dame University
Notre Dame, Indiana

Additional location: South Bend, IN

A University Director’s laptop was stolen before Christmas. It contained personal information of employees, including names, SSNs, and salary information.

Information Source: Dataloss DB

January 2, 2007 News accounts are not clear as to source, but thought to be a realty office
Las Vegas, Nevada

About 40 boxes of financial paperwork, thought to be from loan applications, was found in a dumpster. One of the boxes visible to news reporters was said to contain paperwork with bank account details, photocopies of driver’s licenses, SSNs
and other private information.

Information Source: Media

January 2, 2007  
BayRock Mortgage  
Alpharetta, Georgia

The location listed is the BayRock office and may not be where the theft occurred.

A laptop with investor information was lost when an employee’s rental car that it was in was stolen.

Information Source: Dataloss DB

January 1, 2007  
Wisconsin Department of Revenue via Ripon Printers  
Madison, Wisconsin

Tax forms were mailed to taxpayers in which SSNs were inadvertently printed on the front of some Form 1 booklets. Some were retrieved before they were mailed.

Information Source: Dataloss DB

(608) 224-5163,  
http://privacy.wi.gov/alerts/jan0107.jsp

January 1, 2007  
Wisconsin Department of Revenue via Ripon Printers  
Madison, Wisconsin

Information Source: Dataloss DB

December 30, 2006  
KeyCorp  
Cleveland, Ohio

A laptop computer stolen from a KeyCorp vendor contains personally identifiable information, including SSNs, of 9,300 customers in six states.

Information Source: Dataloss DB

December 30, 2006  
U.S. State Department  
Washington, District Of Columbia

A bag containing approximately 700 completed passport applications, which included Social Security numbers, was reported missing on December 1. The bag, which was supposed to be shipped to Charlotte, NC, was found later in the month at Los Angeles International Airport.

Information Source: Dataloss DB

December 27, 2006  
Montana State University  
Bozeman, Montana

A student working in the loan office mistakenly sent packets containing lists of student names, Social Security numbers, and loan information to other students.

Information Source: Dataloss DB

December 27, 2006  
Deaconess Hospital  
Evansville, Indiana

A computer missing from the hospital holds personal information, including SSNs, of 128 respiratory therapy patients.

Information Source: Dataloss DB

December 22, 2006  
Texas Woman's University  
Dallas, Texas

Additional locations: Denton and Houston, TX

A document containing names, addresses and SSNs of 15,000 TWU students was transmitted over a non-secure connection.

Information Source: Media

December 22, 2006  
Utah Valley State College  
Orem, Utah

171,000 taxpayers

713
Social Security numbers and other personal information of students and faculty were accessible via Yahoo’s search engine. The information was removed from UVSC’s servers. Some Distance Education instructors and some students enrolled in UVSC courses between January 2002 and January 2005 were affected.

Information
Source: Dataloss DB
December 21, 2006  Hunter College of the City University of New York
New York, New York

The full names and Social Security numbers of certain individuals were on a spreadsheet that an employee emailed to a group of students on November 8. Students were instructed to delete the file after the discovery. At least 140 New York residents were affected, but the total number of people affected nationwide was not revealed.

Information
Source: Dataloss DB
December 21, 2006  Santa Clara County employment agency
Santa Clara County, California

A computer stolen from the agency holds the SSNs of approximately 2,500 individuals.

Information
Source: Dataloss DB
December 21, 2006  Goal Financial, LLC
San Diego, California

The location listed is the headquarters. It is not clear where the incident took place.

A portion of borrowers’ names and Social Security numbers were on four hard drives that were accidentally sold before being wiped clean. Employees transferred more than 7,000 files with consumer information to third parties without authorization, and one employee sold the hard drives to the public surplus. The hard drives were retrieved after the mistake was realized on June 13. Affected individuals were notified in June. The student loan company agreed to settle FTC charges in December. The company violated the FTC’s Privacy Rule by failing to take reasonable and appropriate measures to protect personal information.

Information
Source: Dataloss DB
December 21, 2006  Wake County Public School System
Raleigh, North Carolina

A flash drive that contained employee names and Social Security numbers was misplaced. The flash drive was found two days later.

Information
Source: Dataloss DB
December 21, 2006  City University of New York
New York, New York

Confidential data from the University server was accidentally made available through a Google search. The error was discovered on October 17 and faculty, students and staff were affected. The information included full names, Social Security numbers, dates of birth, addresses, email addresses and University library identification card numbers. The copy of the file was removed from Google on October 20.

Information
Source: Dataloss DB
December 21, 2006  New York City Human Resources Administration
Brooklyn, New York

Information from the Office of Temporary and Disability Assistance and the New York State Department of Health was exposed.

A hard drive with human resources information was discovered to be missing. The hard drive may have had temporary and disability assistance applicant reports with names, Social Security numbers and dates of birth.

Information
Source: Dataloss DB
December 20, 2006  Lakeland Library Cooperative
Grand Rapids, Michigan

Information from the Office of Temporary and Disability Assistance and the New York State Department of Health was exposed.

A hard drive with human resources information was discovered to be missing. The hard drive may have had temporary and disability assistance applicant reports with names, Social Security numbers and dates of birth.
Lakeland Library Cooperative serves 80 libraries in eight counties.

Personal information of 15,000 library users in West Michigan was displayed on the Cooperative's Web site due to a technical problem. Information exposed included names, phone numbers, e-mail addresses, street addresses, and library card numbers. Children's names were also listed along with their parents' names on a spreadsheet document. The information has since been removed.

**Information Source:**
Dataloss DB

December 20, 2006  **Big Foot High School**  
Walworth, Wisconsin

Personal information was accidentally exposed on the High School's Web site for a short time, perhaps for about 36 minutes, according to a report. Information included last names, SSNs, and birthdates. Current and former employees were affected.

**Information Source:**
Dataloss DB

December 20, 2006  **Lake County residents and Major League Baseball players**  
Northbrook, Illinois

A Chicago man apparently removed documents from a trash bin outside SFX Baseball Inc., a sports agency that deals with Major League Baseball. Some current and former MLB players and county residents were affected. He used information from the documents to commit identity theft. Information found during a search of the thief's home included SSNs, dates of birth, canceled paychecks, obituaries, and infant death records.

**Information Source:**
Dataloss DB

December 20, 2006  **Deb Shops, Inc.**  
Philadelphia, Pennsylvania

A hacker illegally accessed company Web pages and a related data base used for Internet-based purchases. The intruder may have accessed customers' credit card information including names on cards and credit card numbers.

**Information Source:**
Dataloss DB

December 19, 2006  **Mississippi State University**  
Jackson, Mississippi

SSNs and other personal information were inadvertently posted on a publicly accessible MSU Web site. The breach was discovered last week and the information has since been removed.

**Information Source:**
Dataloss DB

December 19, 2006  **Velocita Wireless, Sprint Nextel**  
Woodbridge, New Jersey

A laptop from the human resources department was stolen during an office burglary on or around October 24. It contained current and former employee names, dates of birth, Social Security numbers and salary information. Affected individuals were contacted between December 13 and 15.

**Information Source:**
Dataloss DB

December 15, 2006  **University of Colorado, Boulder, Academic Advising Center**  
Boulder, Colorado

A server in the Academic Advising Center was the subject of a hacking attack. Personal information exposed included names and SSNs for individuals who attended orientation sessions from 2002-2004. CU-Boulder has since ceased using SSNs as identifiers for students, faculty, staff, and administrators.

http://www.colorado.edu/its/security/awareness/privacy/identitytheft.pdf
December 15, 2006  
City of Wickliffe  
Wickliffe, Ohio  
GOV  HACK  125 employees

Hackers breached security in one of the city's three computer servers containing personal information on some city employees, including names and SSNs.

December 15, 2006  
North Bay Regional Center  
Napa, California  
NGO  STAT  3,000

Thieves took 30 computers and electronic devices from the office. Personal information of clients may have been on some of the computers. This included credit card information for some clients.

December 15, 2006  
City University of New York  
New York, New York  
EDU  STAT  445

Two computers were stolen from the York Support Services office. The computers contained databases including full names, Social security numbers and dates of birth.

December 15, 2006  
LexisNexis, Seisint  
Boca Raton, Florida  
BSO  INSD  618

Unauthorized individuals used the ID and password of a Seisint law enforcement customer to obtain consumers' Social Security numbers, driver's license numbers, names and addresses. The breach was discovered on October 18 and affected individuals were contacted on December 5.

December 14, 2006  
Electronic Registry Systems  
Atlanta, Georgia  
MED  PORT  63,000

Additional locations: Danville, Pennsylvania, Nashville, TN

On Nov. 23, 2006, two computers (one desktop, one laptop) were stolen from Electronic Registry Systems, a business contractor in suburban Springdale, OH, that provides cancer patient registry data processing services. It contained the personal information (name, date of birth, Social Security number, address, medical record number, medical data and treatment information) of cancer patients from hospitals in Pennsylvania, Tennessee, Ohio and Georgia, dating back to 1977 at some hospitals. Hospitals include Emory Hospital, Emory Crawford Long Hospital, Grady Memorial Hospital, as well as Geisinger Health System (PA) and Williamson Medical Center (TN).

UPDATE (1/14/07): The number of affected patients was increased from 25,000 to over 63,000.

December 14, 2006  
Riverside High School  
Durham, North Carolina  
EDU  DISC  Thousands of school employees (at least 2,000)

Two students discovered a breach in the security of a Durham Public Schools computer as part of a class assignment. They reported to school officials that they were able to access a database containing SSNs and other personal information of thousands of school employees. The home of one student was searched by Sheriff's deputies and the family computer was seized.

December 14, 2006  
St. Vrain Valley School District  
Longmont, Colorado  
EDU  PHYS  600 students

Paper records containing student information were stolen, along with a laptop, from a nurse’s car Nov. 20. Personal information included students’ names, dates of birth, names of their schools, what grade they are in, their Medicaid
numbers (presumably SSNs), and their parents' names. The laptop contained no personal data.

Information
Source: Dataloss DB
December 14, 2006  
Bank of America
Charlotte, North Carolina
BSF  INSD  Unknown

A former contractor for Bank of America unauthorizedly accessed the personal information (name, address, phone number, Social Security number) of an undisclosed number of customers, for the purpose of committing fraud.

Information
Source: Dataloss DB
December 13, 2006  
Boeing
Seattle, Washington
BSO  PORT  382,000 current and former employees

In early December, a laptop was stolen from an employee's car. Files contained names, salary information, SSNs, home addresses, phone numbers and dates of birth of current and former employees.

UPDATE (12/14/06): Boeing fired the employee whose laptop was stolen.

UPDATE (1/26/07): The laptop was recovered.

Information
Source: Dataloss DB
December 13, 2006  
Seton Health System
Long Island, New York
MED  PORT  14

The December 8 theft of a laptop may have exposed clinical and personal information. The information included names, Social Security numbers, addresses, dates of birth, medical record information, telephone number, and insurance information. The laptop was stolen from a Seton Home Health Care nurse's car.

Information
Source: Dataloss DB
December 12, 2006  
University of California at Los Angeles (UCLA)
Los Angeles, California
EDU  HACK  800,000

Affected individuals can call UCLA at (877) 533-8082, http://www.identityalert.ucla.edu

Hacker(s) gained access to a UCLA database containing personal information on current and former students, current and former faculty and staff, parents of financial aid applicants, and student applicants, including those who did not attend. Exposed records contained names, SSNs, birth dates, home addresses, and contact information. About 3,200 of those notified are current or former staff and faculty of UC Merced and current and former staff of UC’s Oakland headquarters.

Information
Source: Media
December 12, 2006  
University of Texas, Dallas
Dallas, Texas
EDU  HACK  35,000

Affected individuals can call (972) 883-4325, http://www.utdallas.edu/datacompromise/form.html

The University discovered that personal information of current and former students, faculty members, and staff may have been exposed by a computer network intrusion -- including names, SSNs, home addresses, phone numbers and e-mail addresses.

UPDATE (12/14/06): The number of people affected was first thought to be 5,000, but was increased to 6,000.

UPDATE (01/19/07): Officials now say 35,000 individuals may have been exposed.

Information
Source: Dataloss DB
December 12, 2006  
Aetna, Nationwide, WellPoint Group Health Plans, Humana Medicare, Mutual of Omaha Insurance Company, Anthem Blue Cross Blue Shield via Concentra Preferred Systems
Dayton, Ohio
MED  PORT  396,279

A lockbox holding personal information of health insurance customers was stolen Oct. 26. Thieves broke into an office building occupied by insurance company vendor, Concentra Preferred Systems. The lockbox contained computer backup tapes of medical claim data for Aetna and other Concentra health plan clients. Exposed data includes member names, hospital codes, and either SSNs or Aetna member ID numbers. SSNs of 750 medical professionals were also exposed. Officials downplay the risk by stating that the tapes cannot be used on a standard PC.
Officials downplay the risk by stating that the tapes cannot be used on a standard PC.

**UPDATE** (12/23/06): The lockbox also contained tapes with personal information of 42,000 NY employees insured by Group Health Insurance Inc.

**UPDATE** (1/24/07): Personal data of 28,279 Nationwide's Ohio customers were also compromised. 2/11/10 Total changes to 396,279 to reflect final total of records breached in all of the affected companies.

**Information Source:**

<table>
<thead>
<tr>
<th>Date</th>
<th>Company</th>
<th>Location</th>
<th>Records from this breach used in our total:</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 9,</td>
<td><strong>Home Finance &amp; Mortgage, Inc.</strong></td>
<td>Cornelius, North Carolina</td>
<td>146</td>
</tr>
<tr>
<td>2006</td>
<td></td>
<td></td>
<td>records from this breach used in our total: 146</td>
</tr>
<tr>
<td></td>
<td>The company dumped files containing names,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>addresses, Social Security numbers, credit</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>card numbers, and bank account numbers of</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>people who had applied for mortgage loans.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Home Finance and its owners have agreed to</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>pay the State of NC $3,000 for their</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>violations.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Information Source:**

<table>
<thead>
<tr>
<th>Date</th>
<th>Company</th>
<th>Location</th>
<th>Records from this breach used in our total:</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 9,</td>
<td><strong>Virginia Commonwealth University (VCU)</strong></td>
<td>Richmond, Virginia</td>
<td>561 students</td>
</tr>
<tr>
<td>2006</td>
<td></td>
<td></td>
<td>records from this breach used in our total: 561</td>
</tr>
<tr>
<td></td>
<td>Personal information of 561 students was</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>inadvertently sent as attachments on Nov. 20</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>in an e-mail, including names, SSNs, local</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>and permanent addresses and grade-point</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>averages. The e-mail was sent to 195 students</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>to inform them of their eligibility for</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>scholarships.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Information Source:**

<table>
<thead>
<tr>
<th>Date</th>
<th>Company</th>
<th>Location</th>
<th>Records from this breach used in our total:</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 8,</td>
<td>**Segal Group of New York, via a Vermont</td>
<td>Montpelier, Vermont</td>
<td>1,100</td>
</tr>
<tr>
<td>2006</td>
<td>state agency website**</td>
<td></td>
<td>records from this breach used in our total: 1,100</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Names and SSNs of several hundred physicians,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>psychologists and other health care</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>providers were mistakenly posted online by</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Segal Group, a contractor hired by the state</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>to put its health management contract out</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>for bid. The information was posted from</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>May 12 to June 19. It was discovered when a</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>doctor found her own SSN online. A Vermont</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>state agency used to call for bids on state</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>contracts was involved.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>UPDATE</strong> (1/14/07): SSNs of more than</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1,100 doctors, psychothereapists and other</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>health professionals were exposed.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Information Source:**

<table>
<thead>
<tr>
<th>Date</th>
<th>Company</th>
<th>Location</th>
<th>Records from this breach used in our total:</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 8,</td>
<td><strong>Experian, BMA Credit Union</strong></td>
<td>Mesquite, Texas</td>
<td>46</td>
</tr>
<tr>
<td>2006</td>
<td></td>
<td></td>
<td>records from this breach used in our total: 46</td>
</tr>
<tr>
<td></td>
<td>An unauthorized Experian client accessed</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>consumer personal information. The</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>information included name, Social Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>number and address. At least 46 New York</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>residents were affected, but the total</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>number nationwide was not revealed.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Information Source:**

<table>
<thead>
<tr>
<th>Date</th>
<th>Company</th>
<th>Location</th>
<th>Records from this breach used in our total:</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 7,</td>
<td><strong>CIGNA HealthCare Corp</strong></td>
<td>Pittsburgh, Pennsylvania</td>
<td>Unknown</td>
</tr>
<tr>
<td>2006</td>
<td></td>
<td></td>
<td>records from this breach used in our total: Unknown</td>
</tr>
<tr>
<td></td>
<td>A former employee used customer credit card</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>information.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Information Source:**

<table>
<thead>
<tr>
<th>Date</th>
<th>Company</th>
<th>Location</th>
<th>Records from this breach used in our total:</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 7,</td>
<td><strong>Cornell University</strong></td>
<td>Ithica, New York</td>
<td>210</td>
</tr>
<tr>
<td>2006</td>
<td></td>
<td></td>
<td>records from this breach used in our total: 210</td>
</tr>
<tr>
<td></td>
<td>A laptop was stolen from an employee. Names</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>and Social Security numbers were on the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>computer.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Information Source:**

<table>
<thead>
<tr>
<th>Date</th>
<th>Company</th>
<th>Location</th>
<th>Records from this breach used in our total:</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 6,</td>
<td><strong>Premier Bank</strong></td>
<td>Columbia, Missouri</td>
<td>1,800 customers</td>
</tr>
<tr>
<td>2006</td>
<td></td>
<td></td>
<td>records from this breach used in our total: 1,800 customers</td>
</tr>
<tr>
<td></td>
<td>Headquarters in Jefferson City, MO</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A report was stolen the evening of Nov. 16</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>from the car of the bank's VP and CFO while</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>employees were celebrating an award</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>received by the bank. The document contained</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>names and account numbers of customers, but</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>reportedly no SSNs.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
December 5, 2006  
**Army National Guard 130th Airlift Wing**  
Charleston, West Virginia  
GOV  PORT  Unknown

A laptop was stolen from a member of the unit while he was attending a training course. It contained names, SSNs, and birth dates of everyone in the 130th Airlift Wing.

December 5, 2006  
**Nassau Community College**  
Garden City, New York  
EDU  PHYS  21,000

A printout is missing that contains information about each of NCC’s 21,000 students, including names, SSNs, addresses, and phone numbers. It disappeared from a desk in the Student Activities Office.

December 3, 2006  
**City of Grand Prairie**  
Grand Prairie, Texas  
GOV  DISC  hundreds of employees (at least 200)

Employees of the city of Grand Prairie were notified that personal records were exposed on the city’s website for at least a year. Included were the names and SSNs of hundreds of employees. The information has since been removed. The city had been working with a contractor on a proposal for workers’ compensation insurance. Along with the proposal, names and SSNs were mistakenly listed.

December 1, 2006  
**TD Ameritrade**  
Omaha, Nebraska  
BSF  PORT  300  
(201) 369-8373

According to a letter sent to around 300 current and former employees, a laptop was removed (presumably stolen) from the office Oct. 18, 2006, that contained unencrypted information including names, addresses, dates of birth, and SSNs.

December 1, 2006  
**First Banks Inc**  
Louisville, Kentucky  
BSF  PORT  Unknown

A laptop was stolen from the locked office of an employee during a nighttime burglary on November 20. Loan applications, financial statements and credit reports with client names, addresses and Social Security numbers were on the laptop. At least two New York residents were affected, but the total number of affected clients nationwide was not revealed.

November 30, 2006  
**Pennsylvania Department of Transportation (PennDOT)**  
Dunmore, Pennsylvania  
GOV  STAT  11,384

Affected individuals can call (800) PENNDOT if you have questions.

Thieves stole equipment from a driver’s license facility late evening Nov. 28, including computers containing personal information on more than 11,000 people. Information included names, addresses, dates of birth, driver’s license numbers and both partial and complete SSNs (complete SSNs for 5,348 people). Also stolen were supplies used to create drivers licenses and photo IDs. The state maintains 97 driver’s license facilities.

November 30, 2006  
**TransUnion Credit Bureau, Kingman, AZ, court office**  
Chester, Pennsylvania  
BSF  HACK  1,700

Four different scam companies downloaded the credit information of more than 1,700 individuals, including their credit histories and SSNs. They were able to illegitimately obtain the password to the TransUnion account held by the Kingman, AZ, court office, which apparently has a subscription to the bureau’s services.
A Medical Center employee used patient information, including SSNs and dates of birth, to apply for credit cards in their names. As patient liaison, her duties included insurance coverage, registration, and scheduling appointments. She was arrested for 37 counts of identity theft, and was convicted of identity theft and uttering forged writing, according to the criminal complaint.

Shareholders of Republic Bank Limited were mailed letters with their Social Security numbers visible through the address window of the envelope. Computershare is the registered transfer agent for Republic Bank common stock.

A laptop was stolen from the personal car of a Kaiser employee in California on Oct. 4. It contained names, Kaiser ID number, date of birth, gender, and physician information. The data did not include SSNs.

An employee's USB drive was inside a purse stolen from a car trunk. It contained personal information on 48 faculty members and more than 2,500 students and applicants of a teacher credentialing program. Information included names, SSNs, campus ID numbers, phone numbers, and e-mail addresses.

Information was removed from the site within an hour after officials became aware of the situation.

School district computers sold to the WH Group at auctions between 1999 and early 2006 contained the birth dates, SSNs, driver's license numbers and Department of Juvenile Justice records of approximately 100,000 students. The computers also held sensitive data for more than 1,000 school district employees.

UPDATE(12/10/06): A judge ordered the WH Group to return the computers and the confidential data on them to the school district.
A company hired to print and mail health insurance information to former Chicago Public School employees mistakenly included a list of the names, addresses and SSNs of the nearly 1,740 people receiving the mailing. Each received the 125-page list of the 1,740 former employees.

**Information Source:**
Dataloss DB

**November 25, 2006**
**Family Health Center of Clark County**
**Jeffersonville, Indiana**

Two computers stolen from an Indiana state health department contractor, the Family Health Center of Clark Count, contained the names, addresses, birth dates, SSNs and medical and billing information for more than 7,500 women. The data were collected as part of the state's Breast and Cervical Cancer Program.

**Information Source:**
Dataloss DB

**November 20, 2006**
**Administration for Children's Services**
**New York, New York**

More than 200 case files from the Emergency Children's Services Unit of ACS were found on the street in a plastic garbage bag. The files contain sensitive information of families, social workers and police officers.

**Information Source:**
Dataloss DB

**November 20, 2006**
**Haywood Mortgage Associates Inc.**
**Bethesda, Maryland**

A former employee is believed to have downloaded confidential client information to a USB device shortly before leaving the company. Client names, Social Security numbers, addresses, dates of birth, driver's license numbers, credit card account numbers, mortgage loan account numbers, auto and personal loan numbers, employment information and credit reports could have been taken. The incident occurred sometime around September 7. Clients were notified on January 8 of 2007.

**Information Source:**
Dataloss DB

**November 20, 2006**
**Bank of Jena, Experian**
**Jena, Louisiana**

An unauthorized user was able to access Experian consumer information through the Bank of Jena. Names, Social Security numbers, addresses, dates of birth and account numbers could have been accessed. At least 29 New York residents were affected, but the total number of residents affected nationwide was not revealed.

**Information Source:**
Dataloss DB

**November 18, 2006**
**KeyCorp**
**Cleveland, Ohio**

An email containing a spreadsheet with the SSN, name, address and closed account number of 17 NY residents was accidentally emailed to an external client distribution list of 159 businesses and individuals on or around November 9. The recipients were asked to destroy the email. It is not clear if the 17 New York residents were the only people affected by this incident.

**Information Source:**
Dataloss DB

**November 17, 2006**
**Jefferson College of Health Sciences**
**Roanoke, Virginia**

An email containing the names and SSNs of 143 students intended for one employee was inadvertently sent to the entire student body of 900.

**Information Source:**
Dataloss DB
The October 27 theft of an employee's laptop exposed employee information. A list of employees dating back to December 2004 was on the hard drive of the laptop. Employee names, Social Security numbers and salary information may have been exposed.

**Information Source:** Dataloss DB

**November 16, 2006**

**American Cancer Society (ACS)**

**Louisville, Kentucky**

Headquarters in Atlanta, GA. If you have tips, call (502) 574-5673

An unspecified number of laptop computers were stolen from the Louisville offices of the American Cancer Society. It is not clear what personal information was exposed, if any.

**Information Source:** Media

**November 15, 2006**

**Internal Revenue Service (IRS)**

**Washington, District Of Columbia**

According to documents obtained under the Freedom of Information Act, 478 laptops were either lost or stolen from the IRS between 2002 and 2006. 112 of the computers held sensitive taxpayer information such as SSNs.

**UPDATE (04/05/07):** A report by the Treasury Inspector General for Tax Administration noted that at least 490 IRS computers have been stolen or lost since 2003 in 387 security breach incidents that potentially jeopardized taxpayers' personal information.

**UPDATE (04/17/07):** The Inspector General’s assessment of 20 buildings in 10 cities discovered four separate locations at which hackers could have easily gained access to IRS computers and taxpayer data using wireless technology.

**Information Source:** Media

**November 15, 2006**

**Boeing, Co**

**Chicago, Illinois**

A laptop was stolen from an employee's home on or around November 6. The laptop contained salary planning files from 2002 that had Social Security numbers, names, driver's licenses and state identification numbers. Credit and debit card numbers, security codes and passwords for financial accounts may have also been exposed.

**Information Source:** Dataloss DB

**November 15, 2006**

**Look Tours LLC**

**North Las Vegas, Nevada**

A number of computers were stolen during a September 28 office burglary. Some of the information on the computers included name, address, email address and credit card number and information. Customers and some current and former employees and consultants were affected.

**Information Source:** Dataloss DB

**November 15, 2006**

**Stony Brook University**

**Stony Brook, New York**

A computer stolen on August 15 contained names and Social Security numbers. People involved in the Professional Teachers Program were affected. An employee of a moving company used by the University is believed to be responsible for the theft. The computer was returned on October 6 and was used by unauthorized persons during its absence.

**Information Source:** Dataloss DB

**November 15, 2006**

**Expedia Corporate Travel (now Egencia)**

**Bellevue, Washington**

A former call center employee somehow gained access to credit card numbers and may have misused the information. The former employee attempted to make unauthorized charges at least twice. The discovery was made on October 24.

**Information Source:** Dataloss DB
On Oct. 15, a laptop computer was discovered stolen from the college. (It has since been recovered by law enforcement). The computer contains Social Security numbers and other data for Connors students plus 22,500 high school graduates who qualify for the Oklahoma Higher Learning Access Program scholarships.

Information
Source: Dataloss DB
Records from this breach used in our total: 22,500

1-888-222-8086

The names and Social Security numbers of Hertz employees dating back to 2002 were discovered on the home computer of a former employee.

Information
Source: Dataloss DB
Records from this breach used in our total: 0

A disk containing the personal information of approximately 1,000 KSL employees is missing. KSL is a contractor for Los Alamos National Laboratory.

Information
Source: Dataloss DB
Records from this breach used in our total: 1,000

Paper documents were lost when the package containing them was damaged by a carrier's mechanical equipment. The documents may have been thrown away by the carrier. The information on the documents included name, Social Security number and address. At least 49 New York residents were affected, but the total number of people affected nationwide was not disclosed.

Information
Source: Dataloss DB
Records from this breach used in our total: 49

From Sept. 29 to Oct. 9, thieves used card skimmers to steal bank account numbers and PIN codes from gas station customers and used the information to fabricate debit cards and make ATM withdrawals.

Information
Source: Dataloss DB
Records from this breach used in our total: 440

Hackers broke into the city's web site and compromised the online job application database, which included Social Security numbers.

Information
Source: Dataloss DB
Records from this breach used in our total: 5,800

A class of 2006 Fall graduation list was found to be accessible online. The file had only been available for 17 hours. Classes, majors, names, Social Security numbers, addresses, home phone numbers and dates of birth were on the list.

Information
Source: Dataloss DB
Records from this breach used in our total: 768
The location listed is the headquarters. The breach may have occurred elsewhere.

The July 11 theft of an employee's laptop left sensitive data exposed. Names, tax identification numbers and Social Security numbers of people who used their Social Security number as a tax ID were exposed.

Information Source: Dataloss DB
November 6, 2006 "Bowling Green Police Department" Bowling Green, Ohio GOV DISC Approx. 200 victims or suspects

The police dept. accidentally published a report on their website containing personal information on nearly 200 people the police had contact with on Oct. 21. Data included names, Social Security numbers, driver's license numbers, etc.

Information Source: Dataloss DB
November 6, 2006 Ingersoll Rand Montvale, New Jersey BSO PORT 1510

The September 29 theft of an employee's laptop resulted in the exposure of emails with names and Social Security numbers of former employees. The laptop was stolen from the employee's car while it sat in a restaurant parking lot.

Information Source: Dataloss DB
November 3, 2006 "University of Virginia (UVA)" Charlottesville, Virginia EDU DISC 632 students

Due to a computer programming error, Student Financial Services sent e-mail messages to students containing 632 other students' Social Security numbers.

Information Source: Dataloss DB
November 3, 2006 "West Shore Bank" Ludington, Michigan BSF CARD About 1,000

Customers' debit cards and possibly credit cards were compromised from a security break last summer at a common MasterCard point-of-purchase provider.

Information Source: Dataloss DB
November 3, 2006 Wesco Muskegon, Michigan BSR CARD Unknown

Wesco gas stations experienced a breach in credit card transactions from July 25-Sept. 7 resulting in inaccurate charges to customer accounts.

Information Source: Dataloss DB
November 3, 2006 Starbucks Corp. Seattle, Washington BSR PORT 60,080

1-800-453-1048

Starbucks lost track of four laptop computers. Two held employee names, addresses, and Social Security numbers. Current and former U.S. employees and about 80 Canadian workers and contractors were affected.

Information Source: Dataloss DB
November 3, 2006 Several Joliet area motels Joliet, Illinois BSO INSD Unknown

Motel owners and employees allegedly stole and sold customers' credit card numbers.

Information Source: Media
In September 2006, a laptop computer was stolen from the insurance brokerage firm. It contained client information including the names, birthdates, and drivers license numbers of Villanova University students and staff who drive university vehicles.

Information Source: Dataloss DB
November 2, 2006

Colorado Department of Human Services via Affiliated Computer Services (ACS)
Dallas, Texas

GOV STAT Up to 1.4 million

For questions, call ACS at (800) 350-0399

On Oct. 14, a desktop computer was stolen from a state contractor who processes Colorado child support payments for the Dept. of Human Services. Computer also contained the state's Directory of New Hires.

UPDATE (12/07/2006) When initially posted to this list, the number 1.4 million was not added to the total because we could not confirm if SSNs were exposed. The PRC was contacted by an affected individual today who confirmed that names, addresses, SSNs and dates of birth were exposed.

Information Source: Dataloss DB
November 2, 2006

Greater Media, Inc.
Philadelphia, Pennsylvania

BSO PORT Unknown

A laptop computer containing the Social Security numbers of the radio broadcasting company's current and former employees was stolen from their Philadelphia offices.

Information Source: Dataloss DB
November 2, 2006

McAlester Clinic and Veterans Affairs Medical Center
Muskegee, Oklahoma

MED PORT 1,400 veterans

Three disks containing billing information, patient names and Social Security numbers, were lost in the mail.

Information Source: Dataloss DB
November 2, 2006

Intermountain Health Care
Salt Lake City, Utah

MED PORT 6,244

A computer was purchased at a second-hand store, Deseret Industries, that contained the names, Social Security numbers, employment records, and other personal information about Intermountain Health Care employees employed there in 1999-2000.

Information Source: Dataloss DB
November 2, 2006

Compulinx
White Plains, New York

BSO INSD Up to 50 Compulinx employees

The CEO of Compulinx was arrested for fraudulently using employees' names, addresses, Social Security numbers and other personal information for credit purposes. (It is unclear whether customers' data was also used).

Information Source: Media
November 1, 2006

U.S. Army Cadet Command
Fort Monroe, Virginia

GOV PORT 4,600 high school seniors

1-866-423-4474, Email: mydata@usaac.army.mil

A laptop computer was stolen that contained the names, addresses, telephone numbers, birthdates, Social Security numbers, parent names, and mother's maiden names of applicants for the Army's four-year ROTC college scholarship.
October 31, 2006, Avaya Maitland, Florida

Additional location: Basking Ridge, NJ. A laptop stolen from an Avaya employee on October 16 in Florida contained personally identifiable information, including names, addresses, W-2 tax form information and SSNs.

Information Source: Dataloss DB

Records from this breach used in our total: 0

October 31, 2006, Community National Bank, Crowe Chizek & Company LLC, Great Neck, New York

The Bank was notified of a potential security breach by its auditor Crowe. Two laptops belonging to Crowe auditors were stolen from a car in a restaurant parking lot on October 12. One laptop contained the names, Social Security or tax identification numbers, addresses and account numbers of clients from a November 2005 confirmation trial.

Information Source: Dataloss DB

Records from this breach used in our total: 90

October 31, 2006, Yates County Public Health, Penn Yan, New York

A laptop computer used for Child Health Plus, Medicaid and Family Health Plus plans was stolen from a vehicle on October 20. It contained application information which included name, Social Security number, date of birth, driver’s license number, bank account and personal checking information and employer information. At least 68 New York residents were affected, but the total number of affected individuals nationwide was not revealed.

Information Source: Dataloss DB

Records from this breach used in our total: 68

October 30, 2006, National Financial Partners (NFP), New York, New York

A former payroll department employee may have had access to former and current employee information. The information included Social Security numbers, addresses and birth dates. The employee was not authorized to view the information. It is unclear if the employee still had access to the electronic files after termination.

Information Source: Dataloss DB

Records from this breach used in our total: 4,327

October 29, 2006, New York University, New York, New York

Backup CDs from the Continuing Medical Education program at NYU Medical Center were lost or stolen. Names, Social Security numbers, addresses, telephone and fax numbers, student ID numbers, debit or credit card information and degree information for students participating in the program between 1999 and the discovery of the loss may have been exposed.

Information Source: Dataloss DB

Records from this breach used in our total: 30,000

October 27, 2006, Gymboree, San Francisco, California

A thief stole 3 laptop computers from Gymboree’s corporate headquarters. They contained unencrypted human resources data (names and Social Security numbers) of thousands of workers.

Information Source: Dataloss DB

Records from this breach used in our total: 20,000

October 27, 2006, Hancock Askew & Co., Savannah, Georgia

On October 5, 2006, a laptop computer containing 401(k) information for employees of at least one company (Atlantic Plastics, Inc.) was stolen from accounting firm Hancock Askew.

Information Source: Dataloss DB

Records from this breach used in our total: 0

October 27, 2006, LexisNexis, Boca Raton, Florida

A package containing an employee’s laptop computer was lost by an overnight courier service during shipping. The laptop may have included the names, Social Security numbers, driver’s license numbers, dates of birth and addresses of certain individuals. At least 53 residents of Maine and 396 residents of New York were affected, but the total number of affected individuals nationwide was not reported.
On September 26 it was discovered that a computer server was stolen during an office burglary. The server had employee names and Social Security numbers. Current and former employees were notified at the end of October after an investigation of the breach.

Overseas hackers broke into two computers at Children's Hospital. One contains private patient data (including Social Security numbers) and the other holds billing and banking information.

Mortgage files that included personal financial details about loan applicants were found in a dumpster. Empire Equity will pay $12,500 to the State of NC.

The Denver Police Dept. reports that LimeWire's file-sharing program was exploited to access personal and financial information from approximately 75 different individual and business account names from all over the country. The information, which included tax records, bank account information, online bill paying records and other material, appears to have been stolen directly from computers that were using LimeWire's filesharing software program.

A thumb drive is missing from the TSA command center at Portland International Airport and believed to contain the names, addresses, phone numbers and Social Security numbers of approximately 900 current and former employees.

An employee stole the names, birthdates, and Social Security numbers from patients who were hospitalized or had day-surgeries from June 22 to Sept 21. She used 3 patients' information to open multiple credit accounts.

The Social Security numbers of some Tuscarawas and Warren County voters were available on the LexisNexis Internet database service. Local boards of elections may be the source of the information.

UPDATE (11/1/06): LexisNexis says it has now removed the SSNs.
A computer storage device that may have held the personal information of current and former employees was lost or stolen. The device had names, Social Security numbers, addresses and telephone numbers. The device was discovered missing on October 16 at the Transportation Security Administration's command center at Portland International Airport.

The laptop of a research doctor was stolen from her locked office at the Institute. It included records of patients and her research data.

A courier's envelope was delivered to the Credit Union ripped and missing the twenty reports it was supposed to contain. Some of the reports contained confidential information such as name, address, telephone number, credit card number, and financial institution checking account number.

On July 28, 2006, a contractor working for Advanced Receivables Strategy, a medical billing records company, misplaced CDs containing the names and SSNs of 266,200 patients, employees, physicians, and board members of St. Francis hospitals in Indiana and Illinois. About 260,000 patients and about 6,200 employees, board members and physicians were affected for a total of 266,200. Also affected were records of Greater Lafayette Health Services. The disks were inadvertently left in a laptop case that was returned to a store. The purchaser returned the disks. The records were not encrypted even though St. Francis and ARS policies require encryption.

An official from the not-for-profit Illinois Ballot Integrity Project says his organization hacked into Chicago's voter database, compromising the names, SSNs and dates of birth of 1.35 million residents. The Chicago Election Board is reportedly looking into removing SSNs from the database. Election officials have patched the flaw that allowed the intrusion.

A flash drive that contained visitor names, Social Security numbers, children's names, children's dates of birth and dates of visit was lost or stolen during an emergency evacuation. A researcher working with data from New York Children's Environmental Study conducted in Community Medicine reported that the flash drive she left in her computer was missing after she returned sometime around October 5.

On Sept. 6, an unencrypted laptop computer containing veterans' names, Social Security numbers, and medical diagnosis, was stolen from the Hospital. Veterans who receive pulmonary care were affected.
Information Source: Dataloss DB

October 20, 2006
BlueCross BlueShield of Western New York, HealthNow New York Inc., Administrative Services of Kansas
Buffalo, New York

BSF PORT 96

The theft occurred in a Kansas hospital. Potential HealthNow New York Inc. members were affected.

The laptop of an employee of HealthNow’s outside claims vendor Administrative Services of Kansas was stolen during the lunch break of a presentation. The laptop had potential member names and Social Security numbers. The theft occurred sometime around June 19 and notification letters were sent on October 16.

Information Source: Dataloss DB

October 19, 2006
Allina Hospitals and Clinics
Minneapolis, Minnesota

MED PORT 17,000

Individuals in 17,000 households

A laptop stolen from a nurse’s car on October 8 contains the names and SSNs of individuals in approximately 17,000 households participating in the Allina Hospitals and Clinics obstetric home-care program since June 2005.

Information Source: Dataloss DB

October 19, 2006
University of Minnesota
Minneapolis-St.Paul, Minnesota

EDU PORT 200 students

(Not included in total)

In June, a University of Minnesota art department laptop computer stolen from a faculty member while traveling in Spain holds personally identifiable information of 200 students.

Information Source: Media

October 17, 2006
City of Visalia, Recreation Division
Visalia, California

GOV PHYS 200 current and former employees

 Personally identifiable information of approximately 200 current and former Visalia Recreation Department employees was exposed when copies of city documents were found scattered on a city street.

Information Source: Dataloss DB

October 16, 2006
Germanton Elementary School
Germanton, North Carolina

EDU STAT Unknown

A computer stolen from Germanton Elementary school holds students’ SSNs. The data on the computer are encrypted.

Information Source: Dataloss DB

October 16, 2006
VISA, FirstBank (1st Bank)
Lakewood, Colorado

BSF UNKN Unknown

FirstBank sent a letter to an unknown number of customers informing them their FirstTeller Visa Check Card numbers were compromised when someone accessed “a merchant card processor’s transaction database.” The FirstBank letter said customers would receive new cards by October 27.

Information Source: Dataloss DB

October 16, 2006
Dr, Charles Kay of Orchard Family Practice
Englewood, Colorado

MED PHYS "Hundreds"

Sheriff’s deputies evicting Dr. Charles Kay put files from his office in a nearby parking lot. In a news report, Dr. Kay said he had removed the patient files but not the business files.

Information Source: Media
An office burglary occurred sometime between October 13 and October 15. A computer with the information of some, but not all clients was stolen. Partial list of client information was stolen. Social Security numbers of applicants, names, addresses, phone numbers, dates of birth, income, assets and other mortgage related financial information may have been exposed. At least 34 New York residents were affected, but the total number of affected clients nationwide was not revealed.

**Information Source:** Dataloss DB

October 15, 2006  **Poulsbo Department of Licensing**  Poulsbo, Washington

An unspecified “storage device” containing personally identifiable data of approximately 2,200 North Kitsap (WA) residents has been lost from the Poulsbo Department of Licensing. The data include names, addresses, photographs and driver’s license numbers of individuals who conducted transactions at the Poulsbo branch in late September.

**Information Source:** Media

October 14, 2006  **T-Mobile USA Inc.**  Bellvue, Washington

A laptop computer holding personally identifiable information of approximately 43,000 current and former T-Mobile employees disappeared from a T-Mobile employee’s checked luggage. T-Mobile has reportedly sent letters to all those affected. The data are believed to include names, addresses, SSNs, dates of birth and compensation information.

**Information Source:** Dataloss DB

October 14, 2006  **CBA Information Solutions, Washington Savings Bank**  Bowie, Maryland

An unauthorized user gained access to the log in information of Washington Savings Bank. The unauthorized user could have accessed customer and non-customer names, Social Security numbers, addresses and credit histories. The breach occurred between September 15 and September 21. At least 20 New York residents were affected, but the nationwide total was not reported.

**Information Source:** Dataloss DB

October 13, 2006  **Ohio Ethics Commission**  Columbus, Ohio

Papers belonging to the Ohio Ethics Commission were found floating on the wind in an alley. The documents are related to state employees’ finances and contained SSNs and financial statements. They were supposed to be in the possession of the state archives.

**Information Source:** Dataloss DB

October 12, 2006  **U.S. Census Bureau**  Washington, District Of Columbia

Additional location: Travis Co., TX

This spring, residents of Travis County, TX helped the Census Bureau test new equipment. When the test period ended, 15 devices were unaccounted for. The Census Bureau and the Commerce Department issued a press release saying the devices held names, addresses and birthdates, but not income or SSNs.

**Information Source:** Media

October 12, 2006  **Congressional Budget Office**  Washington, District Of Columbia

Hackers broke into the Congressional Budget Office’s mailing list and sent a phishing e-mail that appeared to come from the CBO.

**Information Source:** Media
Two computers stolen from a University of Texas faculty member's home hold the names, SSNs, grades, e-mail addresses and other information belonging to approximately 2,500 students enrolled in computer science and engineering classes between fall 2000 and fall 2006. The theft occurred on September 29 and was reported on October 2.

Information
Source: Dataloss DB

October 12, 2006
Sears Holding Corporation
Winter Park, Florida

A laptop was stolen from the office on September 28. Certain customers had their information on an access database file that was on the laptop. Names, telephone numbers, addresses, account number, account types and account expiration dates were exposed.

Information
Source: Dataloss DB

October 11, 2006
Republican National Committee (RNC)
Washington, District Of Columbia

The Republican National Committee (RNC) inadvertently emailed a list of donors' names, SSNs and races to a New York Sun reporter.

Information
Source: Dataloss DB

October 11, 2006
DirecTV, Deloitte and Touche LLC
El Segundo, California

A laptop containing the names and Social Security numbers of some current and former DirecTV employees was stolen during a home burglary of a Deloitte and Touche LLP employee. The theft occurred sometime in August. Deloitte and Touche performs audits of The DirecTV Group's pension plans.

Information
Source: Dataloss DB

October 10, 2006
Florida Labor Department
Tallahassee, Florida

The names and SSNs of 4,624 Floridians were accessible on the Internet for approximately 18 days in September. The data were not accessible through websites, but an individual came across the information when Googling his own name. The agency has asked Google to remove the pages from its cache, and has notified all affected individuals by mail. Individuals who had registered with Florida’s Agency for Workforce Innovation were affected.

Information
Source: Dataloss DB

October 9, 2006
Troy Athens High School
Troy, Michigan

For questions or comments, call (248) 823-4035

A hard drive stolen from Troy Athens High School in August contained transcripts, test scores, addresses and SSNs of students from the graduating classes of 1994 to 2004. The school district and the superintendent have notified all affected alumni by regular mail.

Information
Source: Dataloss DB

October 9, 2006
Atlantis Plastic Inc.
Atlanta, Georgia

A laptop was stolen from Atlantis’ accounting firm on October 5. The laptop contained personal information for 720 participants in the Atlantis 401(k) plan. Names, Social Security numbers, dates of birth, addresses and 401(k) account balance information may have been exposed.

Information
Source: Dataloss DB
October 6, 2006  **Cleveland Air Route Traffic Control Center**  Oberlin, Ohio  GOV  STAT  400

A computer hard drive missing from the Cleveland Air Route Traffic Control Center in Oberlin (OH) contains the names and SSNs of at least 400 air traffic controllers.

**Information Source:** Dataloss DB

records from this breach used in our total: 400

October 6, 2006  **Camp Pendleton Marine Corps base via Lincoln B.P. Management**  Camp Pendleton, California  GOV  PORT  2,400

A laptop missing from Lincoln B.P. Management Inc. holds personally identifiable data about 2,400 Camp Pendleton residents.

**Information Source:** Dataloss DB

records from this breach used in our total: 2,400

October 6, 2006  **StarCite Inc.**  Philadelphia, Pennsylvania  BSO  PORT  Unknown

A laptop containing personal information of employees was stolen from a hotel room on September 13. The information included name, Social Security number, date of birth, address, date of hire, occupation, salary, supplemental insurance information, and identified the type and tier of medical and/or dental coverage.

**Information Source:** Dataloss DB

records from this breach used in our total: 0

October 5, 2006  **San Juan Capistrano Unified School District (CA)**  San Juan Capistrano, California  EDU  STAT  Unknown

Five computers stolen from the HQ of San Juan Capistrano Unified School District likely contain the names, SSNs and dates of birth of district employees enrolled in an insurance program.

**Information Source:** Dataloss DB

records from this breach used in our total: 0

October 5, 2006  **Homecoming Financial Network Inc.**  Minneapolis, Minnesota  BSF  DISC  988

On September 9, a web-based tool for mortgage brokers was released that allowed brokers to view all loan applications submitted by all other brokers. The information included names, Social Security numbers and addresses. The flaw was discovered and fixed the next day.

**Information Source:** Dataloss DB

records from this breach used in our total: 988

October 4, 2006  **Orange County Controller**  Orlando, Florida  GOV  DISC  Unknown

A Florida woman discovered her marriage license was visible on the Orange County (FL) controller's Web site with no information blacked out, not even SSNs. She discovered the breach because someone had applied for a loan in her name. The Orange County Comptroller is reportedly paying a vendor $500,000 to black out all SSNs by January 2008.

**Information Source:** Media

records from this breach used in our total: 0

October 3, 2006  **Cumberland County**  Carlisle, Pennsylvania  GOV  DISC  1,200 employees of the county

Cumberland County (PA) officials removed salary board meeting minutes from their Web site because they contained the SSNs of 1,200 county employees. The information was included in minutes from meetings prior to 2000. The county no longer uses SSNs as unique identifiers for employees. Employees will be informed of the data breach in a note included with their paychecks.

**Information Source:** Dataloss DB

records from this breach used in our total: 1,200

October 3, 2006  **Willamette Educational Service District (ESD)**  Salem, Oregon  EDU  STAT  4,500 Oregon high school students [not included in total because not thought to
Seven computers stolen from a Willamette Educational Service District office were believed to contain personal information of 4,500 Oregon high school students. Backup tapes indicate the computers hold information about the students' school clubs but do not contain sensitive information.

Information
Source: Media
October 3, 2006 Picatinny Arsenal Rockaway, New Jersey GOV UNKN Unknown

If you have tips, call (973) 989-0652

28 computers are missing from the Picatinny Arsenal, a Department of Defense Weapons Research Center. The computers were reported lost or stolen over the last two years. None of the computers was encrypted. Officials state the computers did not contain classified information.

Information
Source: Media
October 3, 2006 Western Financial Services Inc. Englewood, Colorado BSF PORT 43

A laptop lost during shipping contained names, Social Security numbers, driver’s license numbers and addresses. The laptop was first discovered missing on or sometime before August 31. At least 43 New York residents were affected, but the number of affected customers nationwide was not reported. Affected individuals were notified on October 4.

Information
Source: Dataloss DB
October 2, 2006 Port of Seattle, Seattle-Tacoma Airport (Sea-Tac) Seattle, Washington GOV PORT 6,939 current and former Seattle-Tacoma International Airport employees

http://www.portseattle.org, (888) 902-PORT

Six CDs missing from the ID Badging office at Seattle-Tacoma International Airport hold the personal information of 6,939 airport workers. The data include names, addresses, birth dates, SSNs and driver’s license numbers, telephone numbers, employer information, and height/weight. The data on the disks were scanned from paper applications for airport badges. The port learned of the missing disks on September 18 and sent letters to the affected employees on Oct. 2.

Information
Source: Dataloss DB
October 2, 2006 Citigroup Chicago, Illinois BSF PORT 11

An employee from a Pennsylvania branch reported a missing laptop after a flight. It is believed that the laptop may have been stolen from the employee’s luggage after the bags were checked-in for a flight from Chicago to Philadelphia sometime around August 26. At least 11 New York residents and an unknown number of clients nationwide may have had their names, Social Security numbers, addresses and other information exposed.

Information
Source: Dataloss DB
September 29, 2006 University of Iowa Department of Psychology Iowa City, Iowa EDU HACK 14,500

A computer containing SSNs of 14,500 psychology department research study subjects was the object of an automated attack designed to store pirated video files for subsequent distribution.

Information
Source: Dataloss DB
September 29, 2006 Kentucky Personnel Cabinet via Bluegrass Mailing Frankfort, Kentucky GOV DISC 146,000

State employees received letters from the Kentucky Personnel Cabinet with their SSNs visible through the envelope windows.
A laptop computer was stolen from the home of an employee on or around May 23. This laptop contained claimants' names, Social Security numbers, and addresses. Nationwide Agribusiness learned of the theft in early September and began the process of developing a privacy and security awareness package for all employees.

Information Source: Dataloss DB  
September 28, 2006  
**Nationwide Agribusiness, Farmland Mutual Insurance Company**  
Columbus, Ohio  
BSF  PORT  306

A computer was stolen from a NC Dept. of Motor Vehicles office, reported Sept. 10. It contains names, addresses, driver's license numbers, SSNs, and in some cases immigration visa information of 16,000 people who have been issued licenses in the past 18 months. Most are residents of Franklin County.

Information Source: Dataloss DB  
September 28, 2006  
**North Carolina Department of Motor Vehicles**  
Louisville, North Carolina  
GOV  STAT  16,000

Documents found by state auditors in recycling bins in a hallway contained IDOT employee names and SSNs.

Information Source: Dataloss DB  
September 28, 2006  
**Illinois Department of Transportation (IDOT)**  
Springfield, Illinois  
GOV  PHYS  40

A manager for the hospital's billing company, Med Data, stole patients' credit card numbers. She gave them to her brother who bought $30,000 worth of clothes and gift cards over the Internet. The woman is scheduled for sentencing in Nov. and her brother's trial is expected Jan. 2007.

Information Source: Media  
September 28, 2006  
**Stevens Hospital Emergency Room via dishonest employee of billing company Med Data**  
Edmonds, Washington  
MED  INSD  30

During the routine process of indexing the search engine of the Department's website, data files from the 2005 Volume of Operations Reports were inadvertently made accessible to members of the public between July 27 and August 29. Personal information included the Social Security numbers of all independent contractors employed by both licensed mortgage bankers and registered mortgage brokers. Social Security numbers of all felons employed by those registrants who also opted to electronically filed their 2005 VOI reports were also available through the Department's website search engine.

Information Source: Dataloss DB  
September 27, 2006  
**New York State Banking Department**  
New York, New York  
BSF  DISC  19,640

A life insurance agent reported that two desktops were stolen from his office. Customer names, Social Security numbers, addresses, dates of birth and policy numbers may have been exposed. An unspecified number of customers nationwide were affected.

Information Source: Dataloss DB  
September 25, 2006  
**New York Life Insurance Company**  
Boston, Massachusetts  
BSF  STAT  Unknown

During the routine process of indexing the search engine of the Department's website, data files from the 2005 Volume of Operations Reports were inadvertently made accessible to members of the public between July 27 and August 29. Personal information included the Social Security numbers of all independent contractors employed by both licensed mortgage bankers and registered mortgage brokers. Social Security numbers of all felons employed by those registrants who also opted to electronically filed their 2005 VOI reports were also available through the Department's website search engine.

Information Source: Dataloss DB  
September 27, 2006  
**New York Life Insurance Company**  
Boston, Massachusetts  
BSF  STAT  Unknown

A life insurance agent reported that two desktops were stolen from his office. Customer names, Social Security numbers, addresses, dates of birth and policy numbers may have been exposed. An unspecified number of customers nationwide were affected.

Information Source: Dataloss DB  
September 25, 2006  
**Movie Gallery US**  
Gastonia, North Carolina  
BSR  PHYS  3,800

A large number of Movie Gallery's files and videos were found in a dumpster. The files contained personal information of people employed by Movie Gallery and people applying for jobs at the video store as well as people applying for movie rental membership. Movie Gallery has agreed to pay $50,000 to the State of NC for the breach.

Information Source: Dataloss DB  
September 25, 2006  
**Movie Gallery US**  
Gastonia, North Carolina  
BSR  PHYS  3,800
September 25, 2006  
**General Electric (GE)**  
**Fairfield, Connecticut**  
**BSO**  
**PORT**  
**50,000 employees**

An employee’s laptop computer holding the names and Social Security numbers of approximately 50,000 current and former GE employees was stolen from a locked hotel room while he was traveling for business.

**Information Source:** Dataloss DB

**September 23, 2006**  
**Erlanger Health System**  
**Chattanooga, Tennessee**  
**MED**  
**PORT**  
**4,150 current and former employees**

Records of hospital employees disappeared from a locked office on Sept. 15. They were stored on a USB jump drive. Information was limited to names and SSNs. Those affected included anyone who went through job status changes from Nov. 2003 to Sept. 2006.

**Information Source:** Dataloss DB

**September 23, 2006**  
**North Fork Bank**  
**Melville, New York**  
**BSF**  
**HACK**  
**3,570**

On the morning of July 31, criminals altered a link on the Personal Banking page of NorthForkBank.com that was designed to take visitors to the My NFB Online sign-on page and redirected them to a counterfeit website. The counterfeit website requested sensitive customer information, although it appears that the counterfeit website may not have functioned as intended. The altered link was identified and repaired within three hours and the hacker’s access was terminated.

**Information Source:** Dataloss DB

**September 22, 2006**  
**Purdue University College of Science**  
**West Lafayette, Indiana**  
**EDU**  
**STAT**  
**2,482**

(866) 307-8520

A file in a desktop computer in the Chemistry Department may have been accessed illegitimately. The file contained names, SSNs, school, major, and e-mail addresses of people who were students in 2000.

**Information Source:** Dataloss DB

**September 22, 2006**  
**University of Colorado, Boulder, Leeds School of Business**  
**Boulder, Colorado**  
**EDU**  
**STAT**  
**1,372 students and former students**

(303) 492-8741

Two computers had been placed in storage during the school’s move to temporary quarters in May. When they were to be retrieved Aug. 28, they were found missing. They had been used by 2 faculty members and included students’ names, SSNs, and grades.

**UPDATE (9/25/06):** One of the computers was found.

**Information Source:** Dataloss DB

**September 22, 2006**  
**Several Indianapolis pharmacies**  
**Indianapolis, Indiana**  
**MED**  
**PHYS**  
**Unknown**

Earlier this year a local TV reporter from WTHR found that dozens of pharmacies disposed of customer records in unsecured garbage bins. Now the Indiana Board of Pharmacy has launched an investigation of 30 pharmacies. Both the Board and the Attorney General say that the pharmacies violated state law.

**Information Source:** Media

**September 21, 2006**  
**Pima County Health Department**  
**Tucson, Arizona**  
**GOV**  
**PHYS**  
**2,500 (no SSNs or financial information reported)**
Vaccination records on 2,500 clients had been left in the trunk of a car that was stolen Sept. 12. The car and records have since been recovered. Records included names, dates of birth and ZIP codes, but no SSNs or addresses.

**Information Source:**
Dataloss DB

**September 21, 2006**  
**U.S. Department of Commerce and Census Bureau**  
**Washington, District Of Columbia**  
GOV PORT Unknown


The agency reported that 1,137 laptops have been lost or stolen since 2001. Of those, 672 were used by the Census Bureau, with 246 of those containing personal data. Secretary Gutierrez said the computers had protections to prevent a breach of personal information.

**Information Source:**
Media

**September 20, 2006**  
**City of Savannah, Georgia**  
**Savannah, Georgia**  
GOV DISC Unknown

(912) 651-6565, [http://www.savannahga.gov/security](http://www.savannahga.gov/security)

Because of a hole in the firewall, a City server exposed personal information online for 7 months. Individuals identified by the Red Light Camera Enforcement Program are affected -- name, address, driver's license number, vehicle identification number, and SSNs of those individuals whose driver's license number is still the SSN.

**Information Source:**
Dataloss DB

**September 20, 2006**  
**Berry College via consultant Financial Aid Services Inc.**  
**Mount Berry, Georgia**  
EDU PHYS Unknown

(800) 961-4692, [http://www.berry.edu/stulife/idprotect/](http://www.berry.edu/stulife/idprotect/)

Student applications for need-based financial aid were misplaced by a consultant -- in both paper and digital form. Data included name, SSN, and reported family income for students and potential students for the 2005-06 academic year.

**Information Source:**
Dataloss DB

**September 19, 2006**  
**Life Is Good**  
**Hudson, New Hampshire**  
BSR HACK 9,250

Hackers accessed the retailer's database which contained customer's credit card numbers. The company said no other personal information was in the database.

**Information Source:**
Dataloss DB

**September 18, 2006**  
**Olean Area Federal Credit Union**  
**Olean, New York**  
BSF HACK 11

An unauthorized party managed to obtain financial information from a fraudulent credit union website link. The information included name, address, Credit Union account number, PIN and account password. More clients who live outside of New York may have been affected.

**Information Source:**
Dataloss DB

**September 18, 2006**  
**DePaul Medical Center, Radiation Therapy Department**  
**Norfolk, Virginia**  
MED STAT More than 100 patients

(757) 889-5945

Two computers were stolen, one on August 28 and the other Sept. 11. Personal data included names, date of birth,
A hacker accessed customer information from the online store. Customer names, credit card numbers, credit card expiration dates, shipping or billing addresses, email addresses and phone numbers may have been exposed.

A security breach exposed private information of student loan borrowers from Aug. 20-22 during a computer software upgrade. Users of the DOE's Direct Loan Web site were able to view information other than their own if they used certain options when accessing the program's web pages. SSNs were among the data elements exposed online. Software company Affiliated Computer Services (ACS) created the technology for the Direct Loan Servicing feature on the DoE's site.

Residents who participated in a scientific study were notified that a flash drive was discovered missing as of Aug. 4, and likely stolen, from an MDCH office. The portable memory device contained names, addresses, phone numbers, dates of birth, and SSNs of participants. The study tracked the long-term exposure to flame retardents ingested by residents in beef and milk.

A Morris auditor's laptop was stolen from the auditor's car. The laptop had three spreadsheets with the names and Social Security numbers of Howard employees. Pension plan, 401(k) and profit-sharing account information was also exposed.

A memory stick containing patient information was found July 18 by a local citizen on the ground at the County Fairgrounds near the hospital's information booth. It was returned to the hospital four weeks later. Data included names, SSNs, dates of birth, and medical records.

Personnel files of employees of the now-closed restaurant were found in a nearby Dumpster. Papers included names and SSNs of former employees.

A hacker may have gained access to student and staff names, addresses and Social Security numbers. Students who received financial aid or worked at the University were affected. The breach was discovered during a routine risk assessment of the University's computer servers.
A temporary employee accessed the personal information of some University employees and used it to establish at least one fraudulent account. The former temp had access to the names, Social Security numbers, addresses, telephone numbers and direct deposit bank account information of a group of employees. The University discovered the breach on August 15 and began notifying affected individuals on August 18.

**Information Source:**
Dataloss DB  
**September 15, 2006**  
Harlem Hospital Center, New York City Health and Hospitals Corporation  
New York, New York  
MED PORT 4,000

A computer hard drive was lost or stolen sometime around September 8. The hard drive contained the names and Social Security numbers of current and former Harlem Hospital employees.

**Information Source:**
Dataloss DB  
**September 14, 2006**  
Nikon Inc. and Nikon World Magazine  
Melville, New York  
BSR DISC 3,235 magazine subscribers

Workers at a Montgomery, AL, camera store discovered that subscription information for the magazine Nikon World was exposed on the Web for at least 9 hours. Data included subscribers' names, addresses and credit card numbers.

**Information Source:**
Dataloss DB  
**September 14, 2006**  
Illinois Department of Corrections (IDOC)  
Springfield, Illinois  
GOV PHYS 16,500

A document containing employees' personal information was found outside the agency's premises where it should not have been. It has since been retrieved. Information included employees' names, SSNs, and salaries.

**Information Source:**
Dataloss DB  
**September 14, 2006**  
GreenPoint Mortgage Funding Inc.  
Novato, California  
BSF PORT 44

A GreenPoint payment processing vendor's storage facility was robbed of several computer disks. The disks contained customer names, addresses, telephone numbers, Social Security numbers, signatures, loan account numbers, bank account information and copies of voided and cleared personal checks.

**Information Source:**
Dataloss DB  
**September 13, 2006**  
American Family Insurance Group  
Madison, Wisconsin  
BSF PORT 2,089 customers

The office of an insurance agent was broken into and robbed last July. Among the items stolen was a laptop with customers’ names, SSNs, and driver’s license numbers.

**Information Source:**
Dataloss DB  
**September 12, 2006**  
City of Paris Kentucky  
Paris, Kentucky  
GOV PORT 130

A portable drive that contained the personal information of current and former city employees was lost or stolen in August. Employee names, Social Security numbers and dates of birth were lost.

**Information Source:**
Dataloss DB  
**September 11, 2006**  
Telesource via Veksta  
Indianapolis, Indiana  
BSO PHYS Unknown

Employees discovered their personnel files in a Dumpster after the company had been bought out by another company Vekstar. The files were discarded when the office was being cleaned out and shut down. Files contained SSNs, dates of birth and photocopies of SSN cards and driver’s licenses.
A clinic employee stole personal information from electronic files and sold it to her cousin, owner of Advanced Medical Claims, who used it to file fraudulent Medicare claims totaling more than $2.8 million. Information included names, SSNs, birthdates, addresses and other details. Both individuals were indicted.

Information Source: Dataloss DB

September 9, 2006
Cleveland Clinic
Naples, Florida
MED INSD 1,100 patients

(866) 907-0675

At least 11 residents of New York were affected, but the total number of affected clients was not released.

A laptop was stolen from a bank employee’s home. The laptop contained bank account information and Social Security numbers.

Information Source: Dataloss DB

September 9, 2006
Discover Bank
Greenwood, Delaware
BSF PORT 11

An encrypted server was stolen during an August 23 office burglary. Customer information was lost.

Information Source: Dataloss DB

September 9, 2006
Action Capital Mortgage Services, Inc.
Poughkeepsie, New York
BSF STAT 923


On Sept. 6, Linden Lab discovered that a hacker accessed its Second Life database through web servers. The affected data included unencrypted account names, real life names, and contact information, plus encrypted account passwords and payment information. Second Life is a 3-D virtual world.

Information Source: Dataloss DB

September 8, 2006
Linden Lab, Second Life
San Francisco, California
BSO HACK Unknown

On August 14-15 eve, two computers were stolen from the desk of an Institute of Technology employee, containing information on students who were freshmen from 1992-2006 -- including names, birthdates, addresses, phone numbers, high schools attended, student ID numbers, grades, test scores, and, academic probation. SSNs of 603 students were also exposed.

Information Source: Dataloss DB

September 8, 2006
University of Minnesota
Minneapolis, Minnesota
EDU STAT 13,084 students including SSNs of 603 students

A confidential list of some of the County’s 25,000 gun permit holders was exposed on the Web by the contractor that is developing a Web-based computer records program for the Sheriff’s Office. Personal information included names, addresses and SSNs.

UPDATE (10/6/06): The Berks County solicitor’s office says the entire list of more than 25,000 gun permit holders was exposed.

Information Source: Dataloss DB

September 8, 2006
Berks County Sheriff’s Office via contractor Canon Technology Solutions
Reading, Pennsylvania
GOV DISC 25,000

A laptop computer was stolen from a soldier’s vehicle contained training and administrative records, including Social Security numbers of up to 100 Florida National Guard soldiers.

Information Source: Dataloss DB

September 7, 2006
Florida National Guard
Bradenton, Florida
GOV PORT 100
September 7, 2006  
**Circuit City and Chase Card Services, a division of JP Morgan Chase & Co.**  
**Wilmington, Delaware**  
BSF  PORT  2.6 million past and current Circuit City credit cardholders

Chase Card Services mistakenly discarded 5 computer data tapes in July containing Circuit City cardholders' personal information.

**Information Source:** Security Breach Letter

September 7, 2006  
**Liberty Mutual Insurance Company**  
**Rancho Cordova, California**  
BSF  PORT  672

A laptop was stolen from an employee’s car on July 14. Names and Social Security numbers of employees of Liberty’s insureds were exposed. Analysis of the breach was completed on August 22 and notifications were sent in early September.

**Information Source:** Dataloss DB

September 7, 2006  
**Mystic Stamp Company**  
**Camden, New York**  
BSR  HACK  13

The website fell victim to an SQL injection attack. Hackers accessed the website database and obtained customer names, addresses, credit card numbers and expiration dates. The breach was discovered on August 29 and the website’s charge card function was disabled.

**Information Source:** Dataloss DB

September 5, 2006  
**Transportation Security Administration (TSA) via Accenture**  
**Washington, District Of Columbia**  
GOV  DISC  1,195 former TSA employees

In late August 2006, Accenture, a contractor for TSA mailed documents containing former employees’ SSN, date of birth, and salary information to the wrong addresses due to an administrative error.

**Information Source:** Dataloss DB

September 5, 2006  
**TLM Partners LP**  
**Palm Beach, Florida**  
BSF  PORT  Unknown

Two backup computer tapes were stolen from a vehicle during a June 8 theft. The tapes contained names, addresses and Social Security numbers. The tapes were discovered missing on July 6 and an unknown number of affected clients were notified on July 11. At least two New York residents were affected.

**Information Source:** Dataloss DB

September 5, 2006  
**Disney Worldwide Services, Inc.**  
**Burbank, California**  
BSR  PORT  23

A laptop with former employee information was stolen. The information included names, Social Security numbers, phone numbers, dates of birth, gender, marital status, workplace email and compensation information. At least 23 New York residents were affected, but the number of affected former employees nationwide was not reported.

**Information Source:** Dataloss DB

September 1, 2006  
**Wells Fargo via unnamed auditor**  
**San Francisco, California**  
BSF  PORT  Unknown

In a letter dated Aug. 28, the company notified its employees that a laptop and data disk were stolen from the locked trunk of an unnamed auditor, hired to audit the employees’ health plan. Data included names, SSNs, and information about drug claim cost and dates from 2005, but no prescription information said the company.

**Information Source:** Security Breach
Personal information of freshmen and graduate engineering students from 1998 through 2005 was exposed on the Internet for 8 months (Jan. - Aug.) due to human error. It was discovered by a student who used a search engine to find her name. The data included SSNs and e-mail addresses.

Information Source: Dataloss DB

September 1, 2006 Virginia Commonwealth University (VCU) Richmond, Virginia

http://old.ts.vcu.edu/security/id_exposure.html

http://old.ts.vcu.edu/security/id_exposure.html

City of Chicago via contractor Nationwide Retirement Solutions, Inc. Chicago, Illinois

Information Source: Dataloss DB

September 1, 2006


City of Chicago via contractor Nationwide Retirement Solutions, Inc. Chicago, Illinois

A laptop was stolen from the home of one of the contractor’s employees in April 2005. It was reported to the city July 2006. Data included names, addresses, phone numbers, birth dates and SSNs for those in the city’s deferred compensation plan.

Information Source: Dataloss DB

September 1, 2006

LandAmerica Credit Services, Inc., Diversified Capital San Jose, California

Information Source: Dataloss DB

September 1, 2006

A hacker may have accessed personal information. A customer named Diversified Capital noticed unusual activity on its account. An investigation revealed that the unauthorized access was most likely the result of a stolen password or unauthorized use of the password. The breach was first noticed on July 17 and notification was sent on August 10.

Information Source: Dataloss DB

August 31, 2006 CoreLogic for ComUnity Lending Sacramento, California

Information Source: Security Breach Letter

August 31, 2006

Labcorp Monroe, New Jersey

Information Source: Security Breach Letter

August 31, 2006

(800) 788-9091 x3925

During a break-in June 4 or 5, a computer was stolen that contained names and SSNs, but according to the company did not have birth dates or lab test results.

Information Source: Dataloss DB

August 31, 2006 Diebold, Inc., GE Capital Canton, Ohio

Information Source: Security Breach Letter

August 30, 2006

Valley Baptist Medical Center Harlingen, Texas

Information Source: Security Breach Letter

August 29, 2006

(877) 840-5999

A programming error on the hospital’s web site exposed names, birth dates, and SSNs of healthcare workers in late August. The error was fixed but it is not known how long the personal information was compromised. The affected
individuals are workers from outside the hospital who provide services and bill the hospital via an online form.

**Information Source:** Dataloss DB

**August 29, 2006**  
**AT&T via vendor that operates an order processing computer**  
San Francisco, California  
BSO  HACK  19,000

Computer hackers accessed credit card account data and other personal information of customers who purchased DSL equipment from AT&T’s online store. The company is notifying fewer than 19,000 customers.

**UPDATE** (9/1/06). The breach was followed by a bogus phishing e-mail to those customers that attempted to trick them into revealing more info such as SSN and birthdate -- essential for crime of identity theft.

**Information Source:** Dataloss DB

**August 29, 2006**  
**Compass Health**  
Everett, Washington  
MED  PORT  Unknown

(800) 508-0059

Compass Health notified some of its clients that a laptop containing personal information, including SSNs, was stolen June 28. The agency serves people who suffer from mental illness.

**Information Source:** Dataloss DB

**August 29, 2006**  
**Wells Fargo, Paymap Inc., First Horizon Home Loans, Western Union**  
Memphis, Tennessee  
BSF  PORT  Unknown

Computer discs with sensitive customer information were stolen from a Paymap facility in September of 2005. People who were subscribers between 1999 and 2002 may have been affected. The theft was not discovered until an unrelated mail fraud investigation was in process. Information included names, addresses, telephone numbers, Social Security numbers, loan account numbers, bank account information, copies of signatures and copies of voided or cleared personal checks.

**Information Source:** Dataloss DB

**August 28, 2006**  
**Copart, Inc.**  
Fairfield, California  
BSR  HACK  43,764 (No SSNs or financial information reported)

Hackers may have acquired the full names of customers, business and home addresses, telephone numbers, email addresses, driver’s license numbers and possibly driver’s license photographs. The website breach was discovered on July 17 and customers were notified on August 28. No Social Security numbers or financial information was accessed.

**Information Source:** Dataloss DB

**August 27, 2006**  
**New Mexico Administrative Office of the Courts**  
Santa Fe, New Mexico  
GOV  DISC  1,500 employees

For 8 days in late May, an unsecured document was exposed on the agency’s FTP site on the state’s computer server. It contained names, birth dates, SSNs, home addresses and other personal information of judicial branch employees. The FTP site was shut down June 2 and has since been redesigned.

**Information Source:** Dataloss DB

**August 26, 2006**  
**University of South Carolina**  
Columbia, South Carolina  
EDU  HACK  6,000

TheState.com reported that the University of South Carolina warned 6,000 current and former students that their information, including Social Security numbers and birth dates, may have been breached when a server was accessed from outside the system.

**Information Source:** Media

**August 26, 2006**  
**PortTix**  
Portland, Maine  
BSO  HACK  2,000

Credit card information for about 2,000 people who ordered tickets online through PortTix was accessed by someone who
hacked into the Web site. PortTix is Merrill Auditorium’s ticketing agency. The Web site was secured as of Aug. 24.

Information Source: Dataloss DB

August 25, 2006  **Dominion Resources**
**Richmond, Virginia**

Two laptops containing employee information were stolen earlier in August. It was not clear what type of data were included. No customer records were on the computers. Dominion operates a gas and electric energy distribution company.

Information Source: Dataloss DB

**Baltimore, Maryland**

(800) 832-5660

A laptop that might contain personal information of people with commercial driver’s licenses was stolen Aug. 22. FMCSA said the data might include names, dates of birth, and commercial driver’s license numbers of 193 individuals from 40 trucking companies.

Information Source: Dataloss DB

August 25, 2006  **Sovereign Bank**
**New Bedford, Massachusetts**

Personal data may have been compromised when 3 managers’ laptops were stolen from 2 separate locations in early August. Customers were notified Aug. 21. Sovereign serves New England and the Mid-Atlantic. The bank said the data included unspecified customer information, but not account data.

Information Source: Dataloss DB

August 25, 2006  **Verizon Wireless**
**Basking Ridge, New Jersey**

A Microsoft Excel spreadsheet file with the information of 5,210 customers was accidentally distributed to 1,800 Verizon Wireless subscribers. The information included names, email addresses, cell phone numbers and cell phone models. The file was accidentally attached to an ad for a Bluetooth wireless headset.

Information Source: Dataloss DB

August 23, 2006  **U.S. Department of Education, Direct Loan Servicing Online**
**Atlanta, Georgia**

http://www.dlssonline.com

A faulty Web site software upgrade resulted in personal information of 21,000 student loan holders being exposed on the U.S. Department of Education’s loan Web site. Information included names, birthdates, SSNs, addresses, phone numbers, and in some cases, account information. Affiliated Computer Services Inc. is the contractor responsible for the breach. The breach did not include those whose loans are managed through private companies.

Information Source: Dataloss DB

August 22, 2006  **AFLAC American Family Life Assurance Co.**
**Greenville, South Carolina**

(888) 794-2352

A laptop containing customers’ personal information was stolen from an agent’s car. It contained names, addresses, SSNs, and birth dates of 612 policyholders. They were notified Aug. 11.

Information Source: Dataloss DB
Time slips revealing personal information were missing and presumed stolen following a July 24 break-in at a storage shed on the administration office's property. The time slips included names and SSNs but not addresses.

**Information Source:** Dataloss DB

**August 22, 2006**
**Beaverton School District**
**Beaverton, Oregon**
**EDU PHYS 1,600 employees**

A vehicle of a home health care nurse was stolen from outside a senior center Aug. 5. Although it was recovered nearby, a laptop left in the rear of the car was not recovered. It contained names, addresses, SSNs, and insurance information of home health care patients.

**UPDATE** (8/23/06). The laptop was returned Aug. 23 by a woman who said she found it in her yard.

**Information Source:** Dataloss DB

**August 21, 2006**
**U.S. Department of Education via contractor, DTI Associates**
**Washington, District Of Columbia**
**GOV PORT 43**

Two laptops were stolen from DTI's office in downtown DC containing personal information on 43 grant reviewers for the Teacher Incentive Fund. DTI could not rule out that the data included SSNs.

**Information Source:** Dataloss DB

**August 18, 2006**
**California Department of Mental Health**
**Sacramento, California**
**GOV PORT 9,468**

A computer tape with employees' names, addresses, and SSNs has been reported missing. Employees were notified Aug. 17 by e-mail.

**Information Source:** Dataloss DB

**August 18, 2006**
**Experian, LA Walker Company**
**Roseville, California**
**BSF HACK 30**

Thirteen New York residents and an unknown number of customers nationwide had their information accessed. The unauthorized access by an Experian client resulted in the exposure of names, dates of birth, account numbers, Social Security numbers and addresses.

**Information Source:** Dataloss DB

**August 17, 2006**
**Williams-Sonoma, Deloitte & Touche**
**San Francisco, California**
**BSR PORT 1,200 current and former employees**

On July 10, a laptop was stolen from the Los Angeles home of a Deloitte & Touche employee who was conducting an audit for W-S. Computer contained employees' payroll information and SSNs.

**Information Source:** Dataloss DB

**August 17, 2006**
**HCA, Inc. Hospital Corporation of America**
**Nashville, Tennessee**
**MED STAT thousands of files**

(800) 354-1036, http://www.hcahealthcare.com

10 computers containing Medicare and Medicaid billing information and records of employees and physicians from 1996-2006 were stolen from one of the company's regional offices. Some patient names and SSNs were exposed, but details are vague. Records for patients in hospitals in the following states were affected: CO, KS, LA, MS, OK, OR, TS, WA.
An employee's car was stolen from the parking lot of a lab. A schedule of patients that included name, reason for visit, date of visit, doctor name and possibly phone number was in the car. The financial information of five patients and more detailed medical information of eight patients was also in the car.

**Information Source:** Dataloss DB

**August 16, 2006**  
**Chevron San Ramon, California**  
Total employees affected is unclear. Nearly half of Chevron's 59,000 workers are from North America, but it is not known if that number includes employees from Canada.

Chevron informed its U.S. workers on Aug. 14 that a laptop was stolen from an employee of an independent public accounting firm who was auditing its benefits plans. The theft apparently occurred Aug. 5. Files contained SSNs and sensitive information related to health and disability plans.

**Information Source:** Dataloss DB

**August 15, 2006**  
**University of Kentucky Lexington, Kentucky**  
The names and SSNs of 630 students were posted on the University's financial aid web site between Friday and Monday, Aug. 11-14.

**Information Source:** Dataloss DB

**August 15, 2006**  
**University of Kentucky Department of Geography Lexington, Kentucky**  
About 80 geography students were notified Aug. 14 that their SSNs were inadvertently listed on an e-mail communication they all received telling them who their academic advisor would be for the coming year.

**Information Source:** Dataloss DB

**August 15, 2006**  
**U.S. Department of Transportation Orlando, Florida**  
On April 24, a DOT employee's laptop computer was stolen from an Orlando hotel conference room. It contained several unencrypted case files. Investigators are determining if it contained sensitive personal information.

**Information Source:** Media

**August 15, 2006**  
**New Century Mortgage Corporation Irvine, California**  
On August 10, a former employee was found to have copied and disseminated customer information to unknown third parties. The information included names, addresses and Social Security numbers.

**Information Source:** Dataloss DB

**August 11, 2006**  
**Madrona Medical Group Bellingham, Washington**  
On Dec. 17, 2005, a former employee accessed and downloaded patient files onto his laptop computer. Files included name, address, SSN, and date of birth. The former employee has since been arrested.

**Information Source:** Dataloss DB

**August 10, 2006**  
**Bay View Acceptance Corporation Covina, California**  
Two disks were missing from a ripped package sent through UPS. The names, Social Security numbers, addresses and phone numbers of account holders were lost. The disks fell out of the package sometime before it arrived on July 12.
Sixty-eight New York residents were affected; the total number of affected customers was not released.

Information
Source: Dataloss DB
August 10, 2006 Weyerhaeuser Company
Washington, District Of Columbia
A book containing payroll data was stolen.

Information
Source: Dataloss DB
August 10, 2006 Manhasset-Lakeville Fire District
Great Neck, New York
A computer was lost or stolen during office renovations. The computer contained member names, dates of birth, Social Security numbers, addresses and names of beneficiaries. The computer is believed to have been destroyed.

Information
Source: Dataloss DB
August 10, 2006 American Heart Association AHA, KGMG
Dallas, Texas
KPMG International was conducting an audit of AHA's retirement accounts when an auditor's laptop was stolen from her car. KPMG notified AHA of the breach and informed them of which employees had their names and Social Security numbers on the laptop. The laptop was stolen from the vehicle at the auditor's home on July 21, but the information did not reach AHA employees until August 17.

Information
Source: Dataloss DB
August 10, 2006 U.S. Department of Transportation
Washington, District Of Columbia
(800) 424-9071, hotline@oig.dot.gov
The DOT's Office of the Inspector General reported a special agent's laptop was stolen on July 27 from a government-owned vehicle in Miami, FL, parked in a restaurant parking lot. It contained names, addresses, SSNs, and dates of birth for 80,670 persons issued commercial drivers licenses in Miami-Dade County, 42,800 persons in FL with FAA pilot certificates and 9,000 persons with FL driver's licenses.

UPDATE (11/21/06): A suspect was arrested in the same parking lot where the theft occurred, but the laptop has not been recovered. Investigators found a theft ring operating in the vicinity of the restaurant parking lot.

Information
Source: Dataloss DB
August 9, 2006 Hunter College of the City University of New York
New York, New York
A computer was stolen from the Writing Center in Thomas Hunter Hall on or around July 5. Its hard drive had a file that contained a list of student names and Social Security numbers. Students who participated in the Spring 2006 CPE intervention session were affected.

Information
Source: Dataloss DB
August 9, 2006 Hoffman-La Roche Inc, McCladrey and Pullen LLP
Washington, District Of Columbia
A laptop computer belonging to an employee of McCladrey and Pullen LLP was stolen on July 18. McCladrey conducts audits of Roche Savings and Pay Deferral Plan. The laptop included names, Social Security numbers, affiliation with the plan, plan account balance and 2005 plan withdrawal amounts.

Information
Source: Dataloss DB
August 8, 2006 Virginia Bureau of Insurance
Richmond, Virginia
(804) 726-2630
The Bureau has advised insurance agents in the state that their SSN may have been exposed on its web site from June 13 through July 31, 2006, due to a programming error. The SSNs were not shown on any web page, but could have been found by savvy computer users using the source code tool of a web browser.
August 8, 2006  Linens 'n Things  
Sterling, Virginia  

A folder holding about 90 receipts was missing from the store. Receipts included full credit or debit account number and name of the card holder.

August 8, 2006  Chautauqua County Department of Social Services  
Jamestown, New York  

Paperwork being used in Medicaid fraud investigations was stolen from an employee's car. The theft occurred sometime between July 31 and August 1. People who were being investigated may have had their private information exposed.

August 7, 2006  U.S. Department of Veterans Affairs via contractor Unisys Corporation  
Reston, Virginia  

Five thousand Philadelphia patients, 11,000 Pittsburgh patients and 2,000 deceased patients were affected. There is a possibility that 20,000 others were also affected.

A computer at contractor's office was reported missing Aug. 3. It contained billing records with names, addresses, SSNs, and dates of birth of veterans at two Pennsylvania locations.

UPDATE (9/15/06): Law enforcement recovered the computer and arrested an individual who had worked for a company that provides temporary labor to Unisys.

August 6, 2006  American Online (AOL)  
New York, New York  

Other locations: nationwide

In late July AOL posted on a public web site data on 20 million web queries from 650,000 users. Some search records exposed SSNs, credit card numbers, or other pieces of sensitive information.

UPDATE (9/26/06): Three individuals whose data were exposed have filed a lawsuit against AOL.

UPDATE (9/27/06): Six men were charged with creating and executing the phishing scheme. The men collected AOL email addresses and infected the computers of users with a program that asked for their credit card and bank account numbers during the AOL login process. AOL users were also spammed with phony email messages that asked for payment on AOL charges.

August 4, 2006  Toyota  
San Antonio, Texas  

Laptop belonging to contractor and containing personal information of job applicants and employees of a Toyota plant was stolen. Data included names and SSNs.

August 4, 2006  PSA HealthCare  
Norcross, Georgia  

A company laptop was stolen from an employee's vehicle in a public parking lot July 15. It contained names, addresses, SSNs, and medical diagnostic and treatment information used in reimbursement claims.
A laptop that contained the information of current and former clients was stolen from an employee sometime around July 24. The names, account numbers and tax identification or Social Security numbers of clients with claims may have been exposed.

Information Source: Dataloss DB

At least nine U.S. citizens were affected by a July 24 incident involving a stolen laptop. The laptop contained information that was assembled for filing claims on behalf of clients in pending class actions. Names, Social Security numbers, tax identification numbers and account numbers may have been exposed.

Information Source: Dataloss DB

A bank employee's briefcase was stolen from the employee's car with documents containing names, phone numbers, and SSNs of customers.

Information Source: Dataloss DB

WSU learned on June 29 that someone gained unauthorized access into 3 computers in its College of Fine Arts box office, containing credit card information for about 2,000 patrons.

Information Source: Dataloss DB

An intrusion into a WSU Psychology Department's server was discovered July 16. It contained information on about 40 applicants to the doctoral program.

Information Source: Dataloss DB

Customers of the discount store have reported money stolen from their bank accounts due to unauthorized ATM withdrawals. Data may have been intercepted by a thief's use of a wireless laptop computer with the thief then creating counterfeit ATM cards and using them to withdraw money.

UPDATE (10/5/06): Parkev Krmoian was indicted by a federal grand jury for allegedly using phony ATM cards made from gift cards. The case is tied to the Dollar Tree customer bank account thefts.

Information Source: Dataloss DB

Questions? Call: (503) 251-3349

Several months ago the car dealership experienced a security breach affecting the personal information of those who bought cars or applied for credit between 2001 and March 2006.
Information
Source: Dataloss DB
July 29, 2006  Sentry Insurance
Stevens Point, Wisconsin

BSF  INSD  112,270

Personal information including SSNs on worker’s compensation claimants was stolen, some of which was later sold on the Internet. At least 72 claimants of the 112,270 who may have had their information accessed had their information sold. No medical records were included. The thief was a lead programmer-consultant who had access to claimants' data. The consultant was arrested and faces felony charges.

Information
Source: Dataloss DB
July 28, 2006  Matrix Bancorp Inc.
Denver, Colorado

BSF  PORT  Unknown

(877) 250-7742

Two laptop computers were stolen during daytime while staffers were away from their desks. One computer contained customers’ account information. The bank says data is encrypted and password protected.

Information
Source: Dataloss DB
July 28, 2006  City of Riverside, California
Riverside, California

GOV  DISC  2,000

The SSNs and financial information regarding 401(k) accounts were accidentally e-mailed to 2,300 city employees due to a computer operator’s error. The data was intended for the city payroll department.

Information
Source: Dataloss DB
July 28, 2006  Merlin Information Services
Kalispell, Montana

BSO  HACK  3,957

The login information for a qualified customer was compromised. This resulted in the possible exposure of customer names, addresses and Social Security numbers.

Information
Source: Dataloss DB
July 27, 2006  Kaiser Permanente Northern California Office
Oakland, California

MED  PORT  160,000 records. Because the data file did not include SSNs, this number is not added to the total below.

(866) 453-3934

A laptop was stolen containing names, phone numbers, and the Kaiser number for each HMO member. The data file did not include SSNs. The data was being used to market Hearing Aid Services to Health Plan members.

Information
Source: Dataloss DB
July 27, 2006  Los Angeles County Department Community Senior Services
Los Angeles, California

GOV  PORT  Unknown

In May, a laptop was stolen from the home of a community and senior services employee. It contained information on LA County employees.

Information
Source: Dataloss DB
July 27, 2006  Los Angeles County, Community Development Commission (CDC)
Monterey Park, California

GOV  HACK  4,800 records (No SSNs or financial information reported)
Earlier in July, a computer hacker located in Germany gained access to the CDC's computer system, containing personal information on 4,800 public housing residents.

Information Source: Date: July 27, 2006

Los Angeles County, Adult Protective Services
Burbank, California

GOV PORT Unknown

Last weekend 11 laptops were stolen from the Burbank office. It is not clear what type of personal information was included.

Information Source: Date: July 26, 2006

U.S. Navy recruitment offices
Trenton, New Jersey

GOV PORT

Additional location: Jersey City, NJ

Two laptop computers with information on Navy recruiters and applicants were stolen in June and July. Also included was information from selective service and school lists. About 4,000 records contained SSNs. Files were password protected.

Information Source: Date: July 26, 2006

West Virginia Division of Rehabilitation Services
Beckley, West Virginia

GOV PORT Unknown

A laptop was stolen July 24 containing clients' names, addresses, SSNs, and phone numbers. Data was password protected.

Information Source: Date: July 26, 2006

Armstrong World Industries, Deloitte & Touche
Lancaster County, Pennsylvania

BSO PORT 12,000

A laptop containing personal information of current and former employers was stolen. The computer was in the possession of the company's auditor, Deloitte & Touche. Data included names, home addresses, phone numbers, SSNs, employee ID numbers, salary data, and bank account numbers of employees who have their checks directly deposited.

Information Source: Date: July 25, 2006

Belhaven College
Jackson, Michigan

EDU PORT 300

An employee carrying a laptop was robbed at gunpoint on July 19 while walking to his car. The computer contained the names and SSNs of college employees.

Information Source: Date: July 25, 2006

Georgetown University Hospital
Washington, District Of Columbia

MED DISC between 5,600 and 23,000 patients were affected (23,000 added to total below)

Patient data was exposed online via the computers of an e-prescription provider, InstantDx. Data included names, addresses, SSNs, and dates of birth, but not medical or prescription data. GUH suspended the trial program with InstantDx.

Information Source: Date: July 25, 2006
July 25, 2006

Old Mutual Capital Inc., subsidiary of United Kingdom-based financial services firm Old Mutual PLC
Kansas City, Missouri

BSF PORT 6,500 fund shareholders

Laptop was stolen sometime in May containing personal information of U.S. clients, including names, addresses, account numbers and some SSNs.

Information Source: Dataloss DB

records from this breach used in our total: 6,500

July 25, 2006

Cablevision Systems Corp., ACS, FedEx
Bethpage, New York

BSO PORT 13,700 current and former employees

Additional locations: Dallas, TX, Connecticut, New Jersey and New York

A tape en route to the company's 401(k) plan record-keeper ACS was lost when shipped by FedEx to Dallas, TX. No customer data was on the tape.

Information Source: Dataloss DB

records from this breach used in our total: 13,700

July 24, 2006

New York City Department of Homeless Services
New York, New York

GOV DISC 8,400

The personal information of 8,400 homeless persons, including SSNs, was leaked in an e-mail attachment July 21, when accidentally sent to homeless advocates and city officials.

Information Source: Dataloss DB

records from this breach used in our total: 8,400

July 24, 2006

Wolters Kluwer
Torrance, California

BSO PORT 8,500

A laptop with Social Security numbers, addresses, and some health plan information for current and former employees was stolen from a docking station at a private office on or around May 29. The laptop may have also included bank account information for 600 employees who had joined the company during 2006. Employees were notified in July.

Information Source: Dataloss DB

records from this breach used in our total: 8,500

July 24, 2006

Heritage Centers
Buffalo, New York

MED PHYS 31

An employee's briefcase was stolen from her car on June 18. The briefcase contained a list of the names, addresses, Social Security numbers, phone numbers, dates of birth and genders of 31 individuals.

Information Source: Dataloss DB

records from this breach used in our total: 31

July 19, 2006

Group 1 Automotive Inc, Weinstein Spira & Company, P.C.
Houston, Texas

BSF PORT 14,000

Five laptops were stolen from a Weinstein Spira office sometime between the night of July 10 and the morning of July 11. The laptops contained personal information of clients and the employees of clients. Names, addresses, Social Security numbers and financial data were accessed.

Information Source: Dataloss DB

records from this breach used in our total: 14,000

July 18, 2006

Nelnet Inc., UPS
Lincoln, Nebraska

BSO PORT 188,000

(800) 552-7925

A computer tape containing personal information of student loan customers and parents, mostly from Colorado, was lost when shipped via UPS. The loans were previously serviced by College Access Network between November 1, 2002 and May 31, 2006.

Information Source: Dataloss DB

records from this breach used in our total: 188,000

July 18, 2006

CS Stars, subsidiary of insurance company Marsh Inc.
Chicago, Illinois

BSF STAT 722,000

751
On May 9, CS Stars lost track of a personal computer containing records of more than a half million New Yorkers who made claims to a special workers' comp fund. The lost data includes SSNs and date of birth but apparently no medical information.

**UPDATE** (7/26/06): Computer was recovered.

**UPDATE** (04/26/07): The *New York Attorney General's office* found that CS Stars violated the state's security breach law. CS Stars must pay the Attorney General's office $60,000 for investigation costs. It was determined that the computer had been stolen by an employee of a cleaning contractor, the missing computer was located and recovered, and that the data on the missing computer had not been improperly accessed.

---

**Information Source:**
- Security Breach Letter
- Records from this breach used in our total: 722,000

**July 18, 2006**

**U.S. Department of Agriculture**

**Wellington, Kansas**

A laptop computer and a printout containing names, addresses and SSNs of 350 employees was stolen from an employee's car and later recovered.

**Information Source:**
- Dataloss DB
- Records from this breach used in our total: 350

**July 17, 2006**

**Vassar Brothers Medical Center**

**Poughkeepsie, New York**

An analysis by Kroll later determined that the laptop contained no personal information, though 257,800 patients were initially notified. This number is not included in the total below.

**UPDATE** (10/5/06) Private investigators determined the laptop did not contain personally identifiable patient information.

**Information Source:**
- Dataloss DB
- Records from this breach used in our total: 0

**July 16, 2006**

**Mississippi Secretary of State**

**Jackson, Mississippi**

The state agency's web site listed 2 million+ Uniform Commercial Code (UCC) filings in which thousands of individuals' SSNs were exposed.

**Information Source:**
- Dataloss DB
- Records from this breach used in our total: 2,000

**July 16, 2006**

**Columbia University**

**New York, New York**

On or around July 7, a computer was stolen from campus. The hard drive contained names, Social Security numbers, passport/visa numbers, tax identification numbers, home and business addresses, telephone contacts and email contacts.

**Information Source:**
- Dataloss DB
- Records from this breach used in our total: 78

**July 14, 2006**

**Northwestern University**

**Evanston, Illinois**


Files containing names and some personal information including SSNs were on 9 desktop computers that had been accessed by unauthorized persons outside the University. The computers were in the Office of Admissions and Financial Aid.

**Information Source:**
- Dataloss DB
- Records from this breach used in our total: 17,000

**July 14, 2006**

**University of Iowa**

**Davenport, Iowa**


Files containing names and some personal information including SSNs were on 9 desktop computers that had been accessed by unauthorized persons outside the University. The computers were in the Office of Admissions and Financial Aid.

**Information Source:**
- Dataloss DB
- Records from this breach used in our total: 280
Laptop computer containing personal information of current and former MBA students was stolen. Data files included SSNs and some contact info.

**Information Source:** Dataloss DB

**July 14, 2006**

**California Polytechnic State University (Cal Poly)**
San Luis Obispo, California

EDU PORT 3,020 students

Call (805) 756-2226 or (805) 756-2171

Laptop computer was stolen from the home of a physics department professor July 3. It included names and SSNs of physics and astronomy students from 1994-2004.

**Information Source:** Security Breach Letter

**July 14, 2006**

**Hampton Circuit Court Clerk - Treasurer’s computer**
Hampton, Virginia

GOV DISC Over 100,000 records (The number containing SSNs is not known yet and not included in total below.)

Public computer in city government building containing taxpayer information was found to display SSNs of many residents -- those who paid personal property and real estate taxes. It was shut down and confiscated by the police on July 12th.

**UPDATE** (7/27/2006) Investigation concluded that the data was exposed due to software problem.

**Information Source:** Dataloss DB

**July 13, 2006**

**Moraine Park Technical College**
Beaver Dam, Wisconsin

EDU PORT 1,500

Additional locations: Fond du Lac and West Bend, WI

Computer disk (CD) with personal information of 1,500 students was reported missing. Information includes names, addresses, phone numbers & SSNs of apprenticeship students back to 1993.

**Information Source:** Dataloss DB

**July 13, 2006**

**New York State Department of Motor Vehicles (DMV), New York State Thruway Authority**, New York

GOV INSD 57 (No SSNs or financial information reported)

A Thruway employee performed searches of DMV records without authorization. The discovery was made on December 27, but the length of time this employee engaged in the behavior was not reported. The employee had access to all the information contained on driver’s licenses.

**Information Source:** Dataloss DB

**July 7, 2006**

**University of Tennessee**
Knoxville, Tennessee

EDU HACK 36,000

(866) 748-1680, [http://security.tennessee.edu](http://security.tennessee.edu). Additional locations: Chattanooga, Martin, Tullahoma and Memphis, TN

Hacker broke into a UT computer containing names, addresses and SSNs of about 36,000 past and current employees. The intruder used the computer from Aug. ’05 to May ’06 to store and transmit movies.

**Information Source:** Dataloss DB

**July 7, 2006**

**National Association of Securities Dealers (NASD)**
Boca Raton, Florida

BSF PORT 73

Ten laptops were stolen on Feb. 25 ’06 from NASD investigators. They included SSNs of securities dealers who were the subject of investigations involving possible misconduct. Inactive account numbers of about 1,000 consumers were also contained on laptops.
July 7, 2006  
**Naval Safety Center, United States Navy**  
Norfolk, Virginia  
GOV  DISC  100,000

The SSNs and other personal information of more than 100,000 naval and Marine Corps aviators and air crew, both active and reserve, were exposed on the Center website and on 1,100 computer discs mailed to naval commands.

July 7, 2006  
**Montana Public Health and Human Services Department**  
Helena, Montana  
MED  STAT  Unknown

A state government computer was stolen from the office of a drug dependency program during a 4th of July break-in. It was not known if sensitive information such as SSNs was compromised.

July 7, 2006  
**City of Hattiesburg**  
Hattiesburg, Mississippi  
GOV  STAT  thousands of city workers and contractors (at least 2,000)

Video surveillance cameras caught 2 intruders stealing hard drives from 18 computers June 23. Data files contained names, addresses, and SSNs of current and former city employees and registered voters as well as bank account information for employees paid through direct deposit and water system customers who paid bills electronically.

July 6, 2006  
**Automatic Data Processing (ADP)**  
Roseland, New Jersey  
BSO  UNKN  0

Payroll service company ADP gave scam-artist names, addresses, and number of shares held of investors, although apparently not SSNs or account numbers. The leak occurred from Nov. '05 to Feb. '06 and involved individual investors with 60 companies including Fidelity, UBS, Morgan Stanley, Bear Stearns, Citigroup, Merrill Lynch. Hundreds of thousands of investors may have been affected.

July 5, 2006  
**Bisys Group Inc.**  
Roseland, New Jersey  
BSF  PORT  61,000

Personal details about 61,000 hedge fund investors were lost when an employee's truck carrying backup tapes was stolen. The data included SSNs of 35,000 individuals. The tapes were being moved from one Bisys facility to another on June 8 when the theft occurred.

July 5, 2006  
**RBS National Bank, Asset Acceptance LLC**  
Bridgeport, Connecticut  
BSF  PORT  1,221

A laptop was stolen from an Asset Acceptance LLC employee's car on June 19. The laptop contained information from RBS National Bank. Customer names, addresses, Social Security numbers, phone numbers and loan information may have been accessed.

July 5, 2006  
**Columbia University**  
New York, New York  
EDU  DISC  98

An emergency contact list from the Columbia University School of International and Public Affairs was posted on an unsecure website on August 2005. Names, business and home phone numbers, addresses, emergency contact person and Social Security numbers were available.
Sometime in May, three laptops were stolen, one of them containing encrypted personal information including names, SSNs, dates of birth, and medical information of all regional donors. They also report losing a laptop with encrypted donor information in June 2005.

Information Source:
Dataloss DB

June 30, 2006
U.S. Department of Veteran Affairs
Washington, District Of Columbia
GOV PORT 16,500

A data tape disappeared from a VA facility in Indianapolis, IN that contained information on legal cases involving U.S. veterans and included veterans’ Social Security numbers, dates of birth and legal documents.

UPDATE (10/11/06): The VA’s Office of the General Counsel is offering identity theft protection services to those affected by the missing tape.

Information Source:
Dataloss DB

June 30, 2006
National Institutes of Health Federal Credit Union
Rockville, Maryland
BSF UNKN

NIHFCU and law enforcement are investigating the identity theft of some of its 41,000 members. No details were given on the type of information stolen, or how it was stolen.

Information Source:
Media

June 30, 2006
Washington Regional Medical Center
Fayetteville, Arkansas
GOV PORT 5,000

A computer from the Human Resources Division of Washington Regional Medical Center was stolen on April 14. The computer was stolen from the employee’s office during a 45 minute absence. Current and former employees may have had their personal information exposed.

Information Source:
Dataloss DB

June 29, 2006
AllState Insurance Huntsville branch
Huntsville, Alabama
BSF STAT 27,000

Over Memorial Day weekend, a computer containing personal data including images of insurance policies, correspondence and Social Security numbers was stolen.

Information Source:
Dataloss DB

June 29, 2006
Nebraska Treasurer’s Office
Lincoln, Nebraska
GOV HACK 309,000

A hacker broke into a child-support computer system and may have obtained names, Social Security numbers and other information such as tax identification numbers for 9,000 businesses.

Information Source:
Dataloss DB

June 29, 2006
Minnesota Department of Revenue
St. Paul, Minnesota
GOV PORT 50,400

http://www.taxes.state.mn.us/taxes/publications/press_releases/content/taxpayer_information.shtml

On May 16, a package containing a data tape used to back up the regional office’s computers went missing during delivery. The tape contained personal information including individuals’ names, addresses, and Social Security numbers.

UPDATE (7/20/06): The package was reported delivered 2 months later, but apparently had been temporarily lost by the U.S. Postal Service.

Information Source:
Dataloss DB
Data from audit reports on Defense Department travel vouchers from the 1970s were inadvertently posted online and included some service members' names, Social Security numbers and addresses. The agency has subsequently removed the information.

**Information Source:**
Dataloss DB

**June 27, 2006**
**Empire Beauty School Inc.**
**Brooklyn, New York**

EDU PHYS 1,132

The June 20 theft of a briefcase from an administrative employee's vehicle caused reports with the names and Social Security numbers of former students to be lost. A laptop was also stolen during the burglary, but it is unlikely that it had personal information.

**Information Source:**
Dataloss DB

**June 27, 2006**
**University of Rochester**
**Rochester, New York**

EDU DISC 286

Former students' names and Social Security numbers were accidentally placed on a publicly accessible web page. Names, Social Security numbers and some standardized test scores were posted. The information was removed after the discovery and it appears that the information on the web page was accessed only once, on June 12 2006.

**Information Source:**
Dataloss DB

**June 27, 2006**
**Maimonides Medical Center, Vision Financial Corp.**
**Harrison, New York**

MED PORT 560

On June 9, an employee of Maimonides' contractor Vision Financial was robbed of personal belongings and a laptop that contained client information. Names, Social Security numbers, addresses, birth dates and amount owed to the Maimonides may have been exposed.

**Information Source:**
Dataloss DB

**June 26, 2006**
**AAAAA Rent-A-Space**
**Colma, California**

BSO DISC 13,000

Customer's account information including name, address, credit card, and Social Security number was easily accessible due to a security gap in AAAAA's online payment system.

**Information Source:**
Dataloss DB

**June 26, 2006**
**King County Elections**
**Seattle, Washington**

GOV DISC Unknown

Public election records with Social Security numbers were made available online. Like in other counties, individuals can request that their specific information be removed by submitting a written request.

**Information Source:**
Dataloss DB

**June 24, 2006**
**Catawba County Schools**
**Newton, North Carolina**

EDU UNKN 619

On June 22, it was discovered that a web site posted names, Social Security numbers, and test scores of students who had taken a keyboarding and computer applications placement test during the 2001-02 school year.

**UPDATE:** The web site containing the data has been removed.

**Information Source:**
Dataloss DB

**June 24, 2006**
**Social Security Administration**
**Atlanta, Georgia**

GOV PORT 228

People in Roanoke, Salem, Blacksburg, Christiansburg, Radford, Rocky Mount, Buchanan, Wytheville, Pulaski, Pearisburg and Fincastle were affected.
A lawyer working for the Social Security Administration broke a work-at-home agreement and brought a laptop with sensitive information to a conference in Atlanta. The laptop was stolen there. Social Security numbers, names and possibly medical information would have been on the laptop.

Information Source: Dataloss DB
June 23, 2006 San Francisco State University
San Francisco, California
EDU PORT 3,000

www.sfsu.edu/%7Eadminrec/reg/idtheft.html

A faculty member’s laptop was stolen from a car on June 1 that contained personal information of former and current students including Social Security numbers, and names and in some instance, phone numbers and grade point averages.

Information Source: Dataloss DB
June 23, 2006 U.S. Navy
Washington, District Of Columbia
GOV UNKN 28,000

Navy personnel were notified on June 22 that a civilian website contained files with personal information of Navy members and dependents including names, birth dates and Social Security numbers.

Information Source: Dataloss DB
June 23, 2006 CBCInnovis Inc., Andover Bank
Conneaut, Ohio
BSF UNKN 1,122

Names, Social Security numbers, addresses, names of creditors, account numbers, payment histories and public records of financial judgments may have been accessed without proper authorization at Andover Bank.

Information Source: Dataloss DB
June 22, 2006 Ohio University
Athens, Ohio
EDU HACK 2,480

http://www.ohio.edu/datasecurity

A breach was discovered on a computer that housed IRS 1099 forms for vendors and independent contractors for calendar years 2004 and 2005.

Information Source: Media
June 22, 2006 Ohio University
Athens, Ohio
EDU HACK Unknown

http://www.ohio.edu/datasecurity

A computer was compromised that hosted a variety of Web-based forms, including some that processed online business transactions. Although this computer was not set up to store personal information, investigators did discover files that contained fragments of personal information, including Social Security numbers. The data is fragmentary and it is not certain if the compromised information can be traced to individuals. Also found on the computer were 12 credit card numbers that were used for event registration.

Information Source: Media
June 22, 2006 University of Kentucky
Lexington, Kentucky
EDU PORT 6,500

The personal data of current and former students including classroom rosters names, grades and Social Security numbers was reported stolen on May 26 following the theft of a professor’s flash drive.

Information Source: Dataloss DB
June 22, 2006 U.S. Department of Agriculture (USDA)
Washington, District Of Columbia
GOV HACK 26,000

http://www.firstgov.gov/usdainfo.shtml

During the first week in June, a hacker broke into the Department’s computer system and may have obtained names,
Social Security numbers and photos of current and former employees and contractors.

Information Source: Dataloss DB

June 22, 2006  
**Federal Trade Commission (FTC)**  
**Washington, District Of Columbia**  
GOV PORT 110

Two laptop computers containing personal and financial data were stolen from an employee's vehicle. The data included names, addresses, Social Security numbers, dates of birth, and in some instances, financial account numbers gathered in law enforcement investigations.

Information Source: Dataloss DB

June 21, 2006  
**Cumberland County Emergency Medical Service**  
**Fayetteville, North Carolina**  
MED PORT 24,350

Portable computer containing personal information of more than 24,000 people was stolen from ambulance of Cumberland Co. Emergency Medical Services on June 8th. It contained information on people treated by the EMS, including names, addresses, and birthdates, plus SSNs of 84% of those listed.

Information Source: Dataloss DB

June 21, 2006  
**Lancaster General Hospital**  
**Lancaster, Pennsylvania**  
EDU STAT Hundreds (at least 200)

Date of letter sent to doctors: June 21, 2006  
Date of news story: July 28, 2006

A desktop computer with personal information of hundreds of doctors was stolen from a locked office June 10. The unencrypted data included names, practice addresses, and SSNs of physicians on medical and dental staff.

Information Source: Security Breach Letter

June 20, 2006  
**Equifax**  
**Atlanta, Georgia**  
BSF PORT 2,500

On May 29, a company laptop containing employee names and partial and full Social Security numbers was stolen from an employee.

Information Source: Dataloss DB

June 20, 2006  
**University of Alabama**  
**Birmingham, Alabama**  
EDU STAT 9,800

In February a computer was stolen from a locked office of the kidney transplant program at the University of Alabama at Birmingham that contained confidential information of donors, organ recipients and potential recipients including names, Social Security numbers and medical information.

Information Source: Dataloss DB

June 20, 2006  
**New Jersey Department of Labor and Workforce Development**  
**Jersey City, New Jersey**  
GOV DISC 498

Customers are being notified that their personal information may have been unintentionally mailed to other customers. A malfunction in the mail processing equipment meant that personal information of unemployment insurance claimants was included with the information of other people. Names, addresses and Social Security numbers were exposed.

Information Source: Dataloss DB

June 18, 2006  
**ING U.S. Financial Services, Jackson Health System**  
**Miami, Florida**  
BSF PORT 13,000

Two ING laptops that carried sensitive data affecting Jackson Health System hospital workers were stolen in December 2005. The computers, belonging to financial services provider ING, contained information gathered during a voluntary life insurance enrollment drive in December and included names, birth dates and Social Security numbers.

Information Source: Dataloss DB
A laptop was stolen from an employee’s home. It contained retirement plan information including Social Security numbers of D.C. city employees.

Information Source: Dataloss DB

June 18, 2006

Ulster County Community College
Stone Ridge, New York

EDU PORT 18

A laptop that contained student information was stolen from a professor’s office on or around June 28. The information included names and Social Security numbers.

Information Source: Dataloss DB

June 17, 2006

Western Illinois University
Macomb, Illinois

EDU HACK 180,000

http://www.wiu.edu/securityalert/

On June 5th, a hacker compromised a University server that contained names, addresses, credit card numbers and Social Security numbers of people connected to the University.

UPDATE (7/5/06): Number affected reduced from 240,000.

Information Source: Dataloss DB

June 17, 2006

Automatic Data Processing (ADP)
Roseland, New Jersey

BSO DISC 80

Personal and payroll information of workers were intended to be faxed between ADP offices and were mistakenly sent to a third party.

Information Source: Dataloss DB

June 17, 2006

California Department of Health Services (CDHS)
Sacramento, California

GOV PHYS 1,550

http://www.applications.dhs.ca.gov/pressreleases/store/PressReleases/06-41.html

On June 12, a box of Medi-Cal forms from December 2005 were found in the cubicle of a California Dept. of Health Services employee. The claim forms contained the names, addresses, Social Security numbers and prescriptions for beneficiaries or their family members.

Information Source: Dataloss DB

June 16, 2006

Union Pacific
Omaha, Nebraska

BSO PORT 30,000

On April 29th, an employee’s laptop was stolen that contained data for current and former Union Pacific employees, including names, birth dates and Social Security numbers.

Information Source: Dataloss DB

June 16, 2006

New York State Controller’s Office
Albany, New York

GOV PORT 1,300

A state controller data cartridge containing payroll data of employees who work for a variety of state agencies was lost during shipment. The data contained names, salaries, Social Security numbers and home addresses.

Information Source: Dataloss DB

June 16, 2006

California Department of Health Services (CDHS)
Sacramento, California

GOV PHYS 1,550

http://www.applications.dhs.ca.gov/pressreleases/store/PressReleases/06-41.html
CDHS documents were inappropriately emptied from an employee’s cubicle on June 5 and 9 rather than shredded. The documents contained state employees and other individuals applying for employment with the state including names, addresses, Social Security numbers and home and work telephone numbers. They were mostly expired state employment certification lists, but also included requests for personnel action, copies of e-mail messages and handwritten notes.

Information Source: Dataloss DB

June 14, 2006  **American International Group (AIG), Indiana Office of Medical Excess, LLC**
New York, New York  
BSF  STAT  930,000

The computer server was stolen on March 31 containing personal information including names, Social Security numbers, birth dates, and some medical and disability information.

**UPDATE** (1/12/2010) A 28-year-old Indianapolis man was sentenced today to two years in state prison for trying to extort $208,000 from an insurance company after stealing a computer server. In March 2006, the man burglarized the Indianapolis office of AIG Medical Excess, threatening to release clients’ personal data on the Internet. The server contained the names of more than 900,000 insured persons, as well as their personal identifying information, and confidential medical information and e-mail communications. At the time of the burglary, the man was an employee of a private security firm that provided security services to the insurance company. On July 23, 2008, Stewart delivered a package to the insurance company. The package included a letter stating that he possessed the stolen server and its confidential data. He asked for $1,000 a week for four years, but the FBI and others intervened. The Indiana State Police, the Indiana Department of Natural Resources, Indianapolis Metropolitan Police Department, and Attorney General also were part of the investigation.

Information Source: Dataloss DB

June 14, 2006  **Law Finance Group Holdings, LLC**
Reno, Nevada  
BSF  STAT  1,237

On April 7, the organization discovered that a computer server had been stolen from its office. The equipment stored information on customers, employees, and prospects. The information included names, Social Security numbers and addresses.

Information Source: Dataloss DB

June 13, 2006  **Minnesota State Auditor**
St. Paul, Minnesota  
GOV  PORT  493

Three laptops possibly containing Social Security numbers of employees and recipients of housing and welfare benefits along with other personal information of local governments the auditor oversees have gone missing.

Information Source: Dataloss DB

June 13, 2006  **Oregon Department of Revenue**
Salem, Oregon  
GOV  HACK  2,200

Electronic files containing personal data of Oregon taxpayers may have been compromised by an ex-employee who downloaded a contaminated file from a porn site. The trojan attached to the file may have sent taxpayer information back to the source when the computer was turned on.

Information Source: Dataloss DB

June 13, 2006  **U.S. Dept of Energy, Hanford Nuecer Reservation**
Richland, Washington  
GOV  UNKN  4,000

Current and former workers at the Hanford Nuclear Reservation were notified that their personal information may have been compromised, after police found a 1996 list with workers’ names, Social Security numbers, birth dates, work titles, assignments, and telephone numbers in a home during an unrelated investigation.

Information Source: Dataloss DB

June 13, 2006  **State of Minnesota**
Minneapolis, Minnesota  
GOV  PORT  Unknown

Three laptops with sensitive information were lost or stolen from the office of a state auditor. The missing laptops may have contained Social Security numbers and other personal information on local government employees. There was no evidence of forced entry and the office is not normally accessible to the general public.
June 12, 2006  Fish & Richardson  Boston, Massachusetts

The June 12 home theft of a laptop resulted in the exposure of current and former employee information. Names and Social Security numbers had once been saved on the laptop. Three former employees were not notified because their contact information could not be found.

Information Source:  Dataloss DB

June 12, 2006  Barnard College  New York, New York

A hacking incident that was discovered on June 6 may have left the names and Social Security numbers of students and employees exposed. The computer that was compromised may have allowed the hacker to access information for all students and employees.

Information Source:  Dataloss DB

June 11, 2006  Denver Election Commission  Denver, Colorado

Records containing personal information on more than 150,000 voters are missing at city election offices. The microfilmed voter registration files from 1989 to 1998 were in a 500-pound cabinet that disappeared when the commission moved to new offices in February. The files contain voters' Social Security numbers, addresses and other personal information.

Information Source:  Dataloss DB

June 11, 2006  Adams State College  Alamosa, Colorado

A laptop computer stolen from a locked closet at Adams State College contained personally identifiable data belonging to 184 high school students who participated in the college's Upward Bound program over the last four years. The theft occurred on August 14, but it was not until late September that staff realized the computer held students' data.

Information Source:  Dataloss DB

June 10, 2006  Nationwide Retirement Solutions  Phoenix, Arizona

The office theft of several laptop computers resulted in the exposure of personal information. City and county employees in Southern Arizona may have had their names, Social Security numbers, birth dates and addresses exposed.

Information Source:  Dataloss DB

June 8, 2006  University of Michigan Credit Union  Ann Arbor, Michigan

Paper documents containing personal information of credit union members were stolen from a storage room. The documents were supposed to have been digitally imaged and then shredded. Instead, they were stolen and used to perpetrate identity theft.

Information Source:  Dataloss DB

June 7, 2006  Colorado Mental Health Institute Fort Logan  Denver, Colorado

A briefcase with paper files was taken from an employee's car while it was at a park on April 21. The briefcase contained paper files with the information of 40 employees and 247 patients. Only 29 employees and 40 patients had their Social Security numbers exposed. Other information included names, addresses, gender and birth dates. Those affected were notified in early June.

Information Source:  Dataloss DB

June 6, 2006  University of Texas at El Paso  El Paso, Texas

Students demonstrated that student body and faculty elections could be rigged by hacking into student information.
Students demonstrated that student body and faculty elections could be rigged by hacking into student information including Social Security numbers.

Information Source: Dataloss DB
June 6, 2006 U.S. Department of Energy
Washington, District Of Columbia GOV HACK 1,502

Names, Social Security numbers, security clearance levels and place of employment for mostly contract employees who worked for National Nuclear Security Administration may have been compromised when a hacker gained entry to a computer system at a service center in Albuquerque, NM eight months prior to press releases.

Information Source: Dataloss DB
June 6, 2006 ARAMARK Corporation
Atlanta, Georgia BSO PORT 6,028

The May 5 theft of a laptop resulted in the exposure of personal information of current and former employees. Social Security numbers and other personal information were lost.

Information Source: Dataloss DB
June 6, 2006 Empire State College
Saratoga Springs, New York EDU INSD 16

On December 15 of 2005, an intruder installed key-logger was discovered on a computer that had been used to access Social Security numbers. The keystroke capture program was installed by a relative of an employee in order to capture and read email messages that the staff member was sending. The program was in operation from March 2004 to January 2005 and again from October 2005 to December 15. The affected PC was removed from the office and had its hard drive scanned and cleaned.

Information Source: Dataloss DB
June 6, 2006 Thomson West
Eagan, Minnesota BSO PORT Unknown

A laptop was discovered stolen on or around April 28. The information on the laptop included employee names, Social Security numbers, addresses and phone numbers. Notifications were sent in early June.

Information Source: Dataloss DB
June 5, 2006 U.S. Internal Revenue Service (IRS)
Washington, District Of Columbia GOV PORT 291

A laptop computer containing personal information of employees and job applicants, including fingerprints, names, Social Security numbers, and dates of birth, was lost during transit on an airline flight.

Information Source: Security Breach Letter
June 5, 2006 Kingsbrook Jewish Medical Center
Brooklyn, New York MED PORT 34,863

A personal computer was stolen from the Hospital's outpatient billing office on December 26, 2005. It is likely that the computer contained spreadsheets with patient names and Social Security numbers embedded in insurance numbers. Those affected were notified May 26, 2006.

Information Source: Dataloss DB
June 3, 2006 Buckeye Community Health Plan
Columbus, Ohio MED PORT 72,000

Four laptop computers containing customer names, Social Security numbers, and addresses were stolen from the Medicaid insurance provider.

Information Source: Dataloss DB
June 3, 2006
June 3, 2006  Humana  Louisville, Kentucky MED DISC and former Medicare enrollees

Personal information of Humana customers enrolled in the company's Medicare prescription drug plans could have been compromised when an insurance company employee called up the data through a hotel computer and then failed to delete the file.

**Information Source:**

Dataloss DB

records from this breach used in our total: 17,000

June 2, 2006  Ahold USA, parent company of Stop & Shop, Giant stores and Tops stores via subcontractor Electronic Data Systems (EDS) Landover, Maryland BSR PORT 92,000

Additional location: Plano, TX

An EDS employee lost a laptop computer during a commercial flight that contained pension data of former employees of Ahold’s supermarket chains including Social Security numbers, birth dates and benefit amounts. The laptop was lost from the checked baggage of a domestic commercial airline flight on May 2, 2006. The laptop was not recovered even though the incident was reported immediately.

**Information Source:**

Dataloss DB

records from this breach used in our total: 92,000

June 1, 2006  Miami University Oxford, Ohio EDU PORT 851

An employee lost a hand-held personal computer containing personal information of students who were enrolled between July 2001 and May 2006.

**Information Source:**

Dataloss DB

records from this breach used in our total: 851

June 1, 2006  Ernst & Young New York, New York BSO PORT 243,000

Additional locations: Throughout the US and UK. Breach occurred in Texas.

A laptop containing names, addresses and credit or debit card information of Hotels.com customers was stolen from an employee's car in Texas.

**Information Source:**

Media

records from this breach used in our total: 243,000

June 1, 2006  University of Kentucky Lexington, Kentucky EDU DISC 1,300

Personal information of current and former University of Kentucky employees including Social Security numbers was inadvertently accessible online for 19 days in May.

**Information Source:**

Dataloss DB

records from this breach used in our total: 1,300

June 1, 2006  YMCA of Greater Providence Providence, Rhode Island NGO PORT 65,000

A laptop computer containing personal information of members was stolen. The information included credit card and debit card numbers, checking account information, Social Security numbers, the names and addresses of children in daycare programs and medical information about the children, such as allergies and the medicine they take, though the type of stolen information about each person varies. Those affected were notified.

**Information Source:**

Dataloss DB

records from this breach used in our total: 65,000

May 31, 2006  Texas Guaranteed Student Loan Corp. via subcontractor Hummingbird Round Rock, Texas BSF UNKN 1,300,000 plus 400,000 for total of 1,700,000

Additional location: Toronto, Canada

Texas Guaranteed (TG) was notified by subcontractor Hummingbird that on May 24, an employee had lost a piece of equipment containing names and Social Security numbers of TG borrowers.

**UPDATE** (6/16/06): TG now says a total of 1.7 million people’s information was compromised, 400,000 more than original estimate of 1.3 million.
Hacker accessed a database that contained personal information on thousands of individuals, such as student and applicant names and Social Security numbers.

The University was informed that a file containing sensitive information remained in the Google cache and could be accessed by those with technological expertise. The file was first indexed in October of 2005. The file was deleted from the server, but it remained in the Google files cache. The file included names, addresses, Social Security numbers, and dates of birth of some current and former employees and their dependents.

The California Department of Financial Institutions has offices in Sacramento, San Francisco, Los Angeles and San Diego.

On May 26, an examiner's laptop was stolen from a car. The laptop contained the personal data of bank customers.

Hacker gained access to member accounts and stole personal information including names, addresses, birth dates, mother's maiden names, Social Security numbers and/or email addresses. Less than 10% of VyStar's 344,000 members were affected.

Security Saving's website host Goldleaf Technologies informed the bank that their website was down. The website had been phished for two hours. Thirteen customers visited the fraudulent website during that time. Passwords, user IDs, account numbers and card numbers could have fallen into the wrong hands.

It was discovered on May 8th that a computer containing personal information including names, addresses and Social Security numbers was breached. The University did not immediately release information on who the breach affected.

An agency laptop computer was stolen from an employee's car. Names and Social Security numbers were on the laptop.

A security breach of a Department of Public Safety computer server potentially exposed names, Social Security numbers and driver's license numbers. Individuals whose personal information was compromised were contacted.
In April, three laptop computers were stolen from the agency’s office. They contained personal information on mental health clients, including Social Security numbers. Those affected were contacted in May.

A former employee was arrested for extortion for attempting to blackmail his former employer for $6.9 million. He threatened to expose company files containing sensitive customer information - including customers' names, addresses, Social Security numbers, loan numbers, and loan types - if the company didn't pay him. He stole the files over the 16 months he worked there.

Two company laptops were stolen in California in March and one company laptop was stolen in Kentucky in April. One incident exposed some customer names and Social Security numbers that were listed along with their claims. The other incident exposed names and Social Security numbers for employees of some of Liberty's commercial insureds.

On May 3, data of all American veterans who were discharged since 1975 including names, Social Security numbers, dates of birth and in many cases phone numbers and addresses, were stolen from a VA employee's home. Theft of the laptop and computer storage device included data of 26.5 million veterans. The data did not contain medical or financial information, but may have disability numerical rankings.

UPDATE (6/29/06): The stolen laptop computer and the external hard drive were recovered.

UPDATE (7/14/06): FBI claims no data had been taken from stolen computer.

UPDATE (8/5/06): Two teens were arrested in the theft of the laptop.

UPDATE (8/25/06): In an Aug. 25 letter, Secretary Nicholson told veterans of the decision to not offer them credit monitoring services. Rather the VA has contracted with a company to conduct breach analysis to monitor for patterns of misuse.

UPDATE (11/2/07): A federal judge questioned the Veterans Affairs Department's computer security and ruled Friday that lawsuits can go forward over the theft of computer equipment containing data on 26.5 million veterans. The lawsuits have been filed as potential class-action cases representing every veteran whose data was released.

UPDATE (1/23/09): The Department of Veterans Affairs has agreed to pay $20 million to current and former military personnel to settle a class action lawsuit.

UPDATE (6/16/09): No less than $75 will be paid for any valid claim, up to a cap of $1,500. If your expenses were higher than that, you might want to opt out of the class-action portion so you can file for your actual damages. In that case, you need to file a letter so it is received by June 29, 2009. You have until Nov. 27, 2009, to mail your claim form to VA Settlement Claims, P.O. Box 6727, Portland, OR 97228-9767. Be sure to keep a copy of the claim form, along with your proof of mailing. To download the claim form and to get more information, go to www.veteransclass.com. Read the FAQ and note the particulars on out-of-pocket expenses and actual damages. You also can call (888) 288-9625.

UPDATE (10/19/12): An investigation into the VA revealed that encryption software has only been installed on 16% of VA computers since the 2006 breach. Six million dollars has been spent on encryption software since the 2006 breach. The investigation began after a 2011 anonymous tip.

A security problem may have exposed customer credit and check card information.
Hackers accessed the credit and debit card accounts of around 100 Frost Bank customers after they took Visa and MasterCard debit card information from the database of a national retailer. Banks across the nation were affected by the breach. Only 100 Frost Bank customers reported fraudulent charges.

A dishonest employee had access to Social Security numbers of donors. The database was used to call previous donors and urge them to give blood again. The employee misused the personal information of at least three people to perpetrate identity theft and had access to the personal information of one million donors.

A laptop computer, owned by PFPC, a third party company that provides record keeping services for M & T’s Portfolio Architect accounts was stolen from a vehicle. The laptop contained clients’ account numbers, Social Security numbers, last name and the first two letters of their first name.

An unencrypted hard drive containing names, addresses and Social Security numbers of AICPA members was lost when it was shipped back to the organization by a computer repair company. AICPA offered one year of free credit monitoring services to affected members.

During an investigation of a computer virus, it was discovered that computers within an office may have been accessed without authorization from within the campus network. Student, faculty and staff names and Social Security numbers were on archived spreadsheets. The spreadsheets contained the personal information of people who requested campus cards between 1998 and 2004.

GE Money Bank issues private label credit cards for Lowe’s Companies Inc. A number of credit card applications were taken form a Lowe’s store in Philadelphia by an unknown person. The information on the applications included names, Social Security numbers, dates of birth, addresses and Lowe’s credit card account numbers. At least 11 consumers discovered fraudulent purchases at Lowe’s stores.
Four computers with the personal information of clients were stolen during an early April burglary. The information did not include credit files, but did have other forms of private customer data.

Names, birth dates, Social Security numbers and medical information were accessed in records of students dating back to 2001, plus faculty, workers and regional campus students.

An employee's laptop computer was stolen during a burglary. The computer contained limited personal information of some current and former Merrill Lynch clients and prospects. The information included names, addresses, account and loan numbers, account and loan balances and the name of clients' financial advisors.

Google accessed confidential information on the HBR website and made the information available on the internet. Social Security numbers, names, phone numbers, dates of birth, addresses and diagnostic information were accessible through Google. Access to the information is now restricted to authorized users with secure identification and passwords. The information was available between August 2005 and January of 2006.

A computer containing names, addresses, Social Security numbers and mortgage loan deposit numbers of existing and prospective customers may have been stolen while being delivered from one bank facility to another.

A sales tax field auditor reported a laptop missing. Contents of the laptop were unknown at the time of the report. The data exposed may have included sales tax audit reports and supporting documentation from closed sales tax audits on 38 businesses. Some of this information would include Social Security number, business and/or home address and bank account information.

Four company hard drives were sold on eBay containing hundreds of thousands of confidential company documents, employee names and Social Security numbers, and confidential memos to the company's CEO.
May 2, 2006  
Ohio University Innovation Center  
Athens, Ohio  
http://www.ohio.edu/datasecurity

A server containing data including e-mails, patent and intellectual property files, and 35 Social Security numbers associated with parking passes was compromised.

Information Source:  
Dataloss DB

records from this breach used in our total: 35

May 2, 2006  
Ohio University  
Athens, Ohio  
http://www.ohio.edu/datasecurity/

Hackers accessed a computer system of the school’s alumni relations department that included biographical information and 137,000 Social Security numbers of alum.

UPDATE (8/30/07): An Ohio judge has granted a motion to dismiss a case against Ohio University (OU) regarding security breaches of the school’s computer systems that compromised alumni data. The two alumni who filed the lawsuit wanted OU to pay for credit monitoring services for everyone whose data were compromised. The judge said the pair had not proven that they had suffered damages for which they could be compensated.

Information Source:  
Dataloss DB

records from this breach used in our total: 137,000

May 2, 2006  
Georgia State Government  
Atlanta, Georgia  

Government surplus computers that sold before their hard drives were erased contained credit card numbers, birth dates, and Social Security numbers of Georgia citizens. The State stopped selling the computers after being notified by a buyer. Thousands of patient records from a psychiatric hospital in Rome, Georgia were found on one computer’s hard drive.

Information Source:  
Dataloss DB

records from this breach used in our total: 0

May 2, 2006  
Countrywide Home Loans  
Plano, Texas  

A former employee is suspected of ordering customer credit reports and providing some of those reports to a third party.

Information Source:  
Dataloss DB

records from this breach used in our total: 90

May 1, 2006  
CBCInnovis Bank Inc., Great Florida Bank  
Miami, Florida  

CBCInnovis, Inc. learned that Great Florida Bank had consumer information accessed without proper authorization. The information may have included names, addresses, Social Security numbers, names of creditors, account numbers, payment histories and financial public records.

Information Source:  
Dataloss DB

records from this breach used in our total: 518

April 28, 2006  
Ohio Secretary of State  
Cleveland, Ohio  

The names, addresses, and Social Security numbers of potentially millions of registered voters in Ohio were included on CD-ROMs distributed to 20 political campaign operations for spring primary election races. The records of about 7.7 million registered voters are listed on the CDs, but it’s unknown how many records contained Social Security numbers, which were not supposed to have been included on the CDs.

UPDATE (9/15/06): A news report said that some Social Security numbers still remain on the agency’s Web site.

Information Source:  
Dataloss DB

Potentially millions of registered voters

April 28, 2006  
U.S. Department of Defense  
Washington, District Of Columbia  

A hacker accessed a Tricare Management Activity (TMA) public server containing personal information about military
employees. TMA is used to provide health care services to military personnel and their families.

**Information Source:** Dataloss DB

**April 28, 2006**

**Sears, Roebuck, Company Contractor Compliance**

**Winter Park, Florida**

BSF DISC 196

A spreadsheet with the business or individual names, identification or Social Security numbers, business addresses and business phone numbers of Sears contractors was accidentally included in an email sent to 373 contractors on April 13. The contractors were instructed to delete the email on April 24 and were also required to send written confirmation that they had done so.

**Information Source:** Dataloss DB

**April 27, 2006**

**Long Island Railrad via contractor Iron Mountain**

**Jamaica, New York**

GOV PORT 17,000

Data tapes containing personal information including names, addresses, Social Security numbers and salary figures of virtually everyone who worked for or currently works for the agency were lost. The lost occurred during delivery by contractor Iron Mountain. Data tapes belonging to the U.S. Department of Veteran’s Affairs may also have been affected.

**Information Source:** Dataloss DB

**April 26, 2006**

**Purdue University**

**West Lafayette, Indiana**

EDU HACK 1,351

A hacker accessed personal information including Social Security numbers of current and former graduate students, applicants to graduate school, and a small number of applicants for undergraduate scholarships. The information compromised goes back three years prior to the incident. Those who were affected were contacted.

**Information Source:** Dataloss DB

**April 26, 2006**

**Aetna, Omni Hotels and the Department of Defense NAF**

**Hartford, Connecticut**

MED PORT 38,253

A laptop containing personal information including names, addresses and Social Security numbers of Department of Defense (35,253) and Omni Hotel employees (3,000) was stolen from an Aetna employee’s car. Members were notified and Aetna offered to pay for the credit monitoring services of those who were affected.

**Information Source:** Dataloss DB

**April 26, 2006**

**Pershing LLC**

**Jersey City, New Jersey**

BSF PORT 92,541

A Pershing employee lost a laptop computer. Personal information of clients may have been stored on the laptop. Names, Social Security numbers, addresses, brokerage account numbers and account holdings may have been exposed.

**Information Source:** Dataloss DB

**April 26, 2006**

**Amica Mutual Insurance**

**Lincoln, Rhode Island**

BSF PORT 751 (number includes only New York residents)

An Amica computer tape with personal information regarding insurance claims was lost in transit. Amica believes the tape was also destroyed or badly damaged in transit.

**Information Source:** Dataloss DB

**April 26, 2006**

**Sterling Renaissance Festival**

**Syracuse, New York**

BSO HACK Unknown

Customers with questions may call (315) 947-5782.

Someone was able to access online orders of Brandywine Limited multiple times between 4/18/06 and 4/20/06. The online order forms include customer names, addresses, credit card numbers and credit card information. Some customers may have also had their telephone numbers and email addresses exposed.
A stolen computer contained the information of students who took engineering classes. The information included names, grades and student identification numbers. Hundreds of students are at risk of identity theft since Social Security numbers were used as student identification numbers.

A hacker accessed the Campus' primary web server and set up a file sharing system. The server involved also contained access databases that had names and Social Security numbers.

Foreign hackers accessed records containing names, biographical information and, in some cases, Social Security numbers and dates of birth of current and prospective students, alumni, faculty members, corporate recruiters and staff members.

A hacker had access to names, Social Security numbers, and partial e-mail addresses of current and former students, faculty, and staff. The University reported that it would not contact those affected after a first and second notification. Anyone claiming to be from the University after these notifications should be viewed with suspicion.

A laptop was taken from a Boeing human resources employee at Sea-Tac airport. It contained Social Security numbers and other personal information, including personnel information from the 2000 acquisition of Hughes Space and Communications.

Customers may call (949) 475-6255.

Several laptops were stolen. Saved emails with the names and Social Security numbers of customers may have been on one of the stolen laptops.

Bear Stearn's realized that unauthorized users could access customer accounts. Former customers could still log into online accounts if their account numbers had been recycled and given to new users. Such information included account holdings and activities, account statements and IRS Forms 1099-DIV and 1099-INT (which included name, address, account number and Social Security number).
A laptop used to submit insurance applications was stolen from a field associate’s home during a burglary. It may have contained the names and Social Security numbers of policyholders and certificate holders.

April 17, 2006

Visiting Nurse Service of New York (VNSNY)
New York, New York

Three separate thefts resulted in the loss of three tablet computers. The computers were used by therapists who were making therapy treatment visits to patients. The personal information on the computers included Social Security numbers. VNSNY warned that unauthorized persons might use the stolen tablets to pose as therapists and enter patient homes.

April 14, 2006

NewTech Imaging
Honolulu, Hawaii

Records containing the names, Social Security numbers and birth dates of more than 40,000 members of Voluntary Employees Benefit Association of Hawaii were illegally reproduced at a copying business before they were to be put onto a compact disc for the State. Police later found the data on a computer that had been confiscated as part of a drug investigation. Those who were on the list and Hawaii Government Employees Association and United Public Workers members who were enrolled in union-sponsored health and group life insurance plans between July and December 1999 were warned. Investigators were only able to speculate that the theft may have occurred in February of 2005.

April 14, 2006

University of South Carolina
Columbia, South Carolina

A department chair distributing information about summer courses sent an email containing sensitive information. A database containing Social Security numbers of students was mistakenly added as an attachment and e-mailed to classmates.

April 13, 2006

Fifth Third Bank
Evansville, Indiana

An employee was able to gain access to around 1,000 customer accounts. He used this information to stalk and harass female news celebrities. He now faces two felony counts of attempting to defraud using personal information and two misdemeanor counts of stalking and repeated harassment.

April 12, 2006

Ross-Simons
Providence, Rhode Island

A security breach exposed account and personal information of those who applied for Ross-Simons' private label credit card. Information exposed includes private label credit card numbers and other personal information of applicants.

April 12, 2006

Greenpoint Mortgage Funding Inc., KPMG International
Novato, California

Laptop computers were stolen from two employees of KPMG who were working with data from Greenpoint. The laptops are believed to have contained customer names, Social Security numbers and FICO scores. At least 32 people from New York alone were affected by the early March theft. Customers were notified during the middle of April.

April 10, 2006

Broward County Records Division
Fort Lauderdale, Florida
Broward County public records with Social Security numbers, driver’s license information and bank account details were made available online. The information has been available online for several years. A new statute that will require county recorders to remove Social Security numbers and financial information from public documents before posting documents online will take effect in 2007. The sensitive information that has already been posted will eventually be removed. Individuals can speed up the process of having their specific information removed by submitting a written request.

Information
Source: Dataloss DB
April 9, 2006  University of Medicine and Dentistry of New Jersey
Newark, New Jersey
EDU HACK 1,850

Hackers accessed Social Security numbers, loan information, and other confidential financial information of students and alumni.

Information
Source: Dataloss DB
April 7, 2006  DiscountDomainRegistry.com
Brooklyn, New York
BSO DISC thousands of domain name registrations

Domain name registrants’ personal information including user names, passwords and credit card numbers was accessible online. The information may have been exposed online for four months.

Information
Source: Dataloss DB
April 6, 2006  Progressive Casualty Insurance
Mayfield Village, Ohio
BSF INSD 13

A dishonest insider accessed confidential information, including names, Social Security numbers, birth dates and property addresses on foreclosure properties she was interested in buying.

Information
Source: Dataloss DB
April 1, 2006  Con Edison
New York, New York
BSO PORT 15,000 Con Edison employees

Con Edison shipped two cartridge tapes to JPMorgan Chase in upstate Binghamton so it could input data on behalf of the NY Dept. of Taxation and Finance. One tape was apparently lost and contained employees’ W-2 data, including names, addresses, Social Security numbers, taxes paid and salaries.

Information
Source: Dataloss DB
April 1, 2006  Shorter College
Rome, Georgia
EDU HACK Unknown

A student was arrested for computer theft and hacking the College’s computer network. The student may have accessed student, staff and faculty information.

Information
Source: Dataloss DB
March 31, 2006  Security Mutual Life Insurance Company of New York
New York, New York
BSF PORT 167

The March 9 theft of a laptop resulted in the exposure of the personal information of disability insurance clients. Client names, Social Security numbers and dates of birth may have been exposed.

Information
Source: Dataloss DB
March 30, 2006  U.S. Marine Corp
Monterey, California
GOV PORT 207,750

A portable drive containing the personal information of Marines was lost in a campus computer lab. The lost drive was being used for research on Marine re-enlistment bonuses and contained names, Social Security numbers, marital status, and enlistment contract details. Enlisted marines on active duty between January 2001 and December of 2005 were
affected. The University notified those whose information may have been compromised.

**Information Source:**
Dataloss DB

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Category</th>
<th>Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 30, 2006</td>
<td>Georgia Technology Authority (GTA)</td>
<td>GOV HACK</td>
<td>573,000</td>
</tr>
<tr>
<td></td>
<td>Atlanta, Georgia</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hackers exploited a security flaw to gain access to confidential information including Social Security numbers and bank-account details of state pensioners. The State only had contact information for 180,000 of those affected and relied on media coverage to get the word out to others.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>March 30, 2006</td>
<td>Connecticut Technical High School System</td>
<td>EDU DISC</td>
<td>1,250</td>
</tr>
<tr>
<td></td>
<td>Middletown, Connecticut</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Social Security numbers of faculty and administrators were mistakenly distributed via email to staff. The email went to 17 principals; at least one forwarded the email to her staff of 77. Those affected were contacted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>March 30, 2006</td>
<td>Snyder, Cohn, Collyer, Hamilton and Associates, P.C., Murry’s Inc.</td>
<td>BSF PORT</td>
<td>Unknown</td>
</tr>
<tr>
<td></td>
<td>Bethesda, Maryland</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>US Protect Corporation was also involved.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A laptop was stolen from Snyder on February 9. Snyder provided the accounting services for Murry’s pension plan and others. The laptop may have contained Social Security numbers, dates of birth and pay information.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>March 29, 2006</td>
<td>University of Nebraska Lincoln (UNL)</td>
<td>EDU DISC</td>
<td>342</td>
</tr>
<tr>
<td></td>
<td>Lincoln, Nebraska</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Students from the College of Engineering had Social Security numbers, email addresses, grade point averages and other personal information posted online. The information may have been posted since November of 2004 and was first noticed in summer of 2005. The problem was finally fixed during the week of March 29 when the file was removed from the Google server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>March 24, 2006</td>
<td>California State Employment Development Division</td>
<td>GOV DISC</td>
<td>64,000</td>
</tr>
<tr>
<td></td>
<td>Sacramento, California</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A computer glitch sent state Employment Development Division 1099 tax forms containing Social Security numbers and income information to the wrong addresses, potentially exposing those taxpayers to identity theft.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>March 24, 2006</td>
<td>Vermont State Colleges</td>
<td>EDU PORT</td>
<td>14,000</td>
</tr>
<tr>
<td></td>
<td>Waterbury, Vermont</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: there are several locations in Vermont. We list the Office of the Chancellor as the primary location.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A laptop containing Social Security numbers and payroll data of students, faculty and staff associated with the five-college system was stolen. It contained information from as long ago as 2000.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>March 24, 2006</td>
<td>California State University, Dominquez Hills</td>
<td>EDU PORT</td>
<td>2,486</td>
</tr>
<tr>
<td></td>
<td>Carson, California</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Students can leave a message at (310) 243-2305 for more information.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The theft of a laptop resulted in the exposure of student and potential student personal information. The University tightened access to campus servers and the campus network.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>Company/Location</td>
<td>Industry</td>
<td>Action</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------</td>
<td>----------</td>
<td>--------</td>
</tr>
<tr>
<td>March 23, 2006</td>
<td>Fidelity Investments, Boston, Massachusetts</td>
<td>BSF, PORT</td>
<td>196,000</td>
</tr>
<tr>
<td>March 22, 2006</td>
<td>District of Columbia Board of Elections and Ethics, Washington, District Of Columbia</td>
<td>GOV, DISC</td>
<td>Unknown</td>
</tr>
<tr>
<td>March 16, 2006</td>
<td>Bananas.com, San Rafael, California</td>
<td>BSR, HACK</td>
<td>274</td>
</tr>
<tr>
<td>March 16, 2006</td>
<td>Mortgage Institute of Michigan, Southfield, Michigan</td>
<td>BSF, UNKN</td>
<td>67</td>
</tr>
<tr>
<td>March 15, 2006</td>
<td>Ernst &amp; Young, IBM, New York, New York</td>
<td>BSF, PORT</td>
<td>84,000</td>
</tr>
<tr>
<td>March 14, 2006</td>
<td>General Motors (GM), Detroit, Michigan</td>
<td>BSO, INSD</td>
<td>100</td>
</tr>
<tr>
<td>March 14, 2006</td>
<td>Buffalo Bisons and Choice One Online, Buffalo, New York</td>
<td>BSO, HACK</td>
<td>Unknown</td>
</tr>
</tbody>
</table>
Mailed applications of DCA licensees or prospective licensees for CA state boards and commissions were stolen. The forms include full or partial Social Security numbers, driver’s license numbers, and potentially payment checks.

Information Source: Dataloss DB

March 10, 2006  
**Long Island University, Alpha Chi National Honors Society**  
Brooklyn, New York  
EDU DISC 51

Students who applied to join Alpha Chi had their Social Security numbers and other personal information sent to an Honors student email list. The email was recalled immediately, but anyone who opened it right away would have been able to access the applicant information. The advisor responsible for the mistake asked the National Office to consider abandoning the use of Social Security numbers.

Information Source: Dataloss DB

March 8, 2006  
**Verizon Communications**  
New York, New York  
BSO PORT Unknown

Two laptops containing employees’ personal information including Social Security numbers were stolen. Verizon is offering affected employees free use of a credit monitoring service.

Information Source: Dataloss DB

March 8, 2006  
**iBill [disputed]**  
Deerfield Beach, Florida  
BSF UNKN 17,781,462 (SSNs and financial information not involved)

A dishonest insider or possibly malicious software linked to iBill was used to post names, phone numbers, addresses, e-mail addresses, Internet IP addresses, login names and passwords, credit card types and purchase amount online. Credit card account numbers, expiration dates, security codes, and Social Security numbers were NOT included, but in our opinion the affected individuals could be vulnerable to social engineering to obtain such information. Whether iBill is the source of the breach has been disputed.

Information Source: Dataloss DB

March 7, 2006  
**Audiolink LLC (Audio Link)**  
Orlando, Florida  
BSR HACK 25

A hacker may have accessed customer names, addresses, telephone numbers, email addresses and credit card information from the company’s website. Audiolink disabled the credit card functions on their website and updated web security.

Information Source: Dataloss DB

March 6, 2006  
**First Horizon Home Loans**  
Lake Oswego, Oregon  
BSF STAT 8

A desktop computer was stolen from one of First Horizon’s financial centers. The desktop contained customer and client files with names, addresses, phone numbers, Social Security numbers and mortgage account numbers.

Information Source: Dataloss DB

March 5, 2006  
**Georgetown University**  
Washington, District Of Columbia  
EDU HACK 41,000

A server was attacked that housed personal information including names, birthdates and Social Security numbers of District seniors served by the Office on Aging. Georgetown managed the server as part of a grant to manage information services provided by the D. C. Office of Aging.

Information Source: Dataloss DB

March 3, 2006  
**Metropolitan State College of Denver (MSCD)**  
Denver, Colorado  
EDU PORT 93,000
A laptop containing student information was stolen. The information included names and Social Security numbers of students who registered for Metropolitan State courses between the 1996 fall semester and the 2005 summer semester.

**Information Source:**
Security Breach Letter

**March 3, 2006**  
**PayDay OK LLC**  
**Ruidoso, New Jersey**  

The company’s website was breached sometime around February 19 by a hacker in an attempt to gain access to certain customers' private information. Social Security numbers, names, addresses, bank account names and bank account numbers may have been compromised. At least 88 individuals were affected.

**Information Source:**
Dataloss DB

**March 2, 2006**  
**Olympic Funding**  
**Chicago, Illinois**

Three hard drives containing clients' names, Social Security numbers, addresses and phone numbers stolen during a break in. Information on the drives was protected via password and security software. The business owner sent letters to his clients alerting them of the theft.

**Information Source:**
Dataloss DB

**March 2, 2006**  
**Los Angeles County Department of Social Services**  
**Los Angeles, California**

It is unclear if this is the same incident that involved the information of 94,000 people being left next to a recycling bin outside of the Department of Public Social Services in January of 2006.

File boxes containing names, dependents, Social Security numbers, telephone numbers, medical information, employer, W-2, and date of birth were left unattended for at least one month. This affects employees and clients.

**Information Source:**
Dataloss DB

**March 2, 2006**  
**Hamilton County Clerk of Courts**  
**Cincinnati, Ohio**

Social Security numbers, and other personal data of residents was posted on the County’s website. Some information was stolen and used to commit identity theft.

**UPDATE** (9/28/06): An identity thief was sentenced to 13 years in prison for the crimes. She stole 100 identities and nearly $500,000. The Web site now blocks access to court documents containing personal information.

**Information Source:**
Dataloss DB

**March 1, 2006**  
**Medco Health Solutions**  
**Columbus, Ohio**

A laptop containing Social Security numbers for State of Ohio employees and their dependents, as well as their birth dates and, in some cases, prescription drug histories was stolen from an employee. The theft occurred in December and Medco contacted Ohio officials in February. The company agreed to provide free credit monitoring and fraud alert services for the affected families for one year.

**Information Source:**
Dataloss DB

**February 23, 2006**  
**Deloitte & Touche, McAfee**

Deloitte & Touche is an international organization with multiple locations throughout the United States.

An external auditor lost a CD with names, Social Security numbers and stock holdings in McAfee of current and former McAfee employees. Three thousand current employees and 6,000 former employees were affected. Current and former employees received two years of free credit monitoring services from Equifax.
February 22, 2006
New Hampshire Department of Motor Vehicles, New Hampshire

Malware was discovered on the DMV server during a routine security check. Though there is no evidence of misuse, credit card information could have been accessed. It is unknown how the malware application got onto the computer. The FBI confiscated the computer.

February 22, 2006
University of Texas M.D. Anderson Cancer Center
Houston, Texas

A laptop containing insurance information for patients was stolen from a PricewaterhouseCoopers employee’s home in November. Patients and patient families were notified in January that their private health information, policy numbers, dates of birth, ZIP codes and Social Security numbers may have been exposed.

February 20, 2006
Capital Computer Associates, Spencerport School District
Albany, New York

Seventeen employees of Spencerport School District had their Social Security numbers and names posted on a website that could be viewed by any office staff at Capital Computer’s client sites in New York State school districts and Boards of Cooperative Educational Services (BOCES). The information was supposed to be fictitious and used to notify users of changes to the software they use to process accounting and human resource data. The posting occurred on February 14 and was removed at the end of the day on February 16.

February 20, 2006
Alltel Corporation
Little Rock, Arkansas

Customer files with cell phone records, Social Security numbers, addresses and phone numbers were found in a dumpster. A landscaper discovered the files and alerted a news crew. A spokesperson for the company said that this is against their official electronic policy.

February 18, 2006
University of Northern Iowa
Cedar Falls, Iowa

A laptop computer holding W-2 forms of student employees and faculty was illegally accessed. The University warned students and faculty to monitor their bank accounts.

February 17, 2006
California Department of Corrections, Pelican Bay State Prison
Sacramento, California

Inmates gained access to files stored in a warehouse. The files contained employees’ Social Security numbers, birth dates and pension account information.

February 17, 2006
Mount St. Mary’s Hospital
Lewiston, New York

Two laptops containing dates of birth, addresses and Social Security numbers of patients were stolen in an armed robbery in New Jersey. The laptops and sensitive files were password protected. The Hospital contacted those whose information may have been compromised. St. Mary’s is just one of ten hospitals that were affected by the theft.

February 16, 2006
Blue Cross and Blue Shield
Jacksonville, Florida
A contractor sent names and Social Security numbers of current and former employees, vendors and contractors to his home computer in violation of company policies. A judge ordered the former computer consultant to reimburse the Jacksonville-based health insurer $580,000 for expenses related to his theft.

Information Source: Dataloss DB
February 16, 2006
University of Washington Medical Center
Seattle, Washington
MED HACK Unknown

The hacked system serves users at Harborview Medical Center, University of Washington Medical Center, University of Washington School of Medicine, UW Medicine Neighborhood Clinics and UW Physicians.

A hacker broke into the UW Medicine computer system in June of 2004. The incident was not discovered until December of 2005. The hacker may have accessed and copied patient and business records for 18 months. The goal of the hacker appears to have been to use the system for its computing power and data storage.

Information Source: Dataloss DB
February 16, 2006
The Princeton Review
New York, New York
BSR DISC Unknown

An unauthorized user attempted to obtain the IDs and passwords of a small number of account holders. A small number of the accounts may have contained names, Social Security numbers, dates of birth, email addresses, mailing addresses and information from college applications. The unauthorized user may have had access to the information before the February 10 incident was discovered. At least 35 New York residents were affected.

Information Source: Dataloss DB
February 15, 2006
U.S. Department of Agriculture (USDA)
Washington, District Of Columbia
GOV DISC 350,000

The Social Security numbers of tobacco farmers were accidentally released when the U.S. Department of Agriculture attempted to comply with the Freedom of Information Act. Those who received the information agreed to destroy any copies and return the original discs, which also contained tax identification numbers.

Information Source: Dataloss DB
February 15, 2006
Old Dominion University
Norfolk, Virginia
EDU DISC 601

An instructor posted a class roster containing names and Social Security numbers to a publicly accessible website. The information was posted during the spring semester of 2004. Letters were sent to affected students which contained websites where the students could check to see if they had been victims of identity theft.

Information Source: Dataloss DB
February 15, 2006
Suffolk County Clerk's Office
Long Island, New York
GOV DISC 7,000

Between 7,000 and 8,000 homeowners had their Social Security numbers accidentally posted online. After realizing the mistake, County officials realized that they could not remove the information. People who pay to access the County's public records online will be able to see the Social Security numbers associated with people and addresses in the system that date back to 2001. The county could not alter public records in any way, but a new program will be implemented to block the Social Security numbers from newly recorded documents.

Information Source: Dataloss DB
February 13, 2006
Ernst & Young
New York, New York
BSO PORT 38,000

Additional locations: Throughout the US and UK

38,000 BP employee in U.S. In addition to Sun, Cisco and IBM employees.

A laptop containing the names, dates of birth, genders, family sizes, Social Security numbers and tax identifiers for current and previous IBM, Sun Microsystems, Cisco, Nokia and BP employees was stolen from a locked car. While Ernst and Young waited until pressured to inform a majority of those affected about the breach, at least one CEO from the affected companies was contacted immediately.

Information Source: Security Breach

records from this breach used in our total: 27,000
records from this breach used in our total: 0
records from this breach used in our total: 0
records from this breach used in our total: 350,000
records from this breach used in our total: 601
records from this breach used in our total: 7,000
records from this breach used in our total: 38,000

778
February 9, 2006
OfficeMax
Naperville, Illinois

BSR HACK
200,000, although total number is unknown.

The location listed is Office Max's headquarters. Sam's Club and other businesses may have also been affected.

Debit card accounts and pin numbers from bank and credit union accounts nationwide (including CitiBank, BoFA, WaMu, Wells Fargo) were exposed. The crooks created counterfeit cards to make fraudulent purchases and withdrawals from card-holder accounts.

UPDATE (3/14/06) New Jersey law enforcement arrested 14 people connected to the crime spree.

Information
Source: DataLoss DB

February 6, 2006
Prudential Financial Inc.
Newark, New Jersey

BSF DISC 1,000

A health insurer claims data were erroneously faxed to a company in Canada by doctors and clinics across the U.S.. Data included the patients' Social Security numbers, bank account details and health care information.

Information
Source: Media

February 4, 2006
FedEx
Los Angeles, California

BSO DISC 1,100

Up to 1,100 workers in Los Angeles and Orange Counties could be affected.

Eighty-five hundred W-2 forms including other workers' tax information such as Social Security numbers and salaries were sent out to employees. Fewer than 1,100 employees had their information exposed. The company suspects that their internal processing center may have misaligned the forms and caused them to be cut in the wrong place. Workers were asked not to open their W-2s, but many had already done so before the notification.

Information
Source: DataLoss DB

February 2, 2006
Presbyterian Healthcare Service
Albuquerque, New Mexico

MED STAT 450

The theft of a computer may have exposed patient and physician information. Names, Social Security numbers, addresses, phone numbers and credit card numbers were on the computer. The computer may have been stolen for the purpose of committing identity theft.

Information
Source: DataLoss DB

February 1, 2006
Blue Cross and Blue Shield of North Carolina
Durham, North Carolina

BSO DISC 629

Social Security numbers of members were printed on the mailing labels of envelopes with information about a new insurance plan. Those who were affected were contacted immediately.

Information
Source: DataLoss DB

February 1, 2006
University of Colorado, Colorado Springs (UCCS)
Colorado Springs, Colorado

EDU HACK 2,500

Names, Social Security numbers, addresses and birth dates of current and former employees were accessed. A computer in the Personnel Department was hacked and infected with a virus. People employed by the University at anytime between the attack and 2004 are at risk. The virus infected other computers at the University and was part of a worldwide attack.

Information
Source: DataLoss DB

January 31, 2006
Boston Globe (The New York Times Company) and The Worcester Telegram & Gazette
Boston, Massachusetts

BSO DISC 240,000

Recycled paper used in wrapping newspaper bundles for distribution turned out to contain credit and debit card information along with routing information for personal checks of subscribers.
January 31, 2006  Honeywell International
Morristown, New Jersey

BSO  UNKN  19,000

Personal information of current and former employees including Social Security numbers and bank account information was posted on an Internet Web site. It was not known whether this was the result of a malicious insider or an administrative error. Current and former employees whose information was compromised were informed immediately and offered free credit monitoring and identity theft insurance.

January 27, 2006  State of Rhode Island website (www.RI.gov)
Providence, Rhode Island

GOV  HACK  4,118

Hackers obtained credit card information in conjunction with names and addresses. The credit card companies were notified of the breach, but not the customers.

January 26, 2006  College of St. Scholastica
Duluth, Minnesota

EDU  STAT  12,000

A computer was stolen from a locked office in the College’s information Technology Department on or around December 24. The computer had Social Security numbers and names of current and former students. The thief was caught and claims that none of the personal information was used.

January 25, 2006  Providence Home Services
Portland, Oregon

MED  PORT  365,000

Backup tapes, laptops and disks containing Social Security numbers, clinical and demographic information were stolen from the car of an employee. In a small number of cases, patient financial data was stolen.

UPDATE (9/26/06) Providence Health System and the Oregon Attorney General have filed a settlement agreement. Providence will provide affected patients with free credit monitoring, offer credit restoration to patients who are victims of identity fraud, and reimburse patients for direct losses that result from the data breach. The company must also enhance its security programs.

UPDATE (7/15/08) Providence Health will pay $100,000 and adhere to a compliance plan under the first ever Resolution Agreement negotiated by CMS (Centers for Medicare and Medicaid Services of the U.S. Dept. of Health and Human Services) under the HIPAA Privacy and Security Standards. The Corrective Action Plan requires Providence to revamp its security policies to include physical protections for portable devices and off-site transport and storage of backup media. Further, it must implement technical safeguards, such as encryption and password protection. And it must conduct random compliance audits and submit compliance reports to HHS for the next three years.

UPDATE (4/16/2012): The Oregon Supreme Court struck down a class-action suit against Providence Health Systems. The Oregon Supreme Court claimed that there was no evidence that any of the 365,000 patients who were affected by the breach suffered any financial loss or other adverse consequences.

January 25, 2006  University of Delaware
Newark, Delaware

EDU  STAT  159

Two separate breaches occurred on the campus during November and December. A computer from the School of Urban Affairs and Public policy was hacked and a back-up hard drive was stolen from the Department of Entomology and Wildlife Ecology. The hacking incident occurred between November 22 and 26 and exposed the Social Security numbers of 159 graduate students. The hard drive theft occurred between December 16 and 18 and the personal information of an unknown number of people was exposed.

January 24, 2006  University of Washington Medical Center
Seattle, Washington

MED  PORT  1,600

Laptops containing names, Social Security numbers, maiden names, birth dates, diagnoses and other personal data were stolen from a UW office. The information was password protected and the affected patients were notified.
January 23, 2006

University of Notre Dame
Notre Dame, Indiana

EDU  HACK  Unknown

Hackers may have accessed Social Security numbers, credit card information and check images of people who donated to the University between November 22 of 2005 and January 12 of 2006.

January 21, 2006

California Army National Guard
Sacramento, California

GOV  PHYS  Hundreds (at least 200)

A briefcase with personal information of National Guardsmen including a seniority roster, Social Security numbers and dates of birth was stolen from the car of an employee. A memo was sent to National Guard soldiers.

January 20, 2006

Indiana University, University Place Conference Center & Hotel
Indianapolis, Indiana

BSO  HACK  Unknown

The computer housing the reservations data base was compromised. Data included credit card account numbers and names.

January 20, 2006

University of Kansas (Kansas University)
Lawrence, Kansas

EDU  DISC  9,200

A computer file with sensitive personal information was accessible to the public. Students who applied and paid an application fee online between April 29, 2001 and December 16, 2005 had their names, Social Security numbers, birth dates, addresses, phone numbers and credit card numbers exposed.

January 17, 2006

City of San Diego, Water & Sewer Department
San Diego, California

GOV  INSD  Unknown

A dishonest employee accessed customer account files, including Social Security numbers, and stole the identities of two individuals.

January 16, 2006

New York City Teachers Retirement System
New York, New York

GOV  INSD  5,800

A dishonest employee and two others were arrested for their part in writing and cashing fraudulent checks. Police found fraudulent checks with the names of 19 pension members and beneficiaries in the apartment of the former employee. The employee was originally hired as a temp and had worked for the company for three years. He had access to the information of 5,800 pension members.

January 15, 2006

Illinois Education Association
Springfield, Illinois

NGO  STAT  Unknown

Two laptops, six desktops and a digital camera were stolen from the Illinois Education Association office sometime prior to the week of January 3. Some of the computers contained Social Security numbers of members. Many member organizations were affected. Over 2,400 members from the Elgin Area School District were affected.

January 12, 2006

People's Bank
Bridgeport, Connecticut

BSF  PORT  90,000
A computer tape containing names, addresses, Social Security numbers, and checking account numbers was lost while being transported by UPS. The bank alerted the affected customers and provided them with a credit monitoring service for one year.

**Information Source:**
Dataloss DB

**January 2, 2006**  
**H&R Block**  
**Kansas City, Missouri**  
BSO DISC Unknown

H&R Block included Social Security numbers in a 40-digit number string on mailing labels. Affected individuals were contacted.

**Information Source:**
Dataloss DB

**January 1, 2006**  
**University of Pittsburgh Medical Center, Squirrel Hill Family Medicine**  
**Pittsburgh, Pennsylvania**  
MED STAT 700

Six computers containing names, Social Security numbers, and birth dates of patients were stolen from doctors' offices. A letter was sent notifying the affected patients.

**Information Source:**
Dataloss DB

**December 28, 2005**  
**Marriott International Inc.**  
**Orlando, Florida**  
BSR PORT 206,000

It is unclear whether backup computer tapes with credit card account information and Social Security numbers were lost or stolen from headquarters during November. Employees and time-share owners and customers were affected.

**Information Source:**
Dataloss DB

**December 25, 2005**  
**Ameriprise Financial Inc.**  
**Minneapolis, Minnesota**  
BSF PORT 226,000

(877) 267-7408

A laptop was stolen from an employee's car on Christmas eve. It contained customers' names and Social Security numbers and in some cases, Ameriprise account information. Around 68,000 customers had their names and Social Security numbers exposed. Around 158,000 customers had their names and internal account numbers exposed.

**UPDATE (08/01/06):** The laptop was recovered by local law enforcement in the community where it was stolen.

**UPDATE (12/11/06):** The company settled with the Massachusetts securities regulator in the office of the Secretary of State. Ameriprise agreed to hire an independent consultant to review its policies and procedures for employees' and contractors' use of laptops containing personal information. Ameriprise will pay the state regulator $25,000 for the cost of the investigation.

**Information Source:**
Dataloss DB

**December 22, 2005**  
**Ford Motor Co.**  
**Dearborn, Michigan**  
BSO STAT 70,000

A computer containing names and Social Security numbers of current and former employees was stolen. Ford alerted those who were affected and offered to pay for their credit monitoring services.

**Information Source:**
Dataloss DB

**December 22, 2005**  
**H&R Block**  
**Kansas City, Missouri**  
BSO DISC Unknown

Many past and present customers received unsolicited copies of the program TaxCut that displayed their Social Security numbers on the outside, embedded in a lengthy string of code.

**Information Source:**
Security Breach Letter

**December 21, 2005**  
**Sunrise Volkswagen**  
**Lynbrook, New York**  
BSR PHYS Unknown

Bank credit applications with names, Social Security numbers, addresses, telephone numbers, employment information
and signatures were obtained by unauthorized access between December 15 and 16.

Information Source: Dataloss DB

December 20, 2005 Guidance Software, Inc. Pasadena, California BSO HACK 3,800

A hacked database exposed credit card numbers of law enforcement officials and network security professionals. The company is a leading provider of software used to diagnose hacked attacks.

UPDATE (4/3/07): The FTC came to a settlement agreement and final consent order against Guidance Software.

Information Source: Dataloss DB

December 16, 2005 La Salle Bank, ABN AMRO Mortgage Group, DHL Ann Arbor, Michigan BSF PORT [2,000,000] Not included in total below.

A backup tape with residential mortgage customers' information was lost in shipment by DHL. It contained Social Security numbers and account information.

UPDATE (12/20/05): DHL found the lost tape.

Information Source: Security Breach Letter

December 16, 2005 Colorado Technical University (CTU) Colorado Springs, Colorado EDU DISC 300

An email was erroneously sent which contained names, phone numbers, email addresses, Social Security numbers and class schedules.

Information Source: Security Breach Letter

December 12, 2005 Sam's Club, a division of Wal-Mart Stores, Inc Bentonville, Arkansas BSR UNKN Unknown

Note: location is corporate headquarters, not necessarily the location of the breach.

Customers who used credit cards at the wholesaler's gas stations discovered fraudulent activity on their credit accounts. Sam’s Club is unaware of how the information was stolen. Visa alerted the affected financial institutions and asked them to provide fraud monitoring services for the affected customers.

Information Source: Dataloss DB

December 12, 2005 Iowa State University Ames, Iowa EDU HACK 5,500

At least one ISU computer was hacked. Social Security numbers and encrypted credit card numbers may have been obtained. Between 2,000 and 2,500 Social Security numbers are at risk and between 2,300 and 3,000 credit card numbers are at risk. Student, alumni, employee and volunteer information was put at risk.

Information Source: Dataloss DB

December 9, 2005 Oregon Community Credit Union Springfield, Oregon BSF PHYS 200

A packet of insurance forms with names, Social Security numbers and addresses of around 200 Oregon Community Credit Union employees was inside of a stolen car. Someone tried to use the identity of an employee after the theft. The company is on alert and purchased extended identity theft insurance for those who were affected by the theft.

Information Source: Dataloss DB

December 8, 2005 San Antonio Independent School District San Antonio, Texas EDU PORT 1,000

A laptop with personal information of more than a thousand teachers was stolen from an employee's unlocked car. The
information included names, Social Security numbers and dates of birth.

**Information**
**Source:** Dataloss DB

**J-Sargeant Reynolds Community College**
Richmond, Virginia

EDU DISC 26,000

The names, Social Security numbers and addresses of students taking non-credit classes from 2000 to 2003 were posted online for months. The information was compiled for a mailing list, but an employee posted it on the College's server. A student informed officials of the mistake after accessing the information online. The College began the process of removing the information from the web.

**Information**
**Source:** Dataloss DB

**Federal Reserve Bank of Dallas**
Dallas, Texas

GOV PHYS 8,000

A courier truck dropped canceled personal and business checks on northbound Central Expressway near Woodall Rodgers Freeway around 4 a.m. The incident closed the freeway exit until 7 a.m. Employees from the Federal Reserve, the courier company and the Texas Department of Transportation removed many checks, though some disappeared. Some unaffiliated people also returned checks to the authorities. A very similar incident happened in August of 2005.

**Information**
**Source:** Dataloss DB

**Idaho State University, Office of Institutional Research**
Pocatello, Idaho

EDU HACK Unknown

Contact: Information Technology Services (208) 282-2872, [http://www.isu.edu/announcement/](http://www.isu.edu/announcement/)

ISU discovered a security breach in a server containing archival information about students, faculty, and staff, including names, Social Security numbers, birth dates, and grades. Anyone who was a student or employee between 1995 and 2005 could be affected.

**Information**
**Source:** Dataloss DB

**Washington State Employment Security Department**
Olympia, Washington

GOV PORT 530

A laptop was stolen from the trunk of an auditor’s car. Names, Social Security numbers and earnings of former employees from 2002 to 2005 were exposed. The Employment Security Department does not have all of the contact information for those affected and used the media to help notify those whose information was compromised. The laptop contained unemployment insurance reports for 49 Seattle businesses that were undergoing routine audits by Employment Security between November 2004 and October 2005.

**Information**
**Source:** Dataloss DB

**Cornell University**
Ithaca, New York

EDU HACK 900

The University discovered a security breach last summer that exposed names, addresses, Social Security numbers, bank names and account numbers.

**Information**
**Source:** Dataloss DB

**First Trust Bank**
Memphis, Tennessee

BSF PORT 100,000

A man claiming to be a janitor bypassed security and stole a laptop from the bank. The laptop contained Social Security numbers and other personal information of current and former customers. Affected customers were contacted and the theft was caught on tape.

**Information**
**Source:** Dataloss DB

**University of San Diego**
San Diego, California

EDU HACK 7,800

Hackers gained access to computers containing personal income tax data, including Social Security numbers, names, and addresses. Faculty members, students and vendors had their information compromised and were notified by the University.
Two separate departments were breached by hacking within a short period of time. A School of Education computer with the names and Social Security numbers of 772 students registered in online education courses was attacked in late August. A Department of English computer that had the Social Security numbers of 180 faculty, graduate assistant and other teaching staff from the department was also hacked in August. The larger breach appears to be the result of someone attempting to establish an illegal movie sharing system. The smaller breach was a possible attempt to log onto and control one server in order to gain control over servers of other campuses. Those affected received notification and Social Security numbers have been removed from both servers.

A laptop containing names, Social Security numbers, bank account information and other human resources data was stolen. Affected current and former employees were notified.

Students at the Indianapolis and Bloomington campuses may have been affected.

A hacker may have accessed the names, Social Security numbers and grades of students who enrolled in Introduction to Business courses between 2001 and 2005. The computer may have been hacked and installed with malware as early as August. A representative believes the breach occurred because the files were stored on a computer that did not have current anti-virus and system-protection software.

On October 16 of 2005 computers were stolen from campus which contained the names, Social Security numbers, addresses and birth dates of current and prospective students. Notifications were sent to those who were affected.

A hacker compromised a server containing names, Social Security numbers, driver's licenses, state ID numbers, dates of birth, phone numbers, bank names, bank codes, bank account numbers and Scottrade account numbers. Scottrade alerted all affected customers.

On or around June 18, 2005 a laptop computer was stolen with information on parolees. It was unclear from the letter we received whether Social Security numbers were involved.

A desktop containing Social Security numbers and other information was stolen from a regional sales office in California. Affected consumers were notified and offered one year of free credit monitoring services.
Information
Source: Dataloss DB
November 7, 2005  Papa John’s Louisville, Kentucky
BSR  DISC  Unknown

An error made thousands of customer comments and internal corporate emails available to anyone searching the Internet. Customer comments submitted between September 29 and November 7 were viewable and had customer names, addresses, phone numbers and email addresses attached. The company stated that "customer feedback over the last five weeks...could be viewed by a user who would have to enter a very specific, unpublished URL." The system now requires a password.

Information
Source: Dataloss DB
November 5, 2005  Safeway, Hawaii Pleasanton, California
BSR  PORT 1,400 in Hawaii, perhaps more elsewhere

Additional locations: Hawaii (where affected employees work). Laptop was stolen from a private home in California.

A division director’s laptop was stolen. Names and Social Security numbers of some Hawaii workers were compromised by the theft. The theft occurred in August and letters were sent to affected employees in October.

Information
Source: Dataloss DB
November 4, 2005  Keck School of Medicine, University of Southern California (USC) Los Angeles, California
EDU  STAT 50,000

A computer server containing names and Social Security numbers of patients, donors and employees was stolen from a campus computer room.

Information
Source: Security Breach Letter
November 1, 2005  University of Tennessee Medical Center Knoxville, Tennessee
MED  PORT 3,800

A laptop was stolen from the University’s medical billing office. Personal information lost included names, Social Security numbers and birth dates. Affected patients were not informed of the theft for nearly two months.

Information
Source: Dataloss DB
October 29, 2005  University of Tennessee Knoxville, Tennessee
EDU  DISC 1,900

People at any of the University of Tennessee campuses may have been affected.

Nineteen hundred students and employees had their names and Social Security numbers posted on the Internet from spring of 2004 until the discovery in October of 2005. A student searched her name and found it listed with her Social Security number on a UT email discussion group site. Information pertaining to individuals who had either paid or owed small amounts of money to the University was shared among 10 employees and the information technology office. The information was mistakenly coded as public rather than private.

Information
Source: Dataloss DB
October 21, 2005  Wilcox Memorial Hospital Lihue, Hawaii
MED  PORT 130,000

A backup computer data drive containing medical record numbers, addresses, names and Social Security numbers of current and former patients was lost. Letters have been sent to affected patients.

Information
Source: Dataloss DB
October 20, 2005  Monmouth University West Long Branch, New Jersey
EDU  DISC 677

The names and Social Security numbers of 677 students were posted online for over four months. The University corrected the error and notified students after a student notified them of the problem. A glitch seems to have caused the information to be found through a simple Internet search.
October 20, 2005  
**Vermont Technical College**  
Randolph Center, Vermont  
EDU  DISC  Unknown

Names, Social Security numbers, addresses, SAT scores and ethnicity of all students enrolled during 2003 were posted online from January 2004 until the mistake was discovered in October of 2005. Someone accidentally sent the data to a publicly accessible place.

October 15, 2005  
**Montclair State University**  
Montclair, New Jersey  
EDU  DISC  9,100

Names and Social Security numbers of undergraduates were posted online for nearly four months. An undergraduate alerted the University after running a Google.com search of his name. The University warned all students of the problem.

October 12, 2005  
**Ohio State University Medical Center**  
Columbus, Ohio  
MED  DISC  2,800

Appointment information including Social Security numbers, birth dates, addresses, phone numbers, medical record numbers, reasons for appointments, and physicians was exposed online.

October 8, 2005  
**Blockbuster**  
New York, New York  
BSR  PHYS  Unknown

Hundreds of files were dumped in clear garbage bags on the street. Recent membership applications revealed customer names, birth dates, addresses, phone numbers, driver’s license numbers, credit card number, credit card expiration date and signatures. For some strange reason, the applications also included customer Social Security numbers. The files were dumped after the store went out of business.

September 29, 2005  
**University of Georgia**  
Athens, Georgia  
EDU  HACK  1,600

A hacker may have accessed the names and Social Security numbers of at least 1,600 people working for the College of Agricultural and Environmental Sciences. The University is attempting to contact individuals who may have been affected.

September 28, 2005  
**RBC Dain Rauscher**  
Minneapolis, Minnesota  
BSF  INSD  households (100 targeted)

Someone claiming to be a former employee obtained customer names, addresses, tax ID number, birth date and Dain Rauscher account number. The former employee sent letters to over 100 customers and claimed that their personal information had been sold in retaliation against the company.

September 23, 2005  
**Bank of America**  
Charlotte, North Carolina  
BSF  PORT  Not disclosed

A laptop was stolen from a Bank of America service provider. Information such as names, account numbers, routing transit numbers, and credit card numbers were compromised by the theft. An unspecified number of Visa Buxx users were contacted by Bank of America.
An unprotected payroll link exposed personal information for Hunter College Campus Schools. Those affected included 335 Queens College law school students, 265 current workers and 171 former workers at local elementary and high schools. All affected people were contacted.

Information Source: Dataloss DB
September 22, 2005
City University of New York
New York, New York
EDU DISC 771

Taxpayers in Alaska, Arizona, California, Hawaii, Idaho, Montana, Nevada, Ohio, Oregon, Utah, Virginia, Washington and Wyoming may have been affected.

A truck carrying checks with tax information for the self-employed was involved in an accident on the San Mateo Bridge. Wind blew about 30,000 pieces of mail into the bay and beyond. The IRS agreed to waive penalties and interest for anyone whose payment was affected.

Information Source: Dataloss DB
September 19, 2005
Internal Revenue Service (IRS)
San Francisco, California
GOV PHYS 30,000

A tape containing sensitive information was stolen from a Children’s Health Council office. The tape contained names, Social Security numbers, and detailed medical information for around 6,000 current and former clients. Payroll information for 700 current and former employees was also on the tape. The agency alerted those who may be at risk of identity theft.

Information Source: Dataloss DB
September 17, 2005
North Fork Bank (now Capital One Bank)
New York, New York
BSF PORT 9,000

A report containing Social Security numbers and grades of students was accessible online for three years. The University is attempting to contact those affected via letters and emails. A graduate alerted the University to the exposure after running a Google.com search of her name.

Information Source: Dataloss DB
September 13, 2005
Fort Carson
Colorado Springs, Colorado
GOV PORT 9,300

Four computer hard drives were stolen from the Soldier Readiness Processing center during the weekend of August 20. Personnel records with names, Social Security numbers, ages, ranks, jobs, citizenship information and unit affiliations of soldiers, civilian federal employees and contractors who had been processed through the center since January were on the hard drives.

Information Source: Dataloss DB
September 10, 2005
Kent State University
Kent, Ohio
EDU STAT 100,000

Five desktop computers were stolen from the locked offices of two deans. Names, Social Security numbers, and grades were on the computers. The information goes back to 2000 for students and 2002 for instructors. Affected students and professors were alerted by the University.
A compact disk containing personal information, including SSNs, was lost when shipped by private courier.

**Information**  
**Source:** Dataloss DB  
**Records from this breach used in our total:** 165,000

**August 30, 2005**  
**JP Morgan Chase & Co.**  
**Dallas, Texas**  
**BSF PORT Unknown**

A laptop was stolen on August 8th. It contained personal and financial account information of customers. Those affected were contacted.

**Information**  
**Source:** Dataloss DB  
**Records from this breach used in our total:** 0

**August 30, 2005**  
**California State University, Chancellor’s Office**  
**Long Beach, California**  
**EDU HACK 154**

A computer virus attack exposed names and Social Security numbers. Those affected included two financial aid administrators and 152 students enrolled at various Cal State Universities. Those affected were contacted.

**Information**  
**Source:** Dataloss DB  
**Records from this breach used in our total:** 154

**August 30, 2005**  
**Stark State College of Technology**  
**North Canton, Ohio**  
**EDU DISC 7,058**

Students attempting to access their grades, financial aid information and academic standing were able to view the information of other students. Social Security numbers, GPA, and course enrollment were viewable. A glitch is believed to be the source of the problem.

**Information**  
**Source:** Dataloss DB  
**Records from this breach used in our total:** 7,058

**August 29, 2005**  
**Iowa Student Loan**  
**Des Moines, Iowa**  
**BSF PORT Unknown**

A CD-Rom including Social Security numbers, last name and state of residence was lost while in transit from an outside business partner.

**Information**  
**Source:** Security Breach Letter  
**Records from this breach used in our total:** 0

**August 27, 2005**  
**University of Florida, Health Sciences Center, ChartOne**  
**Gainesville, Florida**  
**EDU PORT 3,851**

A contractor's laptop containing patient names, Social Security numbers, dates of birth, and medical record numbers was stolen. A letter was sent to the affected patients.

**Information**  
**Source:** Dataloss DB  
**Records from this breach used in our total:** 3,851

**August 22, 2005**  
**U.S. Air Force**  
**Washington, District Of Columbia**  
**GOV HACK 33,300**

A hacker used a legitimate user ID and password to access career information, birth dates, and Social Security numbers. Those affected were notified several months after the breach was discovered.

**Information**  
**Source:** Dataloss DB  
**Records from this breach used in our total:** 33,300

**August 19, 2005**  
**University of Colorado**  
**Denver, Colorado**  
**EDU HACK 49,000**

A hacker may have gained access to personal information from June of 1999 to May of 2001, and fall of 2003 to summer of 2005. The information included current and former student names, Social Security numbers, addresses and phone numbers. The University contacted individuals who were affected.

**Information**  
**Source:** Dataloss DB  
**Records from this breach used in our total:** 49,000

**August 17, 2005**  
**California State University, Stanislaus**  
**Turlock, California**  
**EDU HACK 900**
The names and Social Security numbers of student workers were exposed during a hacker attack. The student workers were contacted by the University.

**Information**
**Source:** Dataloss DB
**August 12, 2005** **Verizon**
**New York, New York**
**BSR** **DISC** **Unknown**

A website flaw allowed customers to check the account details of other customers if they knew their phone numbers. Users' minutes and cell phone models could be viewed in this manner. This unintentional feature may have gone unnoticed for five years due to a glitch.

**Information**
**Source:** Dataloss DB
**August 10, 2005** **University of North Texas**
**Denton, Texas**
**EDU** **HACK** **39,000**

A server containing housing records, financial aid inquiries, and in some cases credit card numbers was hacked. UNT sent letters to current, former, and prospective students whose information may have been accessed.

**Information**
**Source:** Dataloss DB
**August 9, 2005** **Sonoma State University**
**Rohnert Park, California**
**EDU** **HACK** **61,709**

Hackers broke into a computer system and may have accessed the names and Social Security numbers of people who applied, attended, or worked at the University between 1995 and 2002. University officials attempted to notify those who were affected.

**Information**
**Source:** Dataloss DB
**August 9, 2005** **University of Utah**
**Salt Lake City, Utah**
**EDU** **HACK** **100,000**

A server containing library archival databases was hacked. The server included names and Social Security numbers of former University employees. The University issued a warning that people may try to get personal information by posing as University officials involved in the investigation.

**Information**
**Source:** Dataloss DB
**August 9, 2005** **Federal Reserve Bank of Dallas**
**Dallas, Texas**
**GOV** **PHYS** **Unknown**

A truck driver lost thousands of Federal Reserve Bank checks headed to Houston. It seems that the back door of the truck was not closed when the driver left the loading area. Paid and canceled checks with Social Security numbers, names, addresses and signatures were scattered on the highway between Dallas and Houston. Most of the checks were not recovered.

**Information**
**Source:** Dataloss DB
**August 5, 2005** **Madison Area Technical College**
**Madison, Wisconsin**
**EDU** **PHYS** **100**

A news crew found around 100 applications in a MATC dumpster. The applications showed names, contact information, Social Security numbers, birth dates, academic records and canceled checks. The applications and transcripts go back to at least 2002. The College agreed to lock the dumpster and destroy documents in a trash compactor on a more frequent basis. It did not state that it would begin shredding documents before dumping them.

**Information**
**Source:** Dataloss DB
**August 4, 2005** **Anderson College**
**Anderson, North Carolina**
**EDU** **PHYS** **800**

A bag with student resident hall assignments was found on campus. The paperwork also had the students' Social Security numbers. The documents were destroyed and a new program that will prevent unauthorized faculty and staff from accessing student Social Security numbers was developed.
August 2, 2005  
University of Colorado  
Denver, Colorado  
EDU  
HACK  
36,000

Hackers accessed files containing names, photographs, Social Security numbers, and University meal card information. Around 7,000 staff members, 29,000 current students, and some former students were affected.

July 31, 2005  
California State Polytechnic University (Cal PolyPomona)  
Pomona, California  
EDU  
HACK  
31,077

Hackers gained access to two computers containing names, Social Security numbers and transfer records. Applicants, current students, current and former faculty, and staff were affected.

July 30, 2005  
San Diego County Employees Retirement Association  
San Diego, California  
GOV  
HACK  
33,000

Two computers that contained personal information for current and retired San Diego County employees were hacked. The information included names, addresses, Social Security numbers, and dates of birth. The San Diego Retirement Association mailed warnings to members.

July 30, 2005  
California State University, Dominguez Hills  
Carson, California  
EDU  
HACK  
9,613

Hackers accessed several computers containing personal information such as names and Social Security numbers. The students who were affected were emailed.

July 30, 2005  
Austin Peay State University  
Clarksville, Tennessee  
EDU  
DISC  
1,500

The University removed student Social Security numbers, grade point averages and names that were accidentally posted. A student alerted the University to the problem after searching his name and finding the information on the website. A school employee put the internal documents on the website to email other staff members the information, but forgot to remove the information from the website.

July 21, 2005  
University of Colorado, Boulder  
Boulder, Colorado  
EDU  
HACK  
49,000

Prospective students, current students, staff, faculty and University health care service recipients may have had their data exposed in a campus server breach. The information included names, Social Security numbers, addresses, student ID numbers, birth dates, and lab test information. The University mailed letters and sent emails to the individuals affected.

UPDATE (08/20/2005) The number of students affected was increased from an estimate of 42,000 to 49,000.

July 13, 2005  
Arizona Biodyne  
Phoenix, Arizona  
MED  
PORT  
57,000

Arizona Biodyne is an affiliate of Magellan Health Services and manages behavioral health for Blue Cross of Arizona.

A safe with computer backup tapes containing financial, personal and medical records was stolen from Arizona Biodyne. Policyholders’ addresses, phone numbers, dates of birth and Social Security numbers were among the personal information lost. Partial treatment histories and doctor information for some patients was also lost.
July 12, 2005  University of Southern California (USC)  Los Angeles, California  
EDU  DISC  270,000 possibly accessed, dozens exposed

A reporter contacted USC based on an individual’s claim to be able to access personal information on college applicants online. USC removed the site pending investigation and sent letters to affected individuals.

Information 
Source: Security Breach Letter

July 7, 2005  Michigan State University  East Lansing, Michigan  
EDU  HACK  27,000

Student information was compromised during an attack on the College of Education server. The information included Social Security numbers, names, addresses, student courses, and personal identification numbers. The breach occurred in April and students were emailed in July.

Information 
Source: Dataloss DB

July 6, 2005  City National Bank, Iron Mountain  Los Angeles, California  
BSF  PORT  Unknown

Two tapes containing Social Security numbers, account numbers, and other customer information were lost or stolen during transportation. The tapes have been missing since April. City National Bank notified its customers.

Information 
Source: Dataloss DB

July 1, 2005  University of California San Diego  La Jolla, California  
EDU  HACK  3,300

A University server was hacked in April. The server contained Social Security numbers, driver’s license numbers, and credit card numbers from people who attended or worked at UCSD Extension between the time of the incident and 2000. UCSD contacted those who were affected two months after the incident.

Information 
Source: Dataloss DB

June 30, 2005  Ohio State University Medical Center, MTE Consulting  Columbus, Ohio  
MED  PORT  15,000

A laptop containing patient information was stolen from a financial consultant. MTE Consulting notified OSU medical center a month after the laptop was stolen and OSU sent a brief letter to the affected clients.

Information 
Source: Dataloss DB

June 29, 2005  Bank of America  Charlotte, North Carolina  
BSF  PORT  18,000

A laptop containing the names, Social Security numbers, and addresses of customers was stolen from a consultant’s car.

Information 
Source: Dataloss DB

June 29, 2005  Medica Health Plans  Minnetonka, Minnesota  
MED  INSD  Unknown

It was discovered that two employees had engaged in unauthorized activities for an extended period of time. The computer administrators were fired for sabotaging the company’s computers and downloading data. Sensitive information for 1.2 million Medica members may have been accessed. The former employees prolonged their activities and avoided heavier punishment by hiding and destroying evidence of their activities.

Information 
Source: Dataloss DB

June 28, 2005  Lucas County Children Services  Toledo, Ohio  
GOV  DISC  900

Data from around 500 former and 400 current employees from as far back as 1991 were sent outside the organization via e-mail. The data included names, Social Security numbers, and telephone numbers. Current employees were contacted immediately and letters were sent to former employees.
A laptop being stored in the trunk of a car was stolen in Minneapolis, Minnesota. Two people later reported identity fraud problems.

University officials became aware of an October 26, 2003 hacking incident. The personal information included Social Security numbers and addresses for students, faculty, and staff. The University began contacting those affected in June of 2005.

A password-protected laptop containing former employee names, Social Security numbers, birth dates, and benefits information was stolen from a consultant's car trunk. The consulting company has been identified as Hewitt Associates. Kodak sent letters and offered one-year of credit monitoring services and identity theft insurance covering up to $50,000 in fraud.

CASPIAN, a consumer privacy group, notified CVS of a security hole that allowed people to access information about purchases made by customers who used a CVS Corp. loyalty card. Anyone with someone's card number, zip code and the first three letters of the customer's last name could have a list of recent purchases sent to an email account. The company removed Internet access to the information. Fifty million loyalty cards have been issued.

A former librarian with access to the personal information of students, faculty, staff and patrons was convicted of Social Security fraud. The former librarian used Social Security information to obtain fraudulent loans. The University used Social Security numbers to track who checked out library materials. At the time of the press release it was unclear whether any information had been stolen from the University.

A laptop containing the names, Social Security numbers, and in some cases birthdays of current and former University employees was stolen from a human resources administrator's car.

The motion to dismiss by Savvis: [http://www.box.net/shared/static/180zctq8dz.pdf](http://www.box.net/shared/static/180zctq8dz.pdf)

Over 40 million card accounts were exposed to potential fraud due to a security breach that occurred at a third-party processor of payment card transactions. Of the more than 40 million accounts exposed, information on 68,000 Mastercard accounts, 100,000 Visa accounts and 30,000 accounts from other card brands are known to have been exported by the hackers. The data exported included names, card numbers and card security codes.
UPDATE (2/23/2006) CardSystems agreed to settle Federal Trade Commission charges that it failed to take appropriate security measures to protect sensitive personal information. The company must implement a comprehensive security program and obtain audits every 2 years for 20 years.


UPDATE (5/28/2009) Merrick Bank has launched a multi-million dollar lawsuit against Savvis, accusing the vendor of erroneously telling it that CardSystems Solutions complied with Visa and MasterCard security regulations less than a year before the payment processor’s systems were hacked, compromising up to 40 million credit card accounts. Less than a year later the security breach occurred. Hackers were able to get hold of the data because CardSystems kept unencrypted card information on its servers - in contravention of the regulations for which Savvis certified it.

Information Source:
Dataloss DB

June 10, 2005 Federal Deposit Insurance Corp. (FDIC) Washington, District Of Columbia

Personal information including the names, birthdays, salaries, and Social Security numbers of former Federal Deposit Insurance Corporation employees was stolen. Some of the information was used for fraudulent purposes. Affected employees from as far back as July 2002 were notified.

Information Source:
Dataloss DB

June 6, 2005 Citigroup, UPS New York, New York

Customers are being notified that backup tapes containing their account information were lost or stolen while being shipped by UPS.

Information Source:
Dataloss DB

June 4, 2005 Duke University Medical Center Durham, North Carolina

A hacker broke into the computer system, stealing thousands of passwords and fragments of Social Security numbers. Fourteen thousand affected people were notified, including 10,000 employees of Duke University Medical Center.

Information Source:
Dataloss DB

May 30, 2005 Motorola Schaumburg, Illinois

Two computers were stolen from third party vendor Affiliated Computer Services (ACS). They had security safeguards and contained names and Social Security numbers of Motorola employees. Motorola notified affected staff by email and offered fraud insurance coverage.

Information Source:
Dataloss DB

May 28, 2005 Merlin Information Services Kalispell, Montana

An individual fraudulently obtained personal information about thousands of victims from Merlin Information Services and used that information to commit identity theft by opening up credit card accounts. He posed as a private investigator, thus giving Merlin the impression that he was a legitimate user of their services. He conducted at least 1,873 queries through the Merlin system to obtain information on approximately 5,875 people.

Information Source:
Media

May 27, 2005 Cleveland State University Cleveland, Ohio

A laptop containing personal information from applicants, current students, and former students was stolen from the University’s admissions office. The information included Social Security numbers and addresses from as far back as 2001. Letters were sent to those affected.

UPDATE (12/24/05): CSU found the stolen laptop
May 19, 2005  
**Valdosta State University**  
Valdosta, Georgia

A computer server containing campus ID card information and Social Security numbers was hacked. The cards were designed to be used as debit cards by students and employees.

May 18, 2005  
**Jackson Community College**  
Jackson, Michigan

A hacker may have downloaded the passwords and Social Security numbers of employees and students. The College sent new, high security passwords to students and employees.

May 18, 2005  
**University of Iowa**  
Iowa City, Iowa

A computer containing credit card numbers and campus ID numbers for University Book Store customers was breached by a hacker.

May 16, 2005  
**Westborough Bank**  
Westborough, Massachusetts

A former employee who ran an investment program from 1998 to 2001 may have given Social Security numbers and account information to a convicted felon known for defrauding senior citizens. The bank mailed warning letters.

May 14, 2005  
**Georgia Technology Authority (GTA)**  
Atlanta, Georgia

A former computer programmer for Georgia Technology Authority downloaded state driver's license information which contained names, addresses, driver's license numbers, and in some cases Social Security numbers.

May 12, 2005  
**Hinsdale Central High School**  
Hinsdale, Illinois

Two students were accused of hacking into the School's computer system and stealing student and staff Social Security numbers. The students had the information for months before being caught. Letters were sent to affected families. The Social Security Administration and the Federal Trade Commission were also notified.

May 11, 2005  
**Stanford University**  
Stanford, California

The University's Career Development Center was hacked. This exposed the names, Social Security numbers, and other personal information of users. Names and credit card information for some employers that registered with the site were also in the database.

May 7, 2005  
**Department of Justice**  
Washington, District Of Columbia

The laptop was stolen from Omega World Travel of Fairfax, VA.

A laptop containing password protected names and travel account credit card information was stolen sometime between May 7 and May 9.
Information Source: Dataloss DB
May 5, 2005 Purdue University West Lafayette, Indiana

EDU HACK 11,360

Hackers accessed a program which contained University credit card information and the Social Security numbers of current and former employees. Letters were sent to employees and former employees.

Information Source: Dataloss DB
May 5, 2005 Arbella Mutual Insurance Company Quincy, Massachusetts

BSF DISC Unknown

The Massachusetts Registry of Motor Vehicles was the breached entity.

A customer discovered that he could view the Registry of Motor Vehicles database by visiting a website printed on the bottom of his insurance paperwork. He was able to look up people by name and then obtain their address, date of birth, license number, driving history and even their Social Security number most times. The company corrected the problem quickly. The company believes the error was temporary and that few outsiders were able to access the information.

Information Source: Dataloss DB
May 4, 2005 Colorado Health Department Denver, Colorado

GOV PORT 1,600 (families)

A laptop containing Social Security numbers, medical records, family medical history, and addresses was stolen from an employee's car. The State Health Department is not monitoring the affected group and has only contacted some of the families involved.

Information Source: Dataloss DB

BSO PORT 600,000

Backup tapes containing the personal information of current and former employees from as far back as 1986 was lost or stolen during shipping. An 800 number was set up to answer questions and provide free credit monitoring for one year.


Information Source: Dataloss DB
April 29, 2005 Oklahoma State University Stillwater, Oklahoma

EDU PORT 37,000

A laptop used for student job placement seminars was lost or stolen. It contained the Social Security numbers of current and former students.

Information Source: Dataloss DB
April 28, 2005 Georgia Southern University Stateboro, Georgia

EDU HACK tens of thousands (at least 20,000)

Hackers accessed a University server which contained thousands of credit card and Social Security numbers collected over three years. Students who received bookstore credit through scholarship or financial aid between the fall 2003 and spring of 2005 semesters, and anyone who made credit purchases at campus stores, stadium, or website are at risk. Email alerts were sent to students and alumni.

Information Source: Dataloss DB
April 28, 2005 Wachovia, Bank of America, PNC Financial Services Group and Commerce Bancorp Hackensack, New Jersey

BSF INSD 676,000

Note: location listed is the corporate headquarters of Bank of America, not necessarily where the breach occurred.

Bank employees illegally sold account information to someone posing as a collection agency. Customers affected were notified and received one year of free credit monitoring services.
A hacker may have stolen the credit card information of visitors attending a performing arts venue.Warnings were sent to Wharton visitors who used their credit cards anytime between September of 2003 and the incident.

Two computers used for converting paper medical records into digital files were stolen. One of the computers contained Social Security numbers and medical records for hundreds of patients. Letters were sent to about 16,000 patients.

The compromised information included Social Security numbers and grades from master’s alumni classes 1997 through 2004, job offer information from master’s alumni classes 1995 through 2004, contact information for all alumni, and Social Security numbers and grades from doctoral students enrolled between 1998 and 2004. Between 5,000 and 6,000 of those affected had their credit card information and Social Security numbers compromised. Emails and letters were sent to those who were affected.

A backup tape was lost, stolen, or accidentally destroyed while being shipped. The tape contained account information from clients or former clients between the years of 2001 and 2003. Ameritrade notified the affected clients and offered one free year of credit protection services.

Credit card data was stolen. Individuals holding the HSBC-issued General Motors Mastercard were told their cards should be replaced.

UPDATE (07/10/07): U.S. Secret Service agents found Ralph Polo Lauren customers’ credit card numbers in the hands of Eastern European cyber thieves who created high-quality counterfeit credit cards. Victims are from the U.S., Europe, Asia and Canada, among other places, Several Cuban nationals in Florida were arrested with more than 200,000 credit card account numbers.

A laptop containing the names, Social Security numbers, and medical information of Medi-Cal beneficiaries was stolen from the car trunk of an employee. The Department of Health Services began notifying beneficiaries in late May.

RuffaloCODY is the software management company.

The University’s donor database was breached sometime in late 2004. The database was managed by a software company for nonprofit organizations named RuffaloCODY. Letters were sent to the alumni who may have had their personal information stolen.
A hacker gained access to a server containing the names, credit card information, and billing addresses of 15,000 customers. Letters were mailed to all customers who bought products through the educational website for national parks.

**April 8, 2005**

**Eastern National**  
Ft. Washington, Pennsylvania

A hacker gained access to a server containing the names, credit card information, and billing addresses of 15,000 customers. Letters were mailed to all customers who bought products through the educational website for national parks.

**Information Source:**  
Dataloss DB  
records from this breach used in our total: 15,000

**April 8, 2005**

**San Jose Medical Group**  
San Jose, California

A hacker gained access to a server containing the names, credit card information, and billing addresses of 15,000 customers. Letters were mailed to all customers who bought products through the educational website for national parks.

**UPDATE (10/10/07):** A former branch manager at the San Jose Medical Group has been sentenced to almost two years in prison for stealing medical records for about 187,000 patients. The accused pleaded guilty in May to one count of health care-related theft after he stole computer equipment from his former employer, including a DVD that contained patients’ names, Social Security numbers, medical diagnoses and other information.

**Information Source:**  
Dataloss DB  
records from this breach used in our total: 187,000

**April 6, 2005**

**University of California, San Francisco (UCSF)**  
San Francisco, California

A server in the accounting and personnel departments was hacked. It contained information on 7,000 students, faculty, and staff members. The affected individuals were notified March 23.

**Information Source:**  
Dataloss DB  
records from this breach used in our total: 7,000

**April 5, 2005**

**MCI**  
Colorado Springs, Colorado

A laptop containing names and Social Security numbers of current and former employees was stolen from the car trunk of an MCI financial analyst. An MCI spokesperson stated that MCI would continue its policy of allowing laptops to be taken home by employees and will evaluate new security technologies.

**Information Source:**  
Dataloss DB  
records from this breach used in our total: 16,500

**April 5, 2005**

**University of California, Davis**  
Davis, California

The names and Social Security numbers of students, faculty, visiting speakers and staff may have been compromised when a hacker accessed a main computer.

**Information Source:**  
Dataloss DB  
records from this breach used in our total: 1,100

**March 25, 2005**

**Purdue University**  
West Lafayette, Indiana

Computers in the College of Liberal Arts’ Theater Dept. were hacked, exposing personal information of employees, students, graduates, and business affiliates.

**Information Source:**  
Dataloss DB  
records from this breach used in our total: 0

**March 20, 2005**

**Northwestern University**  
Evanston, Illinois

Hackers gained access to multiple computers and gathered user ID and password information from the University’s network. The personal information for around 500 faculty members, 2000 staff members, and 14,000 alumni was compromised.

**Information Source:**  
Dataloss DB  
records from this breach used in our total: 17,500
March 20, 2005  University of Nevada, Las Vegas  Las Vegas, Nevada  EDU  HACK  5,000

A hacker was caught accessing the University's server and may have gotten information from the Student Exchange and Visitor Information System (SEVIS).

Information Source: Dataloss DB  records from this breach used in our total: 5,000

March 16, 2005  California State University, Chico  Chico, California  EDU  HACK  59,000

A university housing and food service computer server containing names and Social Security numbers of faculty, staff, students, former students, and prospective students was hacked.

Information Source: Dataloss DB  records from this breach used in our total: 59,000

March 12, 2005  Las Vegas Department of Motor Vehicles (LV DMV)  Las Vegas, Nevada  GOV  STAT  8,900

A computer and holographic laminate materials were stolen from the Donovan office of the DMV in North Las Vegas.

UPDATE. The equipment was recovered on June 1.

Information Source: Dataloss DB  records from this breach used in our total: 8,900

March 11, 2005  University of California, Berkeley  Berkeley, California  EDU  PORT  98,400

A laptop containing the Social Security numbers of doctoral degree recipients from 1976 to 1999, graduate students enrolled between 1989 and 2003, and graduate school applicants between fall 2001 and spring of 2004 was stolen. Birth dates and addresses for about one-third of the affected people were also on the laptop.

Information Source: Dataloss DB  records from this breach used in our total: 98,369

March 11, 2005  Kaiser Permanente  Oakland, California  MED  DISC  140

A disgruntled employee posted information on her blog noting that Kaiser Permanente included private patient information on systems diagrams posted on the Web.

UPDATE (6/21/2005): The California Department of Managed Health Care fined Kaiser $200,000 for exposing the confidential health information.

Information Source: Dataloss DB  records from this breach used in our total: 140

March 11, 2005  Boston College  Boston, Massachusetts  EDU  HACK  120,000

A hacker gained access to a phone banking database that included alumni addresses and Social Security numbers.

Information Source: Dataloss DB  records from this breach used in our total: 120,000

March 10, 2005  LexisNexis  Dayton, Ohio  BSO  INSD  310000

Unauthorized individuals used IDs and passwords of legitimate customers to obtain consumers’ Social Security numbers, driver’s license numbers, and names and addresses. Most of the breaches were at the company’s subsidiary Seisint Inc., based in Florida.

UPDATE (4/12/05) An internal investigation at LexisNexis has uncovered evidence that an additional 280,000 records may have been involved in this breach, increasing the total from 30,000 to 310,000.

UPDATE (06/30/06): Five men were arrested in connection with this breach.

Information Source: Dataloss DB  records from this breach used in our total: 310,000

March 8, 2005  DSW Shoe Warehouse, Retail Ventures  Columbus, Ohio  BSR  HACK  1,400,000

799
Credit card information from customers in 25 states was compromised.

**UPDATE** (04/19/2005): An additional 1,300,000 customers were added to the initial estimate of 100,000.

**UPDATE** (08/23/2012): DSW was locked in a dispute with National Union over insurance coverage. A federal appellate court ruled that DSW was entitled to insurance coverage of more than $6.8 million in stipulated losses and prejudgment interest.

**Information Source:** Dataloss DB

**February 25, 2005**

**Bank of America Corp.**
**Charlotte, North Carolina**

Computer tapes with credit card information, Social Security numbers, addresses and account numbers were lost. Bank of America began monitoring the customer accounts on the lost tapes and said it would contact cardholders if unusual activity was detected. Around 900,000 of the account holders affected were Defense Department employees.

**Information Source:** Dataloss DB

**February 25, 2005**

**PayMaxx**
**Miramar, Florida**

A software glitch at PayMaxx Inc., a Franklin, Tenn., payroll processing company, accidentally revealed personal financial information on as many as 100,000 individuals, including Social Security numbers. The problem arose in a PayMaxx feature that enabled employees to use the Internet to get their W-2 forms, the standard tax information form issued by companies to their employees.

**Information Source:** Dataloss DB

**February 18, 2005**

**University of Chicago Hospital**
**Chicago, Illinois**

The FBI launched an investigation into possible fraud by at least one hospital employee. As many as 85 patients may have been affected. The hospital contacted all affected patients.

**Information Source:** Dataloss DB

**February 15, 2005**

**ChoicePoint**
**Alpharetta, Georgia**

Fraudsters who presented themselves as legitimate ChoicePoint customers purchased data profiles from ChoicePoint on individuals and used that data to commit identity theft. The initial number of affected records was estimated at 145,000 but was later revised to 163,000.

**UPDATE** (1/26/06): ChoicePoint settled with the Federal Trade Commission for $10 million in civil penalties and $5 million for consumer redress.

**UPDATE** (12/06/06): The FTC announced that victims of identity theft as a result of the data breach who had out-of-pocket expenses can now be reimbursed. The claims deadline is Feb. 4, 2007.

**UPDATE** (06/24/07): Starting Dec. 2006, the FTC began mailing claims forms to victims of the breach. Its Web site provides information about the claims process. Deadline is Aug. 18, 2007. Victims can be reimbursed for out-of-pocket expenses resulting from identity theft connected to the breach. Call (888) 884-8772, or email cpredress@ftc.gov.

**UPDATE** (11/04/07): Since its 2005 data security incident, ChoicePoint has implemented enhancements to its privacy and information security framework including the establishment of an Office of Privacy, Ethics and Compliance to reinforce the responsible use and protection of information at ChoicePoint through policies and procedures, audit and compliance, and outreach and education. Visit www.privacyatchoicepoint.com.

**UPDATE** (1/27/08): Has agreed to pay $10 million to settle a class action lawsuit.

**Information Source:** Security Breach Letter

**February 12, 2005**

**Science Applications International Corp. (SAIC)**
**San Diego, California**

On January 25 thieves broke into a SAIC facility and stole computers containing personal information of past and current employees. Stolen information included names, Social Security numbers, addresses, phone numbers and records of financial transactions.
January 22, 2005  University of Northern Colorado
Greeley, Colorado

A hard drive was lost or stolen. It contained information on current and former University employees and their
beneficiaries and dates back to April of 1997. Names, dates of birth, SSNs, addresses, bank account numbers and routing
numbers may have been accessed.

January 18, 2005  University of California, San Diego
San Diego, California

A hacker breached the security of two University computers that stored the Social Security numbers and names of
students and alumni of UCSD Extension.

January 10, 2005  George Mason University
Fairfax, Virginia

Names, photos, and Social Security numbers of 32,000 students and staff were compromised because of a hacker attack
on the University’s main ID server.
Information Source: Livestream
records from this breach used in our total: 0

Information Source: Alliance Health

Information Source: Thomas Nelson Community College

Information Source: Matson Navigation Company (Horizon Lines)

Information Source: Dungarees

Information Source: CBC Restaurant Corporation (Corner Bakery Cafe)

Information Source: CBC Restaurant Corporation (Corner Bakery Cafe)

Information Source: Sorrento Pacific Financial LLC

Information Source: Word Press

Information Source: Blue Cross Blue Shield of Nebraska

Information Source: W.W Grainger Inc.

Information Source: W.W Grainger Inc.

Information Source: Comcast

Information Source: Comcast

Information Source: Cox Communications

records from this breach used in our total: 0
LoopPay

Humana

PNI Digital Media

United Airlines

ADP, LLC.

Harvard University

Summit Financial Group

Summit Financial Group

Summit Financial Group

Hilton/Hilton Honors Program

Hilton/Hilton Honors Program