Published on *Privacy Rights Clearinghouse* (https://www.privacyrights.org)

How to Reduce Your Risk of Identity Theft [1]

Posted May 01 1995
Revised Dec 05 2017

1. The crime of identity theft

There are two primary types of identity theft:

- "Existing account fraud" or "account takeover fraud" occurs when a thief acquires your credit or debit card information and purchases products and services using either the actual card or the account number and expiration date. Victims may not learn of account takeover until they receive their monthly account statement.
- "New account fraud" or "application fraud" occurs when a thief uses your SSN and other identifying information to open new accounts in your name. Victims are not likely to learn of application fraud for some time, because the monthly account statements are mailed to an address used by the imposter.

This guide discusses strategies for reducing the risk of both types of fraud.

Generally, victims of **credit card** fraud are liable for no more than the first $50 of the loss. In most cases, the victim will not be required to pay any part of the loss. But **debit card** users have less protection against fraud. Not only are individuals' checking accounts wiped out, debit card users could be liable for the total amount of the loss depending on how quickly they report the loss to the financial institution.

Even though victims are usually not saddled with paying their imposters' bills, they are often left with a bad credit report and must spend months and even years regaining their financial health. In the meantime, they have difficulty getting credit, obtaining loans, renting apartments, and even getting hired. Victims of identity theft find little help from the authorities as they attempt to untangle the web of deception that has allowed another person to impersonate them.

Using a variety of methods, criminals steal Social Security numbers (SSNs), driver's licenses, credit and debit card numbers, and other pieces of individuals' identities such as date of birth. They use this information to impersonate their victims, spending as much money as they can in as short a time as possible before moving on to another person's name and identifying information. Identity thieves obtain this information through a variety of means:

- Data breaches [6] in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.
- "Dumpster diving" in trash bins for intact credit card and loan applications and documents containing SSNs.
- Stealing wallets and purses.
- Stealing mail from unlocked mailboxes to obtain newly issued credit cards, bank and credit card statements, pre-approved credit offers, investment reports, insurance statements, benefits documents, or tax information.
- Accessing your credit report fraudulently, for example, by posing as an employer, loan officer, or landlord.
- Obtaining names and SSNs from personnel or customer files in the workplace.

- "Shoulder surfing" at ATM machines in order to capture PIN numbers.
- "Skimming" your credit or debit card information at a point of sale terminal or ATM machine.
- Finding identifying information on Internet sources, via public records sites and fee-based data broker sites.
- Sending email messages that look like they are from your bank, asking you to visit a web site that looks like the bank's in order to confirm account information. This is called "phishing."
- Hacking into unsecured and unencrypted data files of financial institutions, retailers, and credit card transaction processing companies.
- Accessing unsecured web sites that contain sensitive personal information such as Social Security numbers and financial account numbers.

2. Take these steps to reduce your risk of becoming a victim of identity theft:

You cannot prevent identity theft. But you can reduce your risk of fraud by following the tips in this guide.

a. Credit cards, debit cards, and credit reports

1. Reduce the number of credit and debit cards you carry in your wallet. We recommend that you do not use debit cards because of the potential for losses to your checking account. Instead, carry one or two credit cards and your ATM card in your wallet. Nonetheless, debit cards are popular. If you do use them, take advantage of online access to your bank account to monitor account activity frequently. Report evidence of fraud to your financial institution immediately. Learn more about the risks [7] associated with debit cards.

2. When using your credit and debit cards at restaurants and stores, pay close attention to how the magnetic stripe information is swiped by the waiter or clerk. Dishonest employees have been known to use small hand-held devices called skimmers to quickly swipe the card and then later download the account number data onto a personal computer. The thief uses the account data for Internet shopping and/or the creation of counterfeit cards. Likewise, examine point of sale devices and ATM machines for tampering.

3. Do not use debit cards at all when shopping online. Use a credit card because you are better protected in case of fraud. See our online shopping guide [8]. [9]

4. Keep a list or photocopy of all your credit cards, debit cards, bank accounts, and investments -- the account numbers, expiration dates and telephone numbers of the customer service and fraud departments -- in a secure place (not your wallet or purse) so you can quickly contact these companies in case your credit cards have been stolen or accounts are being used fraudulently.

5. Never give out your SSN, credit or debit card number or other personal information over the phone, by mail, or on the Internet unless you have a trusted business relationship with the company and *you* have initiated the call.

6. Always take credit card receipts with you. Never toss them in a public trash container. When shopping, put receipts in your wallet rather than in the shopping bag.

7. Never permit your credit card number to be written onto your checks. It's a violation of California law (Cal. Civ. Code § 1725) and laws in many other states, and puts you at risk for fraud.

8. Watch the mail when you expect a new or reissued credit card to arrive. Contact the issuer if the card does not arrive.

9. Order your credit reports at least once a year. Federal law gives you the right to one free credit report each year from the three credit bureaus: Equifax, Experian, and TransUnion. If you are a victim of identity theft, your credit report will contain the tell-tale signs – inquiries that were not generated by you, as well as credit accounts that you did not open. The earlier you detect fraud, the easier and quicker it will be to clean up your credit files and regain your financial health.

We recommend that you stagger your requests and obtain one report each four months. That way, you can monitor your credit reports on an ongoing basis. But if you are in the market for credit or are a victim of identity theft, order all three at one time. For more information on your free credit reports, visit the Federal Trade Commission website [10].

How to order your free annual credit report:

- By telephone: (877) 322-8228
- Online: www.annualcreditreport.com [11]
- By mail. Print out the order form here [12].

10. Residents of seven states can obtain additional free annual credit reports under state law. These states are: Colorado, Maine, Massachusetts, Maryland, New Jersey, Vermont, and Georgia (two free reports per year in Georgia). If you live in one of these states, be sure to order both your free reports under federal law as well as state law each year – enabling you to even more effectively monitor your credit files on an ongoing basis.

11. Individuals nationwide are able to "freeze" their credit reports with Equifax, Experian, and TransUnion. By freezing your credit reports, you can prevent credit issuers from accessing your credit files except when you give permission. This effectively prevents thieves from opening up new credit card and loan accounts. In most states, security freezes are available at no charge to identity theft victims and for a relatively small fee for non-victims.

- The California Department of Justice's Privacy Enforcement and Protection Unit provides a guide on security freezes for Californians [13]. [13]
- For other states, see Consumer Action's resources [14].
- Brian Krebs' post How I Learned to Stop Worrying and Embrace the Security Freeze [15] is a primer on what you can do to avoid becoming a victim of identity theft

While a security freeze may be the best available deterrent to new account fraud, it may not be the best solution for everyone. It can be cumbersome for individuals who frequently apply for credit, are contemplating a new mortgage, or who plan to change jobs. On the other hand, a security freeze is particularly *well-suited* for seniors who are no longer in the market for new credit. Consumer's Union [16] and Consumer Reports [17] provide more complete discussions of the pros and cons of security freezes. [17]

12. Many companies, including the three credit bureaus, offer credit monitoring services for an annual or monthly fee. They will notify you when there is any activity on your credit report, thus alerting you to possible fraud.

We do not endorse credit monitoring services because we believe that individuals should not have to pay a fee to track their credit. If you decide to subscribe, be sure to choose a service that monitors *all three* credit reports on an *ongoing* basis. You can create your own credit monitoring strategy at no cost by ordering one of your free credit reports each four months. For more information, read PRC's guide Identity Theft Monitoring Services [18].

13. There are many identity theft insurance products available to consumers. We do not recommend them unless they are available as a free or low-cost rider on an existing insurance policy.

b. Passwords and PINS

1. When creating passwords and PINs (personal identification numbers), do not use the last four digits of your Social Security number, mother's mother's maiden name, your birth date, middle name, pet's name, consecutive numbers or anything else that could easily be discovered by thieves. It's It's best to create passwords that combine upper and lower case letters, special characters and numbers.

2. Ask your financial institutions to add extra security protection to your account. Many will allow you to use an additional code or password (a number or word) when accessing your account. Do not use your mother's maiden name, SSN, or date or birth, as these are easily obtained by identity thieves. If asked to create a reminder question, do not use one that is easily answered by others.

3. Memorize all your passwords. Don't record them on anything in your wallet.

4. Shield your hand when using a bank ATM machine or retail point of sale terminal. "Shoulder surfers" may be nearby or a pinhole video camera could be recording your keystrokes.

c. Social Security numbers

1. Protect your Social Security number (SSN). Release it only when absolutely necessary (like tax forms, employment records, most banking, stock and property transactions). The SSN is the key to your credit and banking accounts and is the prime target of criminals.

If a business requests your SSN, ask if it has an alternative number that can be used instead. Speak to a manager or supervisor if your request is not honored. Ask to see the company's written policy on SSNs. If necessary, take your business elsewhere. If the SSN is requested by a government agency, look for the Privacy Act notice. This will tell you if your SSN is required, what will be done with it, and what happens if you refuse to provide it. If your state uses your SSN as your driver's license number, ask to substitute another number.

If possible, do not provide the SSN on job applications. Offer to provide it when you are interviewed or when a background check is conducted. Read PRC's guide My Social Security Number - How Secure Is It? [19]

2. Do not have your SSN or driver's license number printed on your checks. Don't let merchants write your SSN onto your checks because of the risk of fraud.

3. Do not say your SSN out loud when you are in a public place. And do not let merchants, health care providers, or others say your SSN out loud. Whisper or write it down on a piece of paper instead. Be sure to retrieve and shred that paper.

4. Do not carry your SSN card in your wallet except for situations when it is required, the first day on the job, for example. If possible, do not carry wallet cards that display the SSN, such as insurance cards, except when needed to receive healthcare services. A California law places restrictions on the display and transmission of SSNs by companies. For more information, read the California Department of Justice's Privacy Enforcement and Protection Unit guide on SSN "recommended practices [20]." [20]

If you feel you must carry your health insurance or Medicare card with you at all times, try this. Photocopy the card and cut it down to wallet size. Then remove or cut out the last four digits of the SSN. Carry that with you rather than the actual card. But be sure to carry your original Medicare card with you the *first time* you visit your healthcare provider. They are likely to want to make a photocopy of it for their files.

5. It is a violation of federal law for state motor vehicles departments to use the Social Security number as the driver's license (DL) number. (Intelligence Reform and Terrorism Prevention Act of 2004, implemented December 17, 2005) If you are carrying an older driver's license containing your SSN that is not yet ready for renewal, contact the motor vehicles agency in your state and request to have your DL replaced before the actual renewal date. This way, you are not carrying a document in your wallet that contains your SSN.

d. Internet and computer safeguards

1. Install a firewall on your home computer to prevent hackers from obtaining personal identifying and financial data from your hard drive. PRC's guide to securing your computer [21]contains more information.

2. Install and update virus and malware protection software to prevent a worm or virus from causing your computer to send out files or other stored information. PRC's guide to securing your computer [21]contains more information.

3. Password-protect files that contain sensitive personal data, such as financial account information. Create passwords that combine numbers, special characters and letters, upper and lower case. In addition, encrypt sensitive files.

4. When shopping online, do business with companies that provide transaction security protection, and that have strong privacy and security policies. For more online shopping tips, read PRC's guide to online shopping [22].

5. Before disposing of your computer, remove data by using a strong "wipe" utility program. Do not rely on the "delete" function to remove files containing sensitive information. Read more about this in PRC's guide to securing your computer [23]. [24]

6. Never respond to "phishing" email messages. These may appear to be from your bank, eBay, or PayPal. They instruct you to visit their web site, which looks just like the real thing. There, you are told to confirm your account information, provide your SSN, date of birth and other personal information. Legitimate financial companies never email their customers with such requests. These messages are the work of fraudsters attempting to obtain personal information in order to commit identity theft.

7. Be aware that file-sharing and file-swapping programs expose your computer to illegitimate access by hackers and fraudsters. If you use such programs, make sure you comply with the law and know what you are doing. Install and update strong firewall and virus protection.

Many file-sharing programs are downloaded by children without the knowledge of their parents. There are software programs available that identify file sharing software and locate shared files on home computers.

e. Reducing access to your personal data

1. To minimize the amount of information a thief can steal, do not carry extra credit cards, debit cards, your Social Security card, birth certificate or passport in your wallet or purse, except when needed. At work, store your wallet in a safe place.

2. If possible, do *not* carry other cards in your wallet that contain the Social Security number (SSN), including your *Medicare card*, except on days when you need them.

3. To reduce the amount of personal information that is "out there," take these steps:

- Remove your name from the marketing lists of the three credit reporting bureaus -- Equifax, Experian, and TransUnion. Call 888-5OPTOUT or go online to www.optoutprescreen.com [25]. This will limit the number of pre-approved offers of credit that you receive. These, when tossed into the garbage, are a potential target of identity thieves who use them to order credit cards in your name.
- Sign up for the Federal Trade Commission's National Do Not Call Registry [26]. You may also need to register for your state's "do not call" list, if it has one.
- Sign up for the Direct Marketing Association's Mail Preference Service [27]. Your name is added to name deletion lists used by nationwide marketers.
- Have your name and address removed from the phone book and reverse directories.

4. Install a locked mailbox at your residence to deter mail theft. Or use a post office box or a commercial mailbox service. When you are away from home for an extended time, have your mail held at the Post Office, or ask a trusted neighbor to pick it up.

5. When ordering new checks, pick them up at the bank. Don't have them mailed to your home.

6. When you pay bills by mail, do not leave the envelopes containing your checks at your mailbox for the postal carrier to pick up, or in open boxes at the receptionist's desk in your workplace. If stolen, your checks can be altered and then cashed by the imposter. It is best to mail bills and other sensitive items at the drop boxes *inside* the post office rather than neighborhood drop boxes. If you use a neighborhood drop box, always deposit the mail *before* the last pick-up of the day.

f. Responsible information handling

1. Each month, carefully review your credit card, bank and phone statements, including cellular phone bills, for unauthorized use.

2. Convert as much bill-paying as you can to electronic payments by using the Internet for banking and paying bills. With fewer account statements and bills mailed to your home, you will reduce the risk of mail theft and identity theft.

3. Do not toss pre-approved credit offers in your trash or recycling bin without first tearing them into very small pieces or shredding them with a cross-cut shredder. They can be used by "dumpster divers" to order credit cards in your name and mail them to their address. Do the same with other sensitive information like credit card receipts, phone bills, bank account statements, investment account reports, and so on.

4. Use a gel pen for writing checks. Experts say that gel ink contains tiny particles of color that are trapped in the paper, making check washing more difficult .

5. Demand that financial institutions adequately safeguard your data. Discourage your bank from using the last four digits of the SSN as the PIN number they assign to customers. If you have been given the last four SSN digits as a default PIN, change it to something else.

6. When you fill out loan or credit applications, find out how the company disposes of them. If you are not convinced that they store them in locked files and/or shred them, take your business elsewhere. Some auto dealerships, department stores, car rental agencies, and video stores have been known to be careless with customer applications.

7. Store checks in a safe place. In the wrong hands, they could reveal a lot of information about you, including the account number, your phone number and driver's license number.

8. Store personal information securely in your home, especially if you have roommates, employ outside help, or have service work done in your home. Use a locking file cabinet or safe.

9. Any entity that handles personal information should train all its employees, from top to bottom, on responsible information-handling practices. Persuade the companies, government agencies, and nonprofit agencies with which you are associated to adopt privacy policies and conduct privacy training.

10. If your wallet or your Social Security number has been lost or stolen, place fraud alerts on your three credit reports right away. When you request a fraud alert from one bureau, it will notify the other two for you. Your credit file will be flagged with

a statement that says you may be a victim of fraud and that creditors should take additional steps to verify your identity before extending credit. The Fair Credit Reporting Act (FCRA) enables you to place an initial fraud alert for 90 days. The fraud alert may be renewed on the 91st day for another 90 days. You can continue to renew a fraud alert indefinitely. You may cancel the fraud alerts at any time.

- Equifax fraud alert [28] and fraud department (888) 766-0008
- Experian fraud alert [29] and fraud department (888) EXPERIAN (888-397-3742)
- TransUnion fraud alert [30] and fraud department (800) 680-7289

3. Resources

Credit Reporting Agencies

- Equifax
  (888) 766-0008
  http://www.equifax.com [31]
- Experian
  (888) EXPERIAN (397-3742)
  http://www.experian.com [32]
- TransUnion
  (800) 680-7289
  http://www.transunion.com [33]

Federal Trade Commission

- Phone: (877) IDTHEFT (877-438-4338)
- FTC's comprehensive identity theft guide "Taking Charge: What To Do if Your Identity is Stolen [34]." [35]
- FTC's interactive identity theft guide [36].

Identity Theft Resource Center

- Phone: (888) 400-5530
- Web: http://www.idtheftcenter.org [37]

Additional resources:

- FBI Internet Fraud Complaint Center. Report cases involving online fraud and phishing. www.ic3.gov [38]
- For tips on online safety, visit www.onguardonline.gov [39]
- The President's Identity Theft Task Force, www.idtheft.gov/ [40]

Source URL (modified on December 5, 2017): https://www.privacyrights.org/consumer-guides/how-reduce-your-risk-identity-theft

Links
[1] https://www.privacyrights.org/consumer-guides/how-reduce-your-risk-identity-theft
[2] https://www.privacyrights.org/#steps-reduce-victim-id-theft
[3] https://www.privacyrights.org/#passwords-pins
[4] https://www.privacyrights.org/#social-security-numbers
[5] https://www.privacyrights.org/#internet-computer-safeguards
[6] https://www.privacyrights.org/consumer-guides/what-do-when-you-receive-data-breach-notice
[7] https://www.privacyrights.org/consumer-guides/paper-or-plastic-what-have-you-got-lose#2
[8] https://www.privacyrights.org/online-shopping-tips-e-commerce-and-you
[9] https://www.privacyrights.org/node/1321
[10] https://www.consumer.ftc.gov/articles/0155-free-credit-reports
[11] http://www.annualcreditreport.com/
[12] http://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf
[13] http://www.oag.ca.gov/idtheft/facts/freeze-your-credit
[14] http://www.consumer-action.org/english/articles/freeze_your_credit_file#Topic_04
[15] http://krebsonsecurity.com/2015/06/how-i-learned-to-stop-worrying-and-embrace-the-security-freeze/
[16] http://www.consumersunion.org/pdf/SecurityFreeze-Consider.pdf

[17] http://www.consumerreports.org/cro/news/2014/02/should-you-put-a-security-freeze-on-the-credit-file/index.htm
[18] https://www.privacyrights.org/consumer-guides/identity-theft-monitoring-services
[19] https://www.privacyrights.org/consumer-guides/my-social-security-number-how-secure-it
[20] http://www.oag.ca.gov/sites/all/files/pdfs/privacy/protecting_ssns.pdf?
[21] https://www.privacyrights.org/fs/fs36-securing-computer-privacy.htm#firewall
[22] https://www.privacyrights.org/fs/fs23-shopping.htm
[23] https://www.privacyrights.org/%20https%3A//www.privacyrights.org/fs/fs36-securing-computer-privacy.htm#disposal
[24] https://www.privacyrights.org/fs/fs36-securing-computer-privacy.htm#disposal
[25] http://www.optoutprescreen.com/
[26] http://www.donotcall.gov
[27] https://dmachoice.thedma.org/register.php
[28] https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp
[29] https://www.experian.com/fraud/center.html
[30] https://www.transunion.com/fraud-victim-resource/place-fraud-alert
[31] http://www.equifax.com/home/
[32] http://www.experian.com
[33] http://www.transunion.com
[34] https://www.privacyrights.org/%20http%3A//www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf
[35] http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf
[36] https://www.identitytheft.gov/
[37] http://www.idtheftcenter.org/
[38] http://www.ic3.gov
[39] http://www.onguardonline.gov/
[40] http://www.idtheft.gov/