Identity Theft: What to Do if It Happens to You [1]

Posted Jan 01 1997
Revised Sep 21 2018

1. Introduction
2. Contact Credit Bureaus
3. Monitor Your Credit Reports
4. Security Freeze
5. Child Identity Theft
6. FTC Identity Theft Report
7. Law Enforcement
8. New Credit Accounts
9. Existing Credit Accounts
10. Debt Collectors
11. Check and Banking Fraud
12. ATM and Debit Cards
13. Brokerage Accounts
14. U.S. Mail Fraud
15. Social Security Number (SSN) Misuse
16. Internal Revenue Service
17. Passports
18. Mobile Phone Service
19. Student Loans
20. Driver's License
21. Identity Theft Involving Someone You Know
22. Medical Identity Theft
23. False Civil and Criminal Judgments
24. Legal Help
25. Resources

1. Introduction

Identity theft happens when someone misuses information about you without your permission.

- An identity theft victim is a person whose personal information not only has been exposed, but also has been misused.
- If you are a victim of a data breach, you are at greater risk of identity theft, but until your information is misused, you are not considered an identity theft victim.

This guide provides information for victims of identity theft including instructions on how to regain your financial health and who to contact for more help. If you have been notified of a data breach involving your personal information, please see our Consumer Guides What to Do When You Receive a Data Breach Notice [2] and How to Reduce Your Risk of Identity Theft [3]. You may also be interested in our Consumer Guide on Identity Theft Monitoring Services [4].

There are two types of financial 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, a counterfeit card, or the account number and expiration date. Victims may not learn of account takeover until they receive their monthly account statement or check their account online.

- "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 likely mailed to an address used by the imposter.

This guide provides tips and resources about of both types of financial identity theft.

The Federal Trade Commission (FTC) offers a comprehensive one-stop resource [5] for identity theft victims. Their site provides streamlined checklists and sample letters to guide you through the recovery process. It also enables you to create a personal recovery plan.

2. Contact Credit Bureaus

If your Social Security number (SSN) has been compromised, or if you learn you are a victim of new account fraud, immediately place a fraud alert with any one of the three national credit bureaus -- Experian, Equifax, and TransUnion. When you place a fraud alert at any one credit bureau, it will notify the other two for you. A fraud alert can make it harder for an identity thief to open more accounts in your name. When you have a fraud alert, your credit report will be flagged. The fraud alert notifies credit card issuers to verify your identity before issuing credit. The easiest method is to do so online, using one of the links below:

Equifax [6]
P.O. Box 740250, Atlanta, GA 30374- 0241
(800) 525-6285

Experian [7]
PO Box 2002
Allen TX, 75013
(888) 397-3742

TransUnion [8]
P.O. Box 6790, Fullerton, CA 92834-6790.
(800) 680-7289

You can place an initial fraud alert for one year. The credit bureaus will send you a notice of your rights as an identity theft victim. When you receive them, contact each of the three credit bureaus immediately to request two things:

- a free copy of your credit report
- an extension of the fraud alert to seven years.

You must have evidence of attempts to open fraudulent accounts and an identity theft report (police report) to establish the seven-year alert. You may cancel the fraud alerts at any time.

Once you have received your three credit reports, examine each one carefully. Report fraudulent accounts and erroneous information to both the credit bureaus and the credit issuers following the instructions provided with the credit reports. The FTC's *Taking Charge* identity theft guide [9] provides a sample letter to send to the credit bureaus requesting that fraudulent accounts be blocked.

Once you notify the credit bureaus about the fraudulent accounts, they are required to block that information from future reports. The bureaus must also notify the credit grantor of the fraudulent account. Ask the credit bureaus for names and phone numbers of credit grantors with whom fraudulent accounts have been opened if this information is not included on the credit report.

In addition, instruct the credit bureaus in writing to remove *inquiries* that have been generated due to the fraudulent access. You may also ask the credit bureaus to notify those who have received your credit report in the last six months to alert them to the disputed and erroneous information (two years for employers). Under California law, when you provide a copy of the police report to the credit bureaus, they must remove the fraudulent accounts from your credit report. (Cal. Civ. Code § 1785.16(k))

3. Monitor Your Credit Reports

Be aware that fraud alerts may not entirely prevent new fraudulent accounts from being opened by the imposter. Credit issuers do

not always pay attention to fraud alerts, even though the law requires it. That is why we recommend that you check your credit reports again in a few months.

Federal law enables you to receive a free credit report [10] once a year from each of the three credit bureaus. This is over and above the free reports you can order when you place fraud alerts on your three credit reports. Once you have received your free credit reports as a part of the fraud alert process, follow up in a few months by taking advantage of your free copy.

Laws in several states give individuals additional opportunities to obtain free credit reports. For confirmed identity theft victims who live in California, you can get one free report each month for the first 12 months upon request. (Cal. Civ. Code § 1785.15.3) And in seven states, whether a victim or not, you can receive one free credit report each year under state law, over and above the free report you can receive yearly under federal law. These states are: Colorado, Georgia (2 per year), Maine, Maryland, Massachusetts, New Jersey, and Vermont.

4. Security Freeze

Consumers can place a security freeze on their credit files at the credit reporting agencies (Equifax, Experian, and TransUnion) at no cost. With a freeze in place, you can prevent *new creditors* (such as a credit card company or lender) from seeing your credit reports. The freeze prevents fraudulent new accounts because new creditors are not able to check your credit report. Requests for access to your credit file will be denied. Most creditors will not issue new credit if they cannot see the consumer's credit report.

You must separately request a freeze from *each* of the three major credit reporting agencies in order to be fully effective. The websites of each of the credit reporting agencies provide instructions for placing a security freeze:

- Equifax [11]
- Experian [12]
- TransUnion [13]

If you want to apply for new credit, you can remove a security freeze temporarily. You can also permanently remove a freeze.

A security freeze does not apply to credit checks for:

- Employment or background screening purposes
- Tenant screening
- Insurance underwriting
- Identity verification purposes

Security freezes will not impact your credit score or your relationship with your *existing creditors*. Any existing creditor can continue to see your credit reports in order to periodically review your account.

A security freeze cannot stop misuse of your existing bank or credit accounts. You still must check your accounts for any errors or fraudulent activity.

Security freezes should not be confused with credit locks. Credit bureaus often encourage consumers to use a credit lock rather than a security freeze. While a security freeze provides protection that is governed by law, locks are governed by your contractual agreement [14] for each credit bureau. Having a contractual agreement is not as good as having protections under law. For example, the contract may include provisions that you may be better off not agreeing to, such as an arbitration agreement.

5. Child Identity Theft

Children can become victims of identity theft without their parents even knowing about it. The perpetrator may be a relative of the child, particularly a relative with bad credit. In some cases, the child and parents may not become aware of the identity theft until years after it occurs. Therefore, the crime of child identity theft may be vastly underreported.

A key sign of identity theft in children is receiving age-inappropriate mail, such as a credit card application or a bill. If you want to find out if someone has used your child's identity to obtain credit, you should contact the three nationwide credit bureaus and ask them to check if your child has a file. Ask them to search using your child's name and Social Security number. Normally, a child would not have a file at a credit bureau unless the child is a victim of identity theft. The Identity Theft Resource Center describes the special procedures [15] required to check if your child has a credit file.

Child identity theft can be very difficult to resolve. If your child has become a victim, it's best to seek the assistance of an organization that has experience in resolving this issue. The Identity Theft Resource Center [16] offers an extensive Fact Sheet

[17] with tips and resources for resolving child identity theft.

6. FTC Identity Theft Report

Report the crime to the FTC at IdentityTheft.gov [18]. Although the FTC does not itself investigate identity theft cases, they share such information with investigators nationwide who are fighting identity theft. Based on the information you enter, the FTC complaint system will create your Identity Theft Report. Print and save your FTC Identity Theft Report.

7. Law Enforcement

When you report identity theft using IdentityTheft.gov [18], you'll answer some questions about what happened. IdentityTheft.gov then creates an "Identity Theft Report," which is your official statement about the crime. In most cases, you can use your Identity Theft Report in place of a police report to clear your account and credit records of transactions that resulted from the identity theft.

You can also report the crime to your local police or sheriff's department. You might also want to report it to police department(s) where the crime occurred if it's somewhere other than where you live. Tell the police someone stole your identity and you need to file a report. Bring your FTC Identity Theft Report with you. If they are reluctant to take a report, show them the FTC's Memo to Law Enforcement [19]. *Get a copy of the report.* Keep the phone number of your investigator handy and give it to creditors and others who require verification of your case.

FTC regulations define an "identity theft report" to include a report made to a *local, state, or federal* law enforcement agency. If your local police department refuses to file a report and your situation involves fraudulent use of the U.S. mail, you can obtain an identity theft report from the U.S. Postal Inspector. If your case involves fraudulent use of a driver's license in your name, you might be able to obtain a report from your state's Department of Motor Vehicles.

8. New Credit Accounts

If your credit report shows that the imposter has opened new accounts in your name, contact those creditors immediately by telephone and in writing. Creditors will likely ask you to fill out fraud affidavits. The FTC provides a uniform affidavit form [20] that most creditors accept.

Ask the credit grantors in writing to furnish you and your investigating law enforcement agency with copies of the documentation, such as the fraudulent application and transaction records. Both federal and California law give you the right to obtain these documents. (FCRA § 609(e), and Cal. Penal Code § 530.8). The California Attorney General Privacy Enforcement and Protection Unit provides instructions and sample letters [21] on how to obtain documentation from credit grantors.

A victim of identity theft must provide a copy of the FTC affidavit or another affidavit acceptable to the company, plus government-issued identification, and a copy of an "identity theft report" (police report) in order to obtain the documents created by the imposter. The business must provide copies of these records to the victim within 30 days of the victim's request at no charge. The law also allows the victim to authorize a law enforcement investigator to get access to these records.

When you have resolved the fraudulent account with the creditor, ask for a letter stating that the company has closed the disputed account and has discharged the debts. Keep this letter in your files. You may need it if the account reappears on your credit report.

9. Existing Credit Accounts

If your existing credit accounts have been used fraudulently, phone the credit card company at the number displayed on the back of the card. Also report it in writing right away. Request replacement cards with new account numbers. You will likely be asked to provide a fraud affidavit or a dispute form. Send the letter to the address given for "billing inquiries," *not* the address for sending payments. Carefully monitor your accounts for evidence of new fraudulent activity. Report it immediately. Add secure and unique passwords to all accounts.

10. Debt Collectors

If debt collectors try to get you to pay the unpaid bills on fraudulent accounts, ask for the name of the collection company, the name of the person contacting you, phone number, and address. Tell the collector that you are a victim of fraud and are not responsible for the account. Ask for the name and contact information for the referring credit issuer, the amount of the debt, account number, and dates of the charges. Ask if they need you to complete their fraud affidavit form or whether you can use the FTC fraud affidavit. Follow up by writing to the debt collector explaining your situation. Ask that they confirm in writing that you do not owe the debt and that the account has been closed.

A debt collector must notify the creditor that the debt may be a result of identity theft. (FCRA § 615(g)). For additional information on dealing with debt collectors, read our guide [22].

11. Check and Banking Fraud

If you have had checks stolen or bank accounts set up fraudulently, ask your bank to report it to ChexSystems, a consumer reporting agency that compiles reports on checking accounts.

Your bank should be able to provide you with a fraud affidavit. Put "stop payments" on any outstanding checks that you are unsure about. Close your checking account and other affected accounts and obtain new account numbers.

- ChexSystems Inc., [23] Attn: Consumer Relations, 7805 Hudson Rd., Suite 100, Woodbury, MN 55125.
  (800) 428-9623.
  Place a security alert [24] on your ChexSystems report:

If your own checks are rejected at stores where you shop, contact the check verification company that the merchant uses. You have a right to obtain any reports that these companies compile about you. For ChexSystems and any of the check verification companies that you have had to contact as a result of your identity theft situation, we recommend that you request a copy of your file once a year. Make sure your file has been corrected. If not, you will find it difficult to open new bank accounts and/or write checks. More information is available by reading PRC's guide [25] on these "specialty reports."

12. ATM and Debit Cards

If your ATM or debit card has been stolen or compromised, report it immediately. Contact your bank and fill out a fraud affidavit. Get a new card, account number, and password. Closely monitor your account statements. If someone uses your ATM or debit card before you report it lost or stolen, your liability depends on how quickly you report it. You may be liable if the fraud is not reported immediately. Start with a phone call and immediately follow up in writing.

ATM and debit card transactions are subject to the Electronic Fund Transfer Act (EFTA) (15 U.S.C. § 1693). Even if you are a victim of identity theft, your liability for charges can increase the longer the crime goes unreported. For more on EFTA, see the FTC's guide [26] and its guide [27] on electronic banking.

13. Brokerage Accounts

You do not have the same protections against loss with brokerage accounts as you do with credit and debit card or bank accounts. The Securities Investor Protection Corporatio [28]n restores customer funds only when a brokerage firm fails. If an identity thief or other fraudster targets your brokerage account, refer to your account agreement for information on what to do. Immediately report the incident to the brokerage company and notify the Securities and Exchange Commission [29]. Also notify the Financial Industry Regulatory Association [30]. To protect against fraud, put a password on each of your investment accounts.

14. U.S. Mail Fraud

Notify the local Postal Inspector if you suspect an unauthorized change of your address with the post office or if the U.S mail has been used to commit fraud. Find out where fraudulent credit cards were sent. Notify the local Postmaster to forward all mail in your name to your own address.

Call the U.S. Postal Service at (800) 372-8347 to find the nearest Postal Inspector. File a complaint on its online complaint form [31] or mail your complaint to U.S. Postal Service, Criminal Investigations Service Center, Attn: Mail Fraud, 433 W. Harrison St., Rm. 3255, Chicago, IL 60699-3255.

15. Social Security Number (SSN) Misuse

The Social Security Administration (SSA) does *not* in most cases provide assistance to identity theft victims. But be sure to contact [32] the SSA Inspector General to report Social Security *benefit fraud, employment fraud, or welfare fraud*. As a last resort, you might try to change your number, although *we don't recommend it except for very serious cases*. The SSA will only change the number if you fit their fraud victim criteria. See the Identity Theft Resource Center's Fact Sheet [33] for more information.

If your SSN card has been stolen or lost, order a replacement. Complete the SSA's application [34] online, call the SSA at (800) 772-1213, or visit your local SSA office.

16. Internal Revenue Service

Your SSN can be used fraudulently for tax purposes. Fraudulent tax filing by identity thieves has reached epidemic proportions and is a rapidly growing problem. Identity thieves often use your SSN to file a tax return with the IRS in order to receive a refund. If the tax return is filed before yours, the thief will likely receive the refund. If your SSN has been stolen, it may be used by an imposter to get a job. That person's employer would report income earned to the IRS using your SSN, making it appear that you did not report all of your income on your tax return. The IRS has established the IRS Identity Protection Specialized Unit [35] to assist individuals with such problems. It can be reached at (800) 908-4490.

If you have become a victim of identity theft, you can help protect your tax records from fraudulent activity by filing an IRS Identity Theft Affidavit (Form 14039) [36].

17. Passports

If your passport has been lost or stolen, report it immediately.

- U.S. Dept. of State, Passport Services, Consular Lost/Stolen Passport Section [37]
  1111 19th St., NW, Suite 500, Washington, DC 20036.
  (877) 487-2778
  E-mail: npic@state.gov [38]

18. Mobile Phone Service

Identity thieves often establish fraudulent mobile phone accounts, with monthly bills going unpaid. If the imposter has obtained phone account(s) in your name, contact the phone carrier for information on how to report the situation. Read an FTC blog [39] on phone account hijacking.

19. Student Loans

If an identity thief has obtained a student loan in your name, report it in writing to the school that opened the loan. Request that the account be closed. Also report it to the U.S. Dept. of Education:

U.S. Dept. of Education Inspector General [40]
400 Maryland Ave., SW, Washington, DC 20202-1510
(800) 647-8733

20. Driver's License

You may need to change your driver's license number if someone is using yours as ID on bad checks or for other types of fraud. Contact the Department of Motor Vehicles (DMV) in your state to see if another license was issued in your name. Put a fraud alert on your license if your state's DMV provides a fraud alert process. Go to your local DMV to request a new number. Fill out the DMV's complaint form to begin the investigation process. Send supporting documents with the completed form to the nearest DMV investigation office.

- California DMV fraud unit: Phone: (866) 658-5758. Outside Calif.: (916) 657-2274.
- The California DMV encourages victims to contact them to place "a control" (alert) on their license whenever it is lost or stolen (rather than waiting until they find out it has been misused). It affects only DMV transactions
- DMVs in other states [41] (scroll down).

21. Identity Theft Involving Someone You Know

If a relative's information is being used to perpetrate identity theft, or if you personally know the identity thief, additional information about how to address these situations is available in other fact sheets. Visit the Identity Theft Resource Center website:

- When you know the perpetrator [42] (family member, acquaintance)
- ID theft of the deceased [43]
- Children and ID theft [44]

22. Medical Identity Theft

Medical identity theft occurs when someone uses your name, Social Security number, or other personal information to obtain health care or medical products. Another variation involves false claims for medical care made to your health insurer, again using your personal information. Like other forms of identity theft, victims of medical identity theft may first become aware of a problem

with a call from a debt collector. Medical identity theft can be particularly insidious since remedies involve cleaning up your medical records as well as your credit reports.

For a full discussion of the crime of medical identity theft as well as steps to take if you are a victim, visit the World Privacy Forum's Medical Identity Theft Page. [45] The California Attorney General Privacy Enforcement and Protection Unit has a Consumer Information Sheet titled First Aid for Medical Identity Theft [46] and an October 2013 report titled Medical Identity Theft: Recommendations for the Age of Electronic Medical Records [47].

The Federal Trade Commission has also published medical identity theft guides for consumers and healthcare providers.

- Facts for Consumers [48]
- Business Tips for Dealing with Medical Identity Theft [49]
- FAQ for Health Care Providers and Health Plans [50]

23. False Civil and Criminal Judgments

Sometimes victims of identity theft are wrongfully accused of crimes that were committed by the imposter. If you are wrongfully arrested or prosecuted for criminal charges, contact the police department and the court in the jurisdiction of the arrest. Also contact your state's Department of Justice and the FBI to ask how to clear your name. If a civil judgment is entered in your name for your imposter's actions, contact the court where the judgment was entered and report that you are a victim of identity theft. For more on what to do if you become the victim of criminal identity theft, read the guides provided by the Identity Theft Resource Center [51] and the California Attorney General's [52] Privacy Enforcement and Protection Unit.

24. Legal Help

You may want to consult an attorney to determine legal action to take against creditors, credit bureaus, and/or debt collectors if they are not cooperative in removing fraudulent entries from your credit report or if negligence is a factor. Call the local Bar Association, a Legal Aid office in your area (for low-income households), or the National Association of Consumer Advocates [53] to find an attorney who specializes in consumer law, the Fair Credit Reporting Act, and the Fair Credit Billing Act.

If you are a senior citizen or take care of a dependent adult, be sure to contact an elder law service. Many district attorneys have an elder abuse unit with expertise in financial crimes against seniors.

25. Resources

Federal Trade Commission (FTC)

- Read the FTC's guide, Taking Charge: What to Do if Your Identity is Stolen. [9]
- Visit the FTC's Identity Theft microsite. [54]
- Use the FTC's interactive identity theft guide [5].
- FTC uniform fraud affidavit form [55].
- Identity Theft Hotline: (877) IDTHEFT (877-438-4338)
- FTC Identity Theft Clearinghouse, 600 Pennsylvania Ave. N.W., Washington, DC 20580

Identity Theft Resource Center (ITRC) [56]. The ITRC offers extensive guides and form letters [57] for victims.
(888) 400-5530

California Attorney General Identity Theft Page [58]

U.S. Dept. of Justice [59]. The DOJ prosecutes federal identity theft cases.

FBI Internet Fraud Complaint Center [60]. The Internet Crime Complaint Center (IC3), a partnership between the FBI and the National White Collar Crime Center, allows you to report suspected cases of Internet and e-commerce fraud, including phishing.

Source URL (modified on September 21, 2018): https://www.privacyrights.org/consumer-guides/identity-theft-what-do-if-it-happens-you

Links
[1] https://www.privacyrights.org/consumer-guides/identity-theft-what-do-if-it-happens-you

[2] https://www.privacyrights.org/consumer-guides/what-do-when-you-receive-data-breach-notice
[3] https://www.privacyrights.org/consumer-guides/how-reduce-your-risk-identity-theft
[4] https://www.privacyrights.org/consumer-guides/identity-theft-monitoring-services
[5] https://www.identitytheft.gov/
[6] https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp
[7] http://www.experian.com/fraud
[8] http://www.transunion.com/personal-credit/credit-disputes/fraud-alerts.page
[9] http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf
[10] http://www.consumer.ftc.gov/articles/0155-free-credit-reports
[11] https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
[12] https://www.experian.com/freeze/center.html
[13] https://www.transunion.com/credit-freeze/place-credit-freeze
[14] https://www.consumerreports.org/credit-bureaus/why-credit-freeze-is-better-than-credit-lock/
[15] http://www.idtheftcenter.org/Fact-Sheets/fs-120a.html
[16] http://www.idtheftcenter.org/id-theft/contact-us.html
[17] http://www.idtheftcenter.org/Fact-Sheets/fs-120.html
[18] https://identitytheft.gov/
[19] http://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0088-ftc-memo-law-enforcement.pdf
[20] http://www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf
[21] http://www.oag.ca.gov/idtheft/facts/guide-for-victims
[22] https://www.privacyrights.org/consumer-guides/debt-collection-and-your-rights
[23] https://www.consumerdebit.com/consumerinfo/us/en/index.htm
[24] https://www.consumerdebit.com/consumerinfo/us/en/chexsystems/theftaffidavit/index.htm
[25] https://www.privacyrights.org/consumer-guides/other-consumer-reports-what-you-should-know-about-specialty-reports
[26] http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre04.shtm
[27] http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre14.shtm
[28] http://www.sipc.org
[29] http://www.sec.gov
[30] http://www.finra.org
[31] https://postalinspectors.uspis.gov/forms/MailFraudComplaint.aspx
[32] http://oig.ssa.gov/report-fraud-waste-or-abuse/fraud-waste-and-abuse
[33] http://www.idtheftcenter.org/artman2/publish/v_fact_sheets/Fact_Sheet_113_Social_Security_Number.shtml
[34] https://www.ssa.gov/online/ss-5.pdf
[35] http://www.irs.gov/privacy/article/0,,id=186436,00.html
[36] http://www.irs.gov/file_source/pub/irs-pdf/f14039.pdf
[37] https://travel.state.gov/content/travel/en/passports/after/lost-stolen.html
[38] mailto:npic@state.gov
[39] https://www.ftc.gov/news-events/blogs/techftc/2016/06/your-mobile-phone-account-could-be-hijacked-identity-thief?utm_source=govdelivery
[40] http://www2.ed.gov/about/offices/list/oig/misused/index.html
[41] http://www.usa.gov/Topics/Motor-Vehicles.shtml
[42] http://www.idtheftcenter.org/artman2/publish/v_fact_sheets/Fact_Sheet_115_When_you_personallyknow_the_identity_thief.shtml
[43] http://www.idtheftcenter.org/artman2/publish/c_guide/Fact_Sheet_117_IDENTITY_THEFT_AND_THE_DECEASED_-_PREVENTION_AND_VICTIM_TIPS.shtml
[44] http://www.idtheftcenter.org/artman2/publish/v_fact_sheets/Fact_Sheet_120.shtml
[45] http://worldprivacyforum.org/category/med-id-theft/
[46] http://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/cis_16_med_id_theft.pdf?
[47] http://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/medical_id_theft_recommend.pdf?
[48] https://www.consumer.ftc.gov/articles/0171-medical-identity-theft
[49] http://www.ftc.gov/opa/2011/02/medicalid.shtm
[50] http://business.ftc.gov/documents/bus75-medical-identity-theft-faq-health-care-health-plan
[51] https://www.idtheftcenter.org/Solutions/sn-06.html
[52] https://oag.ca.gov/idtheft/criminal
[53] http://www.consumeradvocates.org/
[54] http://www.ftc.gov/bcp/edu/microsites/idtheft/
[55] https://www.privacyrights.org/www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf
[56] http://www.idtheftcenter.org/

[57] http://www.idtheftcenter.org/Help-for-Victims/document-catalogue.htm
[58] https://www.oag.ca.gov/idtheft
[59] http://www.justice.gov/criminal/fraud/websites/idtheft.html
[60] http://www.ic3.gov/