Identity Theft

This is a series about Identity theft, what it is, how to prevent it and what to do if you become a victim of this crime. This report, compiled by the Federal Trade Commission is available online at:

http://www.consumer.gov/idtheft

Introduction

In the course of a busy day, you may write a check at the grocery store, charge tickets to a ball game, rent a car, mail your tax returns, call home on your cell phone, order new checks or apply for a credit card. Chances are you don't give these everyday transactions a second thought. But someone else may.

The 1990's spawned a new variety of crooks called identity thieves. Their stock in trades are your everyday transactions. Each transaction requires you to share personal information: your bank and credit card account numbers; your income; your Social Security number (SSN); and your name, address and phone numbers. An identity thief co- opts some piece of your personal information and appropriates it without your knowledge to commit fraud or theft. An all- too- common example is when an identity thief uses your personal information to open a credit card account in your name.

Can you completely prevent identity theft from occurring? Probably not, especially if someone is determined to commit the crime. But you can minimize your risk by managing your personal information wisely, cautiously and with heightened sensitivity.

The Congress of the United States asked the Federal Trade Commission to provide information to consumers about identity theft and to take complaints from those whose identities have been stolen. If you've been a victim of identity theft, you can call the FTC's Identity Theft Hotline toll free at 1- 877- IDTHEFT (438- 4338). The FTC puts your information into a secure consumer fraud database and may, in appropriate instances, share it with other law enforcement agencies and private entities, including any companies about which you may complain.

In addition, the FTC has developed the ID Theft Affidavit – a form you can use to alert companies where a new account was opened in your name. A copy of the ID Theft Affidavit is in this booklet. The company can then investigate the fraud and decide the outcome of your claim. You can find a list of some of the companies and organizations that accept or endorse the ID Theft Affidavit at:

http://www.consumer.gov/idtheft

The FTC, working in conjunction with other government agencies, has produced this report to help you guard against and recover from identity theft.

Despite your best efforts to manage the flow of your personal information or to keep it to yourself, skilled identity thieves may use a variety of methods – low- and high tech – to gain access to your data. Here are some of the ways imposters can get your personal information and take over your identity.

How Identity Thieves Get Your Personal Information:

- They steal wallets and purses containing your identification and credit and bankcards.
- They steal your mail, including your bank and credit card statements, pre- approved credit offers, telephone calling cards and tax information.
- They complete a “change of address form” to divert your mail to another location.
- They rummage through your trash, or the trash of businesses, for personal data in a practice known as “dumpster diving.”
- They fraudulently obtain your credit report by posing as a landlord, employer or someone else who may have a legitimate need for – and a legal right to – the information.
- They get your business or personnel records at work.
- They find personal information in your home.
- They use personal information you share on the Internet.
- They buy your personal information from “inside” sources. For example, an identity thief may pay a store employee for information about you that appears on an application for goods, services or credit.
- How identity thieves use your personal information:
- They call your credit card issuer and, pretending to be you, ask to change the mailing address on your credit card account. The imposter then runs up charges on your account. Because your bills are being sent to the new address, it may take some time before you realize there’s a problem.
- They open a new credit card account, using your name, date of birth and SSN. When they use the credit card and don’t pay the bills, the delinquent account is reported on your credit report.
- They establish phone or wireless service in your name.
- They open a bank account in your name and write bad checks on that account.
- They file for bankruptcy under your name to avoid paying debts they’ve incurred under your name, or to avoid eviction.
- They counterfeit checks or debit cards, and drain your bank account.
- They buy cars by taking out auto loans in your name.

Minimizing the Risk

While you probably can’t prevent identity theft entirely, you can minimize your risk. By managing your personal information wisely, cautiously and with an awareness of the issue, you can help guard against identity theft:

- Before you reveal any personally identifying information, find out how it will be used and whether it will be shared with others. Ask if you have a choice about the use of your information: can you choose to have it kept confidential?
- Pay attention to your billing cycles. Follow up with creditors if your bills don’t arrive on time. A missing credit card bill could mean an identity thief has taken over your credit card account and changed your billing address to cover his tracks.
- Guard your mail from theft. Deposit outgoing mail in post office collection boxes or at your local post office. Promptly remove mail from your mailbox after it has been delivered. If you’re planning to be away from home and can’t pick up your mail, call the U. S. Postal Service at 1- 800- 275- 8777 to request a vacation hold. The Postal Service will hold your mail at your local post office until you can pick it up.

- Put passwords on your credit card, bank and phone accounts. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers.

- Minimize the identification information and the number of cards you carry to what you'll actually need.

- Do not give out personal information on the phone, through the mail or over the Internet unless you have initiated the contact or know whom you're dealing with. Identity thieves may pose as representatives of banks, Internet service providers and even government agencies to get you to reveal your SSN, mother's maiden name, financial account numbers and other identifying information. Legitimate organizations with which you do business have the information they need and will not ask you for it.

- Keep items with personal information in a safe place. To thwart an identity thief who may pick through your trash or recycling bins to capture your personal information, tear or shred your charge receipts, copies of credit applications, insurance forms, physician statements, bank checks and statements that you are discarding, expired charge cards and credit offers you get in the mail.

- Be cautious about where you leave personal information in your home, especially if you 4 have roommates, employ outside help or are having service work done in your home.

- Find out who has access to your personal information at work and verify that the records are kept in a secure location.

- Give your SSN only when absolutely necessary. Ask to use other types of identifiers when possible.

- Don't carry your SSN card; leave it in a secure place.

- Order a copy of your credit report from each of the three major credit-reporting agencies every year. Make sure it is accurate and includes only those activities you've authorized. The law allows credit bureaus to charge you up to $9.00 for a copy of your credit report. Your credit report contains information on where you work and live, the credit accounts that have been opened in your name, how you pay your bills and whether you've been sued, arrested or filed for bankruptcy. Checking your report on a regular basis can help you catch mistakes and fraud before they wreak havoc on your personal finances.

Credit Bureaus

Equifax – http://www.equifax.com

To order your report, call: 800- 685- 1111
Or, write: P. O. Box 740241
Atlanta, GA 30374- 0241

To report fraud, call: 800- 525- 6285
TDD: 800- 255- 0056

Experian – http://www.experian.com

To order your report, call: 888- EXPERIAN (397- 3742)
Or, write: P. O. Box 2104
Allen, TX 75013

To report fraud, call: 888- EXPERIAN (397- 3742)/ TDD: 800- 972- 0322

TransUnion – http://www.transunion.com
To order your report, call: 800- 916- 8800
Or, write: P. O. Box 1000
Chester, PA 19022

To report fraud, call: 800- 680- 7289
TDD: 877- 553- 7803 and write:
Fraud Victim Assistance Division
P. O. Box 6790
Fullerton, CA 92634- 6790

Your employer and financial institution will likely need your SSN for wage and tax reporting purposes. Other private businesses may ask you for your SSN to do a credit check, such as when you apply for a car loan. Sometimes, however, they simply want your SSN for general record keeping. You don't have to give a business your SSN just because they ask for it. If someone asks for your SSN, ask the following questions:

- Why do you need my SSN?
- How will my SSN be used?
- What law requires me to give you my SSN?
- What will happen if I don't give you my SSN?

Sometimes a business may not provide you with the service or benefit you're seeking if you don't provide your SSN. Getting answers to these questions will help you decide whether you want to share your SSN with the business. Remember, though, that the decision is yours.

Choosing to Share Your Information – or Not

What happens to the personal information you provide to companies, marketers and government agencies? They may use your information just to process your order. They may use it to create a profile about you and then let you know about products, services or promotions. Or they may share your information with others. More organizations are offering consumers choices about how their personal information is used. For example, many let you "opt out" of having your information shared with others or used for promotional purposes. You can learn more about the choices you have to protect your personal information from credit bureaus, state Departments of Motor Vehicles and direct marketers. Credit Bureaus

Credit Bureaus

Pre-Screened Credit Offers - If you receive pre- screened credit card offers in the mail (namely, those based upon your credit data), but don't tear them up after you decide you don't want to accept the offer, identity thieves may retrieve the offers for their own use without your knowledge.

To opt out of receiving prescreened credit card offers, call: 1- 888- 5- OPTOUT (1- 888- 567- 8688). The three major credit bureaus use the same toll- free number to let consumers choose not to receive pre- screened credit offers.

Marketing Lists - Of the three major credit bureaus, only Experian offers consumers the opportunity to have their names removed from lists that are used for marketing and promotional purposes. To have your name removed from Experian's marketing lists, call 1- 800- 407- 1088.

Departments of Motor Vehicles - Take a look at your driver's license. All the personal information on it - and more - is on file with your state Department of Motor Vehicles (DMV). A state DMV may distribute your personal information for law enforcement, court proceedings and insurance underwriting purposes, but may not distribute it for direct marketing without your express consent. Contact your state DMV for more information.

Direct Marketers - The Direct Marketing Association's (DMA) Mail, E- mail and Telephone Preference Services allow consumers to opt out of direct mail marketing, e- mail marketing and/ or telemarketing solicitations from many national companies. Because your name will not be on their lists, it also means that these companies can't rent or sell your name to other companies.

To remove your name from many national direct mail lists, write:

DMA Mail Preference Service
Preference Service Mgr.
1120 Avenue of the Americas
New York, NY 10036- 6700

To remove your e-mail address from many national direct e- mail lists, visit: http://www.e-mps.org

To avoid unwanted phone calls from many national marketers, send your name, address, and telephone number to:

DMA Telephone Preference Service
Preference Service Mgr.
1120 Avenue of the Americas
New York, NY 10036- 6700

For more information, visit: http://www.the-dma.org

Sometimes an identity thief can strike even if you've been very careful about keeping your personal information to yourself. If you suspect that your personal information has been stolen and misappropriated to commit fraud or theft, take action immediately, and keep a record of your conversations and correspondence. Exactly which steps you should take to protect yourself depends on your circumstances and how your identity has been misused. However, three basic actions are appropriate in almost every case.

Your First Three Steps

First, contact the fraud departments of each of the three major credit bureaus. Tell them that you're an identity theft victim. Request that a "fraud alert" be placed in your file, as well as a victim's statement asking that creditors call you before opening any new accounts or changing your existing accounts. This can help prevent an identity thief from opening additional accounts in your name.

At the same time, order copies of your credit reports from the credit bureaus. Credit bureaus must give you a free copy of your report if your report is inaccurate because of fraud, and you request it in writing. Review your reports carefully to make sure no additional fraudulent accounts have been opened in your name or unauthorized changes made to your existing accounts. Also, check the section of your report that lists "inquiries." Where "inquiries" appear from the company that opened the fraudulent account, request that these "inquiries" be removed from your report. In a few months, order new copies of your reports to verify your corrections and changes, and to make sure no new fraudulent activity has occurred.

Second, contact the creditors for any accounts that have been tampered with or opened fraudulently. Creditors can include credit card companies, phone companies and other utilities, and banks and other lenders. Ask to speak with someone in the security or fraud department of each creditor, and follow up with a letter. It's particularly important to notify credit card companies in writing because that's the consumer protection procedure the law spells out for resolving errors on credit card billing statements.

Immediately close accounts that have been tampered with and open new ones with new Personal Identification Numbers (PINs) and passwords. Here again, avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers.

Third, file a report with your local police or the police in the community where the identity theft took place. Get a copy of the police report in case the bank, Credit Card Company or others need proof of the crime. Even if the police can't catch the identity thief in your case, having a copy of the police report can help you when dealing with creditors.

Your Next Steps

Although there's no question that identity thieves can wreak havoc on your personal finances, there are some things you can do to take control of the situation. For example:

Stolen mail. If an identity thief has stolen your mail to get new credit cards, bank and credit card statements, pre-screened credit offers or tax information, or if an identity thief has falsified change- of- address forms, that's a crime. Report it to your local postal inspector. Contact your local post office for the phone number for the nearest postal inspection service office or check the Postal Service web site at:

http://www.usps.gov/websites/depart/inspect

Change of address on credit card accounts If you discover that an identity thief has changed the billing address on an existing credit card account, close the account. When you open a new account, ask that a password be used before any inquiries or changes can be made on the account. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers. Avoid using the same information and numbers when you create a PIN.

Bank accounts If you have reason to believe that an identity thief has tampered with your bank accounts, checks or ATM card, close the accounts immediately. When you open new accounts, insist on passwordonly access to minimize the chance that an identity thief can violate the accounts. In addition, if your checks have been stolen or misused, stop payment.

You can contact the following major check verification companies to learn more about the services they provide in helping you track your stolen or misused checks:

- SCAN: 1-800-262-7771
- TeleCheck: 1-800-710-9898 or 927-0188
- CrossCheck: 1-707-586-0431
- Equifax Check Systems: 1-800-437-5120
- International Check Services: 1-800-526- 5380

If your ATM card has been lost, stolen or otherwise compromised, cancel the card as soon as you can and get another with a new PIN.

Investments If you believe that an identity thief has tampered with your securities investments or a brokerage account, immediately report it to your broker or account manager and to the Securities and Exchange Commission. You can file a complaint with the SEC by visiting the Complaint Center at:

http://www.sec.gov/complaint.shtml

Be sure to include as much detail as possible. If you do not have access to the Internet, write to the SEC at: SEC Office of Investor Education and Assistance, 450 Fifth Street, NW, Washington, DC 20549- 0213, or call 202- 942- 7040.

Phone service If an identity thief has established new phone service in your name; is making unauthorized calls that seem to come from - and are billed to - your cellular phone; or is using your calling card and PIN, contact your service provider immediately to cancel the account and/ or calling card. Open new accounts and choose new PINs. If you are having trouble getting fraudulent phone charges removed from your account, contact your state Public Utility Commission for local service providers or the Federal Communications Commission for long- distance service providers and cellular providers at:

http://www.fcc.gov/ccb/enforce/complaints.html or

1-888-CALL-FCC

Employment If you believe someone is using your SSN to apply for a job or to work, that's a crime. Report it to the SSA's Fraud Hotline at 1- 800- 269- 0271. Also call SSA at 1- 800- 772- 1213 to verify the accuracy of the earnings reported on your SSN, and to request a copy of your Social Security Statement. Follow up your calls in writing.

Driver's license If you suspect that your name or SSN is being used by an identity thief to get a driver's license or a non-driver's ID card, contact your Department of Motor Vehicles. If your state uses your SSN as your driver's license number, ask to substitute another number.

Bankruptcy If you believe someone has filed for bankruptcy using your name, write to the U. S. Trustee in the Region where the bankruptcy was filed. A listing of the U. S. Trustee Program's Regions can be found at:

http://www.usdoj.gov/ust

or look in the Blue Pages of your phone book under US Government - Bankruptcy Administration. Your letter should describe the situation and provide proof of your identity.

The U. S. Trustee, if appropriate, will make a referral to criminal law enforcement authorities if you provide appropriate documentation to substantiate your claim. You also may want to file a complaint with the US Attorney and/ or the FBI in the city where the bankruptcy was filed.

Criminal records/arrests In rare instances, an identity thief may create a criminal record under your name. For ex ample, your imposter may give your name when being arrested. If this happens to you, you may need to hire an attorney to help resolve the problem. The procedures for clearing your name vary by jurisdiction.

Should I Apply for a New Social Security Number?

Under certain circumstances, SSA may assign you a new SSN - at your request - if, after trying to resolve the problems brought on by identity theft, you continue to experience problems. Consider this option carefully. A new SSN may not resolve your identity theft problems, and may actually create new problems. For example, a new SSN does not necessarily ensure a new credit record because credit bureaus may combine the credit records from your old SSN with those from your new SSN. Even when the old credit information is not associated with your new SSN, the absence of any credit history under your new SSN may make it more difficult for you to get credit. And finally, there's no guarantee that a new SSN wouldn't also be misused by an identity thief.

The FTC collects complaints about identity theft from consumers who have been victimized. Although the FTC does not have the authority to bring criminal cases, the Commission can help victims of identity theft by providing information to assist them in resolving the financial and other problems that can result from this crime. The FTC also refers victim complaints to other appropriate government agencies and private organizations for further action. If you've been a victim of identity theft, file a complaint with the FTC by contacting the FTC's Identity Theft Hotline by telephone:

Toll-free 1-877-IDTHEFT (438- 4338)
TDD: 202-326-2502
Mail: Identity Theft Clearinghouse,
Federal Trade Commission
600 Pennsylvania Avenue, NW,
Washington, DC 20580 Online: http://www.consumer.gov/idtheft

Other agencies and organizations also are working to combat identity theft. If specific institutions and companies are not being responsive to your questions and complaints, you also may want to contact the government agencies with jurisdiction over those companies.

Federal Laws The Federal government and numerous states have passed laws that address the problem of identity theft. The Identity Theft and Assumption Deterrence Act, enacted by Congress in October 1998 (and codified, in part, at 18 U. S. C. §1028) is the federal law directed at identity theft.

Violations of the Act are investigated by federal law enforcement agencies, including the U. S. Secret Service, the FBI, the U. S. Postal Inspection Service and SSA's Office of the Inspector General. Federal identity theft cases are prosecuted by the U. S. Department of Justice. In most instances, a conviction for identity theft carries a maximum penalty of 15 years imprisonment, a fine and forfeiture of any personal property used or intended to be used to commit the crime. The Act also directs the U. S. Sentencing Commission to review and amend the federal sentencing guidelines to provide appropriate penalties for those persons convicted of identity theft.

Schemes to commit identity theft or fraud also may involve violations of other statutes, such as credit card fraud; computer fraud; mail fraud; wire fraud; financial institution fraud; or Social Security fraud. Each of these federal offenses is a felony and carries substantial penalties - in some cases, as high as 30 years in prison, fines and criminal forfeiture.

State Laws Many states have passed laws related to identity theft; others may be considering such legislation. Where specific identity theft laws do not exist, the practices may be prohibited under other laws. Contact your State Attorney General's office or local consumer protection agency to find out whether your state has laws related to identity theft, or visit:

http://www.consumer.gov/idtheft

State laws that had been enacted at the time of this booklet's publication are listed below.

Alabama 2001 Al. Pub. Act 312; 2001 A1. SB 144
Alaska Alaska Stat § 11.46.180
Arizona Ariz. Rev. Stat. § 13- 2008
Arkansas Ark. Code Ann. § 5- 37- 227
California Cal. Penal Code §§ 530.5- 530.7
Colorado Colo. Rev Stat. § 18- 5- 102
Connecticut 1999 Gen. Stat. § 53(a)- 129(a)
Delaware Del. Code Ann. tit. II, § 854
Florida Fla. Stat. Ann. § 817.568
Georgia Ga. Code Ann. §§ 16- 9- 121, 16- 9- 127
Hawaii Haw. Rev. Stat. § 708- 810z
Idaho Idaho Code § 18- 3126
Illinois 720 III. Comp. Stat. 5/ 16 G
Indiana Ind. Code Ann. § 35- 43- 5- 4 (2000)
Iowa Iowa Code § 715A. 8
Kansas Kan. Stat. Ann. § 21- 4018
Kentucky Ky. Rev. Stat. Ann. § 514.160
Louisiana La. Rev. Stat. Ann. § 14: 67.16
Maine Me. Rev. Stat. Ann. tit. 17- A, § 354- 2A
Maryland Md. Code Ann. art. 27 § 231
Massachusetts Mass. Gen. Laws ch. 266, § 37E
Michigan Mich. Comp. Laws § 750.285
Minnesota Minn. Stat. Ann. § 609.527
Mississippi Miss. Code Ann. § 97- 19- 85
Missouri Mo. Rev. Stat. § 570.223
Montana H. B. 331, 2001 Leg. (not yet codified)
Nevada Nev. Rev. Stat. § 205.463- 465
New Hampshire N. H. Rev. Stat. Ann. § 638: 26
New Jersey N. J. Stat. Ann. § 2C: 21- 17
New Mexico H. B. 317, 2001 Leg. 45th Sess.
North Carolina N. C. Gen. Stat. § 14- 113.20 13
North Dakota N. D. Cent. Codes § 12.1- 23
Ohio Ohio Rev. Code Ann. § 2913.49
Oklahoma Okla. Stat. tit. 21, § 1533.1
Oregon Or. Rev. Stat. § 165.800
Pennsylvania 18 Pa. Cons. State § 4120
Rhode Island R. I. Gen. Laws § 11- 49.1- 1
South Carolina S. C. Code Ann. § 16- 13- 500, 501
South Dakota S. D. Codified Laws § 22- 30A- 3.1.
Tennessee Tenn. Code Ann. § 39- 14- 150
Texas Tex. Penal Code § 32.51
Utah Utah Code Ann. § 76- 6- 1101- 1104
Virginia Va. Code Ann. § 18.2- 186.3
Washington Wash. Rev. Code § 9.35.020
West Virginia W. Va. Code § 61- 3- 54
Wisconsin Wis. Stat. § 943.201
Wyoming Wyo. Stat. Ann. § 6- 3- 901

U. S. Territories

Guam 9 Guam Code Ann. § 46.80
U. S. Virgin Islands 14 VI Code Ann. §§ 3003

Resolving credit problems resulting from identity theft can be time-consuming and frustrating. The good news is that there are federal laws that establish procedures for correcting credit report errors and billing errors, and for stopping debt collectors from contacting you about debts you don't owe. Here is a brief summary of your rights, and what to do to clear up credit problems that result from identity theft.

Credit Reports

The Fair Credit Reporting Act (FCRA) establishes procedures for correcting mistakes on your credit record and requires that your record be made available only for certain legitimate business needs. Under the FCRA, both the credit bureau and the organization that provided the information to the credit bureau (the "information provider"), such as a bank or credit card company, are responsible for correcting inaccurate or incomplete information in your report. To protect your rights under the law, contact both the credit bureau and the information provider.

First, call the credit bureau and follow up in writing. Tell them what information you believe is inaccurate. Include copies (NOT originals) of documents that support your position. In addition to providing your complete name and address, your letter should clearly identify each item in your report that you dispute, give the facts and explain why you dispute the information, and request deletion or correction. You may want to enclose a copy of your report with circles around the items in question. Your letter may look something like the sample at right. Send your letter by certified mail, and request a return receipt so you can document what the credit bureau received and when. Keep copies of your dispute letter and enclosures.

Credit bureaus must investigate the items in question - usually within 30 days - unless they consider your dispute frivolous. They also must forward all relevant data you provide about the dispute to the information provider. After the information provider receives notice of a dispute from the credit bureau, it must investigate, review all relevant information provided by the credit bureau and report the results to the credit bureau. If the information provider finds the disputed information to be inaccurate, it must notify any nationwide credit bureau that it reports to so that the credit bureaus can correct this information in your file. Note that:

- Disputed information that cannot be verified must be deleted from your file.
- If your report contains erroneous information, the credit bureau must correct it.
- If an item is incomplete, the credit bureau must complete it. For example, if your file shows that you have been late making payments, but fails to show that you are no longer delinquent, the credit bureau must show that you're current.
- If your file shows an account that belongs to someone else, the credit bureau must delete it.

When the investigation is complete, the credit bureau must give you the written results and a free copy of your report if the dispute results in a change. If an item is changed or removed, the credit bureau cannot put the disputed information back in your file unless the information provider verifies its accuracy and completeness, and the credit bureau gives you a written notice that includes the name, address and phone number of the information provider.

If you request, the credit bureau must send notices of corrections to anyone who received your report in the past six months. Job applicants can have a corrected copy of their report sent to anyone who received a copy during the past two years for employment purposes. If an investigation does not resolve your dispute, ask the credit bureau to include your statement of the dispute in your file and in future reports.

Second, in addition to writing to the credit bureau, tell the creditor or other information provider in writing that you dispute an item. Again, include copies (NOT originals) of documents that support your position. Many information providers specify an address for disputes. If the information provider then reports the item to any credit bureau, it must include a notice of your dispute. In addition, if you are correct - that is, if the disputed information is not accurate - the information provider may not use it again. For more information, consult How to Dispute Credit Report Errors and Fair Credit Reporting, two brochures available from the FTC or at:

http://www.consumer.gov/idtheft

Credit Cards: The Truth in Lending Act limits your liability for unauthorized credit card charges in most cases to $50 per card. The Fair Credit Billing Act establishes procedures for resolving billing errors on your credit card accounts. The Act's settlement procedures apply to disputes about "billing errors." This includes fraudulent charges on your accounts.

To take advantage of the law's consumer protections, you must:

- write to the creditor at the address given for "billing inquiries," not the address for sending your payments. Include your name, address, account number and a description of the billing error, including the amount and date of the error.

- send your letter so that it reaches the creditor within 60 days after the first bill containing the error was mailed to you. If the address on your account was changed by an identity thief and you never received the bill, your dispute letter still must reach the creditor within 60 days of when the creditor would have mailed the bill. This is why it's so important to keep track of your billing statements and immediately follow up when your bills don't arrive on time.

Send your letter by certified mail, and request a return receipt. This will be your proof of the date the creditor received the letter. Include copies (NOT originals) of sales slips or other documents that support your position. Keep a copy of your dispute letter.

The creditor must acknowledge your complaint in writing within 30 days after receiving it, unless the problem has been resolved. The creditor must resolve the dispute within two billing cycles (but not more than 90 days) after receiving your letter.

For more information, see Fair Credit Billing and Avoiding Credit and Charge Card Fraud, two brochures available from the FTC or at:

http://www.consumer.gov/idtheft

Debt Collectors: The Fair Debt Collection Practices Act prohibits debt collectors from using unfair or deceptive practices to collect overdue bills that a creditor has forwarded for collection.

You can stop a debt collector from contacting you by writing a letter to the collection agency brochure available from the FTC telling them to stop. Once the debt collector receives your letter, the idtheft company may not contact you again – with two exceptions: they can tell you there will be no further contact and they can tell you that the debt collector or the The Electronic Fund Transfer creditor intends to take some specific action.
A collector also may not contact you if, within 30 days after you receive the written notice, you send the collection agency a letter stating you do not owe the money. Although such a letter should stop the debt collector's calls, it will not necessarily get rid of the debt itself, which may still turn up on your credit report. In addition, a collector can renew collection activities if you are sent proof of the debt. So, along with your letter stating you don't owe the money, include copies of documents that support your position.

If you're a victim of identity theft, including a copy (NOT original) of the police report you filed may be particularly useful. For more information, consult *Fair Debt Collection*, a brochure available from the FTC or at:

http://www.consumer.gov/idtheft

ATM Cards, Debit Cards and Electronic Fund Transfers

The Electronic Fund Transfer Act provides consumer protections for transactions involving an ATM or debit card or other electronic way to debit or credit an account. It also limits your liability for unauthorized electronic fund transfers.

It's important to report lost or stolen ATM and debit cards immediately because the amount you can be held responsible for depends on ***how quickly*** you report the loss.

- If you report your ATM card lost or stolen within two business days of discovering the loss or theft, your losses are limited to $50.

- If you report your ATM card lost or stolen after the two business days, but within 60 days after a statement showing an unauthorized electronic fund transfer, you can be liable for up to $500 of what a thief withdraws.

- If you wait more than 60 days, you could lose all the money that was taken from your account after the end of the 60 days and before you report your card missing.

The best way to protect yourself in the event of an error or fraudulent transaction is to call the financial institution and follow up in writing – by certified letter, return receipt requested – so you can prove when the institution received your letter. Keep a copy of the letter you send for your records.

After notification about an error on your statement, the institution generally has 10 business days to investigate. The financial institution must tell you the results of its investigation within three business days after completing it and must correct an error within one business day after determining that the error has occurred. If the institution needs more time, it may take up to 45 days to complete the investigation – but only if the money in dispute is returned to your account and you are notified promptly of the credit. At the end of the investigation, if no error has been found, the institution may take the money back if it sends you a written explanation.

Note: VISA and MasterCard voluntarily have agreed to limit consumers' liability for unauthorized use of their debit cards in most instances to $50 per card, no matter how much time has elapsed since the discovery of the loss or theft of the card.

For more information, consult *Electronic Banking* and *Credit and ATM Cards: What to Do If They're Lost or Stolen*, two brochures available from the FTC or at:

http://www.consumer.gov/idtheft

Federal Government

Federal Trade Commission (FTC) – http://www.ftc.gov/

The FTC is the federal clearinghouse for complaints by victims of identity theft. Although the FTC does not have the authority to bring criminal cases, the Commission helps victims of identity theft by providing them with information to help resolve the financial and other problems that can result from identity theft. The FTC also may refer victim complaints to other appropriate government agencies and private organizations for action.

If you've been a victim of identity theft, file a complaint with the FTC by contacting:

Identity Theft Hotline
Telephone: 1-877-IDTHEFT (438-4338)
TDD: 202-326-2502
Mail: Identity Theft Clearinghouse, Federal Trade Commission,
600 Pennsylvania Avenue, NW, Washington, DC 20580;
or online: http://www.consumer.gov/idtheft

Federal Trade Commission Publications

- Avoiding Credit and Charge Card Fraud
- Credit and ATM Cards: What to Do If They're Lost or Stolen
- Credit Card Loss Protection Offers: They're The Real Steal
- Electronic Banking
- Fair Credit Billing
- Fair Credit Reporting
- Fair Debt Collection
- Getting Purse-onal: What To Do If Your Wallet or Purse Is Stolen
- How to Dispute Credit Report Errors
- Identity Crisis... What to Do If Your Identity Is Stolen
- Identity Thieves Can Ruin Your Good Name: Tips for Avoiding Identity Theft

Banking Agencies - If you're having trouble getting your financial institution to help you resolve your banking- related identity theft problems - including problems with bank- issued credit cards - contact the agency with the appropriate jurisdiction. If you're not sure which agency has jurisdiction over your institution, call your bank or visit:

http://www.ffiec.gov/nic/default.htm

Federal Deposit Insurance Corporation (FDIC) – http://www.fdic.gov

The FDIC supervises state- chartered banks that are not members of the Federal Reserve System and insures deposits at banks and savings and loans. Call the FDIC Consumer Call Center at: 1-800-934-3342; or write:

Federal Deposit Insurance Corporation
Division of Compliance and Consumer Affairs
550 17th Street, NW
Washington, DC 20429.

FDIC publications:

Classic Cons... And How to Counter Them
www.fdic.gov/consumers/consumer/news/cnsprg98/cons.Html

Your Wallet: A Loser's Manual
www.fdic.gov/consumers/consumer/news/cnfall97/wallet.Html

A Crook Has Drained Your Account. Who Pays?
www.fdic.gov/consumers/consumer/news/cnsprg98/crook.html

Federal Reserve System - http://www.federalreserve.gov

The Fed supervises state-chartered banks that are members of the Federal Reserve System.
Call: 202-452-3693; or write:

Division of Consumer and Community Affairs
Mail Stop 801
Federal Reserve Board
Washington, DC 20551

Or, contact the Federal Reserve Bank in your area. The 12 Reserve Banks are located in:

- Boston
- New York
- Philadelphia
- Cleveland
- Richmond,
- Atlanta
- Chicago
- St. Louis
- Minneapolis
- Kansas City
- Dallas
- San Francisco

National Credit Union Administration (NCUA) http://www.ncua.gov

The NCUA charters and supervises federal credit unions and insures deposits at federal credit unions and many state credit unions. Call: 703-518-6360; or write:

Compliance Officer
National Credit Union Administration,
1775 Duke Street
Alexandria, VA 22314

Office of the Comptroller of the Currency (OCC) http://www.occ.treas.gov

The OCC charters and supervises national banks. If the word "national" appears in the name of a bank, or the initials "N.A." follow its name, the OCC oversees its operations.

Call: 1-800-613-6743 (business days 9:00 a.m. to 4:00 p.m. CST); fax: 713-336-4301; or write:

Customer Assistance Group
1301 McKinney Street
Suite 3710
Houston, TX 77010

OCC publications:

- *Check Fraud: A Guide to Avoiding Losses* – http://www.occ.treas.gov/chckfrd/idassume.htm
- *Identity Theft and Pretext Calling Advisory Letter 2001-4*
  http://www.occ.treas.gov/ftp/advisory/2001-4.doc
- *How to Avoid Becoming a Victim of Identity Theft* – http://www.occ.treas.gov/idtheft.pdf

Office of Thrift Supervision (OTS)
http://www.ots.treas.gov

The OTS is the primary regulator of all federal and many state-chartered thrift institutions, which include savings banks and savings and loan institutions.
Call: 202-906-6000; or write:

Office of Thrift Supervision
1700 G Street, NW
Washington, DC 20552

Department of Justice (DOJ)
http://www.usdoj.gov

The DOJ and its U.S. Attorneys prosecute federal identity theft cases. Information on identity theft is available at:

http://www.usdoj.gov/criminal/fraud/idtheft.html

Federal Bureau of Investigation (FBI)
http://www.fbi.gov

The FBI is one of the federal criminal law enforcement agencies that investigate cases of identity theft. Local field offices are listed in the Blue Pages of your telephone directory.

FBI publication:

- *Protecting Yourself Against Identity Fraud*

Federal Communications Commission (FCC) http://www.fcc.gov

The FCC regulates interstate and international communications by radio, television, wire, satellite and cable. The FCC's Consumer Information Bureau is the consumer's one-stop source for information, forms, applications and current issues before the FCC. Call: 1-888-CALL-FCC; TTY: 1-888-TELL-FCC; or write: Federal Communications Commission, Consumer Information Bureau, 445 12th Street, SW, Room 5A863, Washington, DC 20554. You can file complaints via the online complaint form at:

http://www.fcc.gov

For e-mail questions to: fccinfo@fcc.gov

Internal Revenue Service (IRS) http://www.treas.gov/irs/ci

The IRS is responsible for administering and enforcing the internal revenue laws. If you believe someone has assumed your identity to file federal Income Tax Returns, or to commit other tax fraud, call toll-free: 1-800-829-0433

For assistance to victims of identity theft schemes who are having trouble filing their correct returns, call the IRS Taxpayer Advocates Office, toll-free: 1-877-777-4778

U.S. Secret Service (USSS) - http://www.treas.gov/usss

The U.S. Secret Service is one of the federal law enforcement agencies that investigate financial crimes, which may include identity theft. Although the Secret Service generally investigates cases where the dollar loss is substantial, your information may provide evidence of a larger pattern of fraud requiring their involvement. Local field offices are listed in the Blue Pages of your telephone directory.

- Financial Crimes Division – http://www.treas.gov/usss/financial_crimes.htm
- Frequently Asked Questions: Protecting Yourself http://www.treas.gov/usss/faq.htm

Social Security Administration (SSA)
http://www.ssa.gov

SSA may assign you a new SSN – at your request – if you continue to experience problems even after trying to resolve the problems resulting from identity theft. SSA field office employees work closely with victims of identity theft and third parties to collect the evidence needed to assign a new SSN in these cases.

SSA Office of the Inspector General (SSA/OIG)

The SSA/OIG is one of the federal law enforcement agencies that investigate cases of identity theft. If need to report direct allegations that an SSN has been stolen or misused contact:

SSA Fraud Hotline at: 1-800-269-0271
Fax: 410-597-0118
Or, write:

SSA Fraud Hotline
P.O. Box 17768
Baltimore, MD 21235
Or, by e-mail: oig.hotline@ssa.gov

SSA publications:

- *SSA Fraud Hotline for Reporting Fraud* – http://www.ssa.gov/oig/guidelin.htm
- *Social Security – When Someone Misuses Your Number* (SSA Pub. No. 05-10064) http://www.ssa.gov/pubs/10064.html
- *Social Security – Your Number and Card* (SSA Pub. No. 05-10002) http://www.ssa.gov/pubs/10002.html

U.S. Postal Inspection Service (USPIS) http://www.usps.gov/websites/depart/inspect

The USPIS is one of the federal law enforcement agencies that investigate cases of identity theft. USPIS is the law enforcement arm of the U.S. Postal Service. USPIS has primary jurisdiction in all matters infringing on the integrity of the U.S. mail. You can locate the USPIS district office nearest you by calling your local post office or checking the list at the web site above.

U.S. Securities and Exchange Commission (SEC)

http://www.sec.gov

The SEC's Office of Investor Education and Assistance serves investors who complain to the SEC about investment fraud or the mishandling of their investments by securities professionals. If you've experienced identity theft in connection with a securities transaction, you can file a complaint with the SEC by visiting the Complaint Center at:

http://www.sec.gov/complaint.shtml

Be sure to include as much detail as possible. If you do not have access to the Internet, write to the SEC at:

SEC Office of Investor Education and Assistance
450 Fifth Street, NW
Washington, DC 20549-0213

Or, call: 202-942-7040

U.S. Trustee (UST) - http://www.usdoj.gov/ust

If you believe someone has filed for bankruptcy using your name, write to the U.S. Trustee in the region where the bankruptcy was filed. A list of the U.S. Trustee's Regional Offices is available on the UST web site, or check the Blue Pages of your phone book under U.S. Government – Bankruptcy Administration.

Your letter should describe the situation and provide proof of your identity. The U.S. Trustee, if appropriate, will make a criminal referral to criminal law enforcement authorities if you provide appropriate documentation to substantiate your claim. You also may want to file a complaint with the U.S. Attorney and/or the FBI in the city where the bankruptcy was filed. The U.S. Trustee does not provide legal representation, legal advice or referrals to lawyers. That means you may need to hire an attorney to help convince the bankruptcy court that the filing is fraudulent. The U.S. Trustee does not provide consumers with copies of court documents. Those documents are available from the bankruptcy clerk's office for a fee.

State and Local Governments

Many states and local governments have passed laws related to identity theft; others may be considering such legislation. Where specific identity theft laws do not exist, the practices may be prohibited under other laws. Contact your State Attorney General's office. For a list of state offices, visit:

http://www.naag.org

Or, to find out whether your state has laws related to identity theft, contact the local consumer protection agency.

http://www.consumer.gov/idtheft/

Credit Bureaus

Equifax

http://www.equifax.com

To order your report, call: 1-800-685-1111
Or, write:

P.O. Box 740241
Atlanta, GA 30374-0241

To report fraud, call: 1-800-525-6285
TDD: 800-255-0056 and write:

P.O. Box 740241
Atlanta, GA 30374-0241

Experian
http://www.experian.com

To order your report, call: 1-888-EXPERIAN (397-3742) or write:

P.O. Box 2104
Allen, TX 75013

To report fraud, call: 1-888-EXPERIAN (397-3742)/ TDD: 800-972-0322 and write:

P.O. Box 9532,
Allen, TX 75013

TransUnion
http://www.transunion.com

To order your report, call: 800-916-8800 or write:

P.O. Box 1000
Chester, PA 19022.

To report fraud, call: 1-800-680-7289
TDD: 877-553-7803 and write:

Fraud Victim Assistance Division
P.O. Box 6790,
Fullerton, CA 92634-6790

Credit Bureaus – Report Fraud			
Bureau	**Web site**	**Phone No.**	**Address**
Equifax	http://www.equifax.com	800-685-1111	P.O. Box 740241, Atlanta, GA 30374-0241
Experian	http://www.experian.com	888-EXPERIAN (397-3742)	P.O. Box 2104, Allen, TX 75013
TransUnion	http://www.transunion.com	800-916-8800	P.O. Box 1000, Chester, PA 19022

The following tables are provided as a template to keep track or your accounts other sources of identity info (Utility accounts, etc.) and important points of contact.

Banks, Credit Cards & Other Creditors			
Creditor	**Account No.**	**Phone No.**	**Address**

Local Law Enforcement			
Agency	**Phone No.**	**Point of Contact**	**Address**

Other – Report Fraud		
Miscellaneous	**Phone**	**Address**
Social Security Office		
Library Card		
College/University (Student Info)		
Phone Company		
Gas Company		
Water Company		
Electric Company		
Cable/Satellite TV		
Other		

The following pages include an Identity Theft Affidavit. This form is VERY important if you become a victim of Identity Theft.

ID Theft Affidavit

Victim Information

1. **My full legal name is** _____
   (First) (Middle) (Last) (Jr., Sr., III)

2. (If different from above) **When the events described in this affidavit took place, I was known as**
   _____
   (First) (Middle) (Last) (Jr., Sr., III)

3. **My date of birth is** _____
   (Day/month/year)

4. **My social security number is**_____

5. **My driver's license or identification card state and number are**_____

6. **My current address is** _____

   City _____ **State** _____ **Zip Code** _____

7. **I have lived at this address since** _____
   (Month/year)

8. (If different from above) **When the events described in this affidavit took place, my address was**
   _____

   City _____ **State** _____ **Zip Code** _____

9. **I lived at the address in # 8 from** _____ **until** _____
   (Month/year) (Month/year)

10. **My daytime telephone number is** (____)_____

    My evening telephone number is (____)_____

    Name _____ ***Phone number*** _____

ID Theft Affidavit Continued on Next Page….

How the Fraud Occurred

Check all that apply for items 11 - 17:

11. ☐ I did not authorize anyone to use my name or personal information to seek the money, credit, loans, goods or services described in this report.

12. ☐ I did not receive any benefit, money, goods or services as a result of the events described in this report.

13. ☐ My identification documents (for example, credit cards; birth certificate; driver's license; social security card; etc.) were ☐ stolen ☐ lost on or about _____.
    (Day/month/year)

14. ☐ To the best of my knowledge and belief, the following person(s) used my information (for example, my name, address, date of birth, existing account numbers, social security number, mother's maiden name, etc.) or identification documents to get money, credit, loans, goods or services without my knowledge or authorization:

Provide any information you have regarding any persons you suspect may have used you account information. If you do not have specific contact information state: **UNKNOWN**	
Name:	**Name**:
Address:	**Address**:
Phone Numbers:	**Phone Numbers:**
Additional Info:	**Additional Info:**

15. ☐ I do NOT know who used my information or identification documents to get money, credit, loans, goods or services without my knowledge or authorization.

16. ☐ Additional comments: (For example, description of the fraud, which documents or information were used or how the identity thief gained access to your information.)

(Attach additional pages as necessary.)

Name_____ **Phone number**_____

Victim's Law Enforcement Actions

17. (Check one) I ☐ am ☐ am not willing to assist in the prosecution of the person(s) who committed this fraud.

18. (Check one) I ☐ am ☐ am not authorizing the release of this information to law enforcement for the purpose of assisting them in the investigation and prosecution of the person(s) who committed this fraud.

19. (Check all that apply) I ☐ have ☐ have not reported the events described in this affidavit to the police or other law enforcement agency. The police ☐ did ☐ did not write a report.

If you have contacted the police or other law enforcement agency, please complete the following:	
Agency:	Person who took the report:
Date of Report:	
Phone No.	Email Address (if known)
Agency:	Person who took the report:
Date of Report:	
Phone No.	Email Address (if known)

Documentation Checklist

Please indicate the supporting documentation you are able to provide to the companies you plan to notify. Attach copies (NOT originals) to the affidavit before sending it to the companies.

20. ☐ A copy of a valid government-issued photo-identification card (for example, your driver's license, state-issued ID card or your passport). If you are under 16 and don't have a photo-ID, you may submit a copy of your birth certificate or a copy of your official school records showing your enrollment and place of residence.

21. ☐ Proof of residency during the time the disputed bill occurred, the loan was made or the other event took place (for example, a rental/lease agreement in your name, a copy of a utility bill or a copy of an insurance bill).

22. ☐ A copy of the report you filed with the police or sheriff's department. If you are unable to obtain a report or report number from the police, please indicate that in Item 19. Some companies only need the report number, not a copy of the report. You may want to check with each company.

Name _____ ***Phone number*** _____

Signature

I declare under penalty of perjury that the information I have provided in this affidavit is true and correct to the best of my knowledge.

_____

(Signature) (Date signed)

Knowingly submitting false information on this form could subject you to criminal prosecution for perjury.

_____

(Notary)

[Check with each company. Creditors sometimes require notarization. If they do not, please have one witness (non-relative) sign below that you completed and signed this affidavit.]

Witness:

_____
(Signature) (Printed name)

_____
(Date) (Telephone number)

Name _____ ***Phone number*** _____

Fraudulent Account Statement

Completing this Statement
• Make as many copies of this page as you need. **Complete a separate page for each company you're notifying and only send it to that company.** Include a copy of your signed affidavit. • List only the account(s) you're disputing with the company receiving this form. **See the example below.** • If a collection agency sent you a statement, letter or notice about the fraudulent account, attach a copy of that document (**NOT** the original).

I declare (check all that apply):

☐ As a result of the event(s) described in the ID Theft Affidavit, the following account(s) was/were opened at your company in my name without my knowledge, permission or authorization using my personal information or identifying documents:

Creditor Name/Address	Account No.	Type of Unathorized use	Date issued or opened	Amount or value
Example Example National Bank 22 Main Street Columbus, Ohio 22722	01234567-89	Auto loan	01/05/2000	$25,500.00

☐ During the time of the accounts described above, I had the following account open with your company:

Billing name _____

Billing address _____

Account number _____