Identity Theft and Fraud

What Are Identity Theft and Identity Fraud?

"But he that filches from me my good name/Robs me of that which not enriches him/And makes me poor indeed." - Shakespeare, *Othello*, act iii. Sc. 3.

The short answer is that identity theft is a crime. Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain. These Web pages are intended to explain why you need to take precautions to protect yourself from identity theft.

Unlike your fingerprints, which are unique to you and cannot be given to someone else for their use, your personal data especially your Social Security number, your bank account or credit card number, your telephone calling card number, and other valuable identifying data can be used, if they fall into the wrong hands, to personally profit at your expense. In the United States and Canada, for example, many people have reported that unauthorized persons have taken funds out of their bank or financial accounts, or, in the worst cases, taken over their identities altogether, running up vast debts and committing crimes while using the victims's names. In many cases, a victim's losses may include not only out-of-pocket financial losses, but substantial additional financial

costs associated with trying to restore his reputation in the community and correcting erroneous information for which the criminal is responsible.

In one notorious case of identity theft, the criminal, a convicted felon, not only incurred more than $100,000 of credit card debt, obtained a federal home loan, and bought homes, motorcycles, and handguns in the victim's name, but called his victim to taunt him -- saying that he could continue to pose as the victim for as long as he wanted because identity theft was not a federal crime at that time -- before filing for bankruptcy, also in the victim's name. While the victim and his wife spent more than four years and more than $15,000 of their own money to restore their credit and reputation, the criminal served a brief sentence for making a false statement to procure a firearm, but made no restitution to his victim for any of the harm he had caused. This case, and others like it, prompted Congress in 1998 to create a new federal offense of identity theft.

What Are The Most Common Ways To Commit Identity Theft Or Fraud?

Many people do not realize how easily criminals can obtain our personal data without having to break into our homes. In public places, for example, criminals may engage in "shoulder surfing" watching you from a nearby location as you punch in your telephone calling card number or credit card number or listen in on your conversation if you give your credit-card number over the telephone to a hotel or rental car company.

Even the area near your home or office may not be secure. Some criminals engage in "dumpster diving" going through your garbage cans or a communal dumpster or trash bin -- to obtain copies of your checks, credit card or bank statements, or other records that typically bear your name, address, and even your telephone number. These types of records make it easier for criminals to get control over accounts in your name and assume your identity.

If you receive applications for "pre-approved" credit cards in the mail, but discard them without tearing up the enclosed materials, criminals may retrieve them and try to activate the cards for their use without your knowledge. (Some credit card companies, when sending credit cards, have adopted security measures that allow a card recipient to activate the card only from his or her home telephone number but this is not yet a universal practice.) Also, if your mail is delivered to a place where others have ready access to it, criminals may simply intercept and redirect your mail to another location.

In recent years, the Internet has become an appealing place for criminals to obtain identifying data, such as passwords or even banking information. In their haste to explore the exciting features of the Internet, many people respond to "spam" unsolicited E-mail that promises them some benefit but requests identifying data, without realizing that in many cases, the requester has no intention of keeping his promise. In some cases, criminals reportedly have used computer technology to obtain large amounts of personal data.

With enough identifying information about an individual, a criminal can take over that individual's identity to conduct a wide range of crimes: for example, false applications for loans and credit cards, fraudulent withdrawals from bank accounts, fraudulent use of telephone calling cards, or obtaining other goods or privileges which the criminal might be denied if he were to use his real name. If the criminal takes steps to ensure that bills for the falsely obtained credit cards, or bank statements showing the unauthorized withdrawals, are sent to an address other than the victim's, the victim may not become aware of what is happing until the criminal has already inflicted substantial damage on the victim's assets, credit, and reputation.

Back to Top

What's The Department Of Justice Doing About Identity Theft And Fraud?

The Department of Justice prosecutes cases of identity theft and fraud under a variety of federal statutes. In the fall of 1998, for example, Congress passed the Identity Theft and Assumption Deterrence Act . This legislation created a new offense of identity theft, which prohibits

knowingly transfer[ring] or us[ing], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.

18 U.S.C. § 1028(a)(7). This offense, in most circumstances, carries a maximum term of 15 years' imprisonment, a fine, and criminal forfeiture of any personal property used or intended to be used to commit the offense.

Schemes to commit identity theft or fraud may also involve violations of other statutes such as identification fraud (18 U.S.C. § 1028), credit card fraud (18 U.S.C. § 1029), computer fraud (18 U.S.C. § 1030), mail fraud

(18 U.S.C. § 1341), wire fraud (18 U.S.C. § 1343), or financial institution fraud (18 U.S.C. § 1344). Each of these federal offenses are felonies that carry substantial penalties in some cases, as high as 30 years' imprisonment, fines, and criminal forfeiture.

Federal prosecutors work with federal investigative agencies such as the Federal Bureau of Investigation, the United States Secret Service, and the United States Postal Inspection Service to prosecute identity theft and fraud cases.

Here are some examples of recent cases:

Central District of California. A woman pleaded guilty to federal charges of using a stolen Social Security number to obtain thousands of dollars in credit and then filing for bankruptcy in the name of her victim. More recently, a man was indicted, pleaded guilty to federal charges and was sentenced to 27 months' imprisonment for obtaining private bank account information about an insurance company's policyholders and using that information to deposit $764,000 in counterfeit checks into a bank account he established.

Central District of California. Two of three defendants have pleaded guilty to identity theft, bank fraud, and related charges for their roles in a scheme to open bank accounts with both real and fake identification documents, deposit U.S. Treasury checks that were stolen from the mail, and withdraw funds from those accounts.

Middle District of Florida. A defendant has been indicted on bank fraud charges for obtaining names, addresses, and Social Security numbers from a Web site and using those data to apply for a series of car loans over the Internet.

Southern District of Florida. A woman was indicted and pleaded guilty to federal charges involving her obtaining a fraudulent driver's license in the name of the victim, using the license to withdraw more than $13,000 from the victim's bank account, and obtaining five department store credit cards in the victim's name and charging approximately $4,000 on those cards.

District of Kansas. A defendant pleaded guilty to conspiracy, odometer fraud, and mail fraud for operating an odometer "rollback" scheme on used cars. The defendant used false and assumed identities, including the identities of deceased persons, to obtain false identification documents and fraudulent car titles.

What Can I Do About Identity Theft And Fraud?

To victims of identity theft and fraud, the task of correcting incorrect information about their financial or personal status, and trying to restore their good names and reputations, may seem as daunting as trying to solve a puzzle in which some of the pieces are missing and other pieces no longer fit as they once did. Unfortunately, the damage that criminals do in stealing another person's identity and using it to commit fraud often takes far longer to undo than it took the criminal to commit the crimes.

What Should I Do To Avoid Becoming A Victim Of Identity Theft?

To reduce or minimize the risk of becoming a victim of identity theft or fraud, there are some basic steps you can take. For starters, just remember the word "**SCAM**":

S Be **stingy** about giving out your personal information to others unless you have a reason to trust them, regardless of where you are:

At Home.

1. Start by adopting a "need to know" approach to your personal data. Your credit card company may need to know your mother's maiden name, so that it can verify your identity when you call to inquire about your account. A person who calls you and says he's from your bank, however, doesn't need to know that information if it's already on file with your bank; the only purpose of such a call is to acquire that information for that person's personal benefit. Also, the more information that you have printed on your personal bank checks -- such as your Social Security number or home telephone number -- the more personal data you are routinely handing out to people who may not need that information.
2. If someone you don't know calls you on the telephone and offers you the chance to receive a "major" credit card, a prize, or other valuable item, but asks you for personal data -- such as your Social Security number, credit card number or expiration date, or mother's maiden name -- ask them to send you a written application form.
3. If they won't do it, tell them you're not interested and hang up.

4. If they will, review the application carefully when you receive it and make sure it's going to a company or financial institution that's well-known and reputable. The Better Business Bureau can give you information about businesses that have been the subject of complaints.

On Travel.

1. If you're traveling, have your mail held at your local post office, or ask someone you know well and trust another family member, a friend, or a neighbor to collect and hold your mail while you're away.
2. If you have to telephone someone while you're traveling, and need to pass on personal financial information to the person you're calling, don't do it at an open telephone booth where passersby can listen in on what you're saying; use a telephone booth where you can close the door, or wait until you're at a less public location to call.

C Check your financial information regularly, and look for what should be there and what shouldn't:

What Should Be There.

1. If you have bank or credit card accounts, you should be receiving monthly statements that list transactions for the most recent month or reporting period.
2. If you're not receiving monthly statements for the accounts you know you have, call the financial institution or credit card company immediately and ask about it.
3. If you're told that your statements are being mailed to another address that you haven't authorized, tell the financial institution or credit card representative immediately that you did not authorize the change of address and that someone may be improperly using your accounts. In that situation, you should also ask for copies of all statements and debit or charge transactions that have occurred since the last statement you received. Obtaining those copies will help you to work with the financial institution or credit card company in determining whether some or all of those debit or charge transactions were fraudulent.

What Shouldn't Be There.

1. If someone has gotten your financial data and made unauthorized debits or charges against your financial accounts, checking your monthly statements carefully may be the quickest way for you to find out. Too many of us give those statements, or the enclosed checks or credit transactions, only a quick glance, and don't review them closely to make sure there are no unauthorized withdrawals or charges.
2. If someone has managed to get access to your mail or other personal data, and opened any credit cards in your name or taken any funds from your bank account, contact your financial institution or credit card company immediately to report those transactions and to request further action.

A **A**sk periodically for a copy of your credit report.

Your credit report should list all bank and financial accounts under your name, and will provide other indications of whether someone has wrongfully opened or used any accounts in your name.

M **M**aintain careful records of your banking and financial accounts.

Even though financial institutions are required to maintain copies of your checks, debit transactions, and similar transactions for five years, you should retain your monthly statements and checks for at least one year, if not more. If you need to dispute a particular check or transaction especially if they purport to bear your signatures your original records will be more immediately accessible and useful to the institutions that you have contacted.

Even if you take all of these steps, however, it's still possible that you can become a victim of identity theft. Records containing your personal data -- credit-card receipts or car-rental agreements, for example -- may be found by or shared with someone who decides to use your data for fraudulent purposes.

What Should I Do If I've Become A Victim Of Identity Theft?

If you think you've become a victim of identity theft or fraud, act immediately to minimize the damage to your personal funds and financial accounts, as well as your reputation. Here's a list -- based in part on a checklist prepared by the California Public Interest Research Group (CalPIRG) and the Privacy Rights Clearinghouse -- of some actions that you should take right away:

1. Contact the Federal Trade Commission (FTC) to report the situation, whether --
2. Online,
3. By telephone toll-free at 1-877-ID THEFT (877-438-4338) or TDD at 202-326-2502, or
4. By mail to Consumer Response Center, FTC, 600 Pennsylvania Avenue, N.W., Washington, DC 20580.

Under the Identity Theft and Assumption Deterrence Act , the Federal Trade Commission is responsible for receiving and processing complaints from people who believe they may be victims of identity theft, providing informational materials to those people, and referring those complaints to appropriate entities, including the major credit reporting agencies and law enforcement agencies. For further information, please check the FTC's identity theft Web pages . You can also call your local office of the FBI or the U.S. Secret Service to report crimes relating to identity theft and fraud.

You may also need to contact other agencies for other types of identity theft:

1. Your local office of the Postal Inspection Service if you suspect that an identity thief has submitted a change-of-address form with the Post Office to redirect your mail, or has used the mail to commit frauds involving your identity;
2. The Social Security Administration if you suspect that your Social Security number is being fraudulently used (call 800-269-0271 to report the fraud);
3. The Internal Revenue Service If you suspect the improper use of identification information in connection with tax violations (call 1-800-829-0433 to report the violations).

Call the fraud units of the three principal credit reporting companies:

Equifax:

1. To report fraud, call (800) 525-6285 or write to P.O. Box 740250, Atlanta, GA 30374-0250.
2. To order a copy of your credit report ($8 in most states), write to P.O. Box 740241, Atlanta, GA 30374-0241, or call (800) 685-1111.
3. To dispute information in your report, call the phone number provided on your credit report.
4. To opt out of pre-approved offers of credit, call (888) 567-8688 or write to Equifax Options, P.O. Box 740123, Atlanta GA 30374-0123.

Experian (formerly TRW)

1. To report fraud, call (888) EXPERIAN or (888) 397-3742, fax to (800) 301-7196, or write to P.O. Box 1017, Allen, TX 75013.
2. To order a copy of your credit report ($8 in most states): P.O. Box 2104, Allen TX 75013, or call (888) EXPERIAN.
3. To dispute information in your report, call the phone number provided on your credit report.
4. To opt out of pre-approved offers of credit and marketing lists, call (800) 353-0809 or (888) 5OPTOUT or write to P.O. Box 919, Allen, TX 75013.

Trans Union

1. To report fraud, call (800) 680-7289 or write to P.O. Box 6790, Fullerton, CA 92634.
2. To order a copy of your credit report ($8 in most states), write to P.O. Box 390, Springfield, PA 19064 or call: (800) 888-4213.
3. To dispute information in your report, call the phone number provided on your credit report.
4. To opt out of pre-approved offers of credit and marketing lists, call (800) 680-7293 or (888) 5OPTOUT or write to P.O Box 97328, Jackson, MS 39238.

Contact all creditors with whom your name or identifying data have been fraudulently used. For example, you may need to contact your long-distance telephone company if your long-distance calling card has been stolen or you find fraudulent charges on your bill.

Contact all financial institutions where you have accounts that an identity thief has taken over or that have been created in your name but without your knowledge. You may need to cancel those accounts, place stop-payment orders on any outstanding checks that may not have cleared, and change your Automated Teller Machine (ATM) card, account, and Personal Identification Number (PIN).

Contact the major check verification companies (listed in the CalPIRG-Privacy Rights Clearinghouse checklist) if you have had checks stolen or bank accounts set up by an identity thief. In particular, if you know that a particular merchant has received a check stolen from you, contact the verification company that the merchant uses:

1. CheckRite -- (800) 766-2748
2. ChexSystems -- (800) 428-9623 (closed checking accounts)

3. CrossCheck -- (800) 552-1900
4. Equifax -- (800) 437-5120
5. National Processing Co. (NPC) -- (800) 526-5380
6. SCAN -- (800) 262-7771
7. TeleCheck -- (800) 710-9898

Back to Top | DOJ Home Page | Fraud Section Home Page

Where Can I Find Out More About Identity Theft And Fraud?

A number of government and private organizations have information about various aspects of identity theft and fraud: how it can occur, what you can do about it, and how to guard your privacy. To help you learn more about the problem and its solutions, we've attached a list of Web sites that you might find interesting and informative on identity theft and related topics.

[Note: All Web sites to which these pages cross-link are included as a service for the reader. Cross-links to non-governmental sites do not constitute an endorsement or approval of their content, or of the organizations responsible for that content, by the Department of Justice.]

Government

United States:

California Department of Consumer Affairs
Consumer.gov
Federal Bureau of Investigation
Federal Deposit Insurance Corporation
Federal Trade Commission - Congressional Testimony
Federal Trade Commission - Consumer Alert
United States Postal Inspection Service
United States Secret Service

Canada: Ontario Information and Privacy Commissioner

<http://www.ncjrs.org/>