

## Avoid Being a Victim of Identity Theft

You've probably heard that identity theft is becoming an ever increasing problem in American society. Just watch your nightly news or read your local newspaper. The Federal Trade Commission ("FTC") reports that criminals are inventing all sorts of clever ways to steal your identity. According to a 2003 FTC report, identity theft has affected more than 27 million Americans in the past 5 years and it is on the rise. In 2002 nearly 10 million people reported having been a victim of identity theft, either through new credit card accounts or gaining access to existing bank account(s). On average, criminals collected \$10,200 worth of goods, money or services with other peoples identity.

Despite your best efforts to manage the flow of your personal information, skilled identity thieves may use a variety of methods, both low and hi-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 collect banking information from a check you wrote to a business (there is a greater probability of becoming a victim when writing a check since it includes all banking information, your signature and possibly your drivers license).**
- **They steal credit and debit card account numbers as your card is processed by using a special information storage device in a practice known as "skimming."**
- They steal wallets and purses containing your identification and credit and bank cards.
- They steal your mail, including your bank and credit card statements, pre-approved credit offers, new checks, 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 legal right to, the information.
- They find personal information in your home.
- They scam you, often through email, by posing as legitimate companies or government agencies you do business with.

How identity thieves **use** your personal information:

- **They counterfeit checks or debit cards, and drain your bank account.**
- 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 buy cars by taking out auto loans in your name.
- They give your name to the police during an arrest. If they're released from police custody, but don't show up for their court date, an arrest warrant is issued in your name.

As with any crime, you can't guarantee that you will never be a victim, but you can reduce that risk. By managing your personal information carefully and educating yourself about the issues, you can help guard against identity theft.

- Don't give out personal information on the phone, through mail or over the Internet unless you've initiated the contact or are sure you know who you're dealing with. Identity thieves may pose as representatives of banks, Internet service providers (ISPs) and even government agencies to get you to reveal your SSN, mother's maiden name, account numbers, and other identifying information. Before you share any personal information, confirm that you are dealing with a legitimate organization. You can check the organization's Web site as many companies post scam alerts when their name is used improperly, or you can call customer service using the number listed on your account statement or in the telephone book.
- Don't carry your SSN card; leave it in a secure place.

- Secure personal information in your home, especially if you have roommates, employ outside help or are having service work done in your home.
- Guard your mail and trash from theft:
  - ❖ Deposit outgoing mail in post office collection boxes or at your local post office, rather than in an unsecured mailbox. Promptly remove mail from your mailbox. 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 or are home to receive it.
  - ❖ To prevent 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, checks and bank statements, expired charge cards that you're discarding, and credit offers you get in the mail.
- Carry only the identification information and the number of credit and debit cards that you'll actually need.
- Place 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. When opening new accounts, you may find that many businesses still have a line on their applications for your mother's maiden name. Use a password instead.
- Ask about information security procedures in your workplace or at businesses, doctor's offices or other institutions that collect personally identifying information from you. Find out who has access to your personal information and verify that it is handled securely. Ask about the disposal procedures for those records as well. Find out if your information will be shared with anyone else. If so, ask if you can keep your information confidential.
- Give your SSN only when necessary. Ask to use other types of identification when possible. If your state uses your SSN as your driver's license number, ask to substitute another number. Do the same if your health insurance company uses your SSN as your account number.
- Pay attention to your billing cycles. Follow up with creditors if your bills don't arrive on time. A missing bill could mean an identity thief has taken over your account and changed your billing address to cover his tracks.
- Be wary of promotional scams. Identity thieves may use phony offers to get you to give them your personal information.
- Keep your purse or wallet in a safe place at work as well as any copies you may keep of administrative forms that contain your sensitive personal information.
- Cancel all unused credit accounts.
- When ordering new checks, pick them up at the bank, rather than having them sent to your home mailbox (unless you have a secure mailbox).

**If you think your identity has been stolen, here's what to do now:**

❶ Contact the fraud department of any one of the three major credit bureaus to place a fraud alert on your credit file. The fraud alert requests creditors to contact you before opening any new accounts or making any changes to your existing accounts. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will be automatically notified to place fraud alerts, and all three credit reports will be sent to you free of charge.

❷ Close the accounts that you know or believe have been tampered with or opened fraudulently. Use the ID Theft Affidavit when disputing new unauthorized accounts.

③ File a police report. Get a copy of the report to submit to your creditors and others that may require proof of the crime.

④ File your complaint with the FTC. The FTC maintains a database of identity theft cases used by law enforcement agencies for investigations. Filing a complaint also helps them learn more about identity theft and the problems victims are having.

In addition, you can notify the three major credit bureaus that you do not want personal information about you shared for promotional purposes.

**Equifax - [www.equifax.com](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 and write:  
P.O. Box 740241, Atlanta, GA 30374-0241

Hearing impaired call 1-800-255-0056 and ask the operator to call the Auto Disclosure Line at 1-800-685-1111 to request a copy of your report.

**Experian - [www.experian.com](http://www.experian.com)**

*To order your report*, call: 888-EXPERIAN (397-3742) or write:  
P.O. Box 2002, Allen TX 75013

*To report fraud*, call: 888-EXPERIAN (397-3742) and write:  
P.O. Box 9530, Allen TX 75013  
TDD: 1-800-972-0322

**Trans Union - [www.transunion.com](http://www.transunion.com)**

*To order your report*, call: 800-888-4213 or write:  
P.O. Box 1000, Chester, PA 19022

*To report fraud*, call: 800-680-7289 and write:  
Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92634  
TDD: 1-877-553-7803

For additional information and complete statistics on Identity Theft visit the Federal Trade Commission at <http://www.consumer.gov/idtheft/>