

IDENTITY THEFT

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, change service providers for your cell phone, or apply for a credit card. In each transaction, you reveal bits of personal information, like your bank and credit card account numbers; your income; your social security number (SSN); or your name, address, and phone numbers – a goldmine of information for an identity thief. Once a thief has that information, it can be used without your knowledge to commit fraud or theft.

Identity theft is a serious crime. People whose identities have been stolen can spend time and money cleaning up the mess the thieves have made of their good name and credit record. They may lose out on job opportunities, and loans for education, housing, or cars. They may even get arrested for crimes they didn't commit.

Can you prevent an identity theft? As with any crime, you cannot completely control whether you will become a victim. But according to the Federal Trade Commission (FTC), the nation's consumer protection agency, you can minimize your risk by managing your personal information cautiously.

How Identity Theft Occurs

Skilled identity thieves use a variety of ways to gain access to your personal information. For example, they may get information from businesses or other institutions by stealing it while they're on the job; bribing an employee who has access to these records; hacking these records; and conning information out of employees. Or:

- They may steal your wallet or purse;
- They may steal your personal information through e-mail or the phone by saying they're from a legitimate company and claiming that you have a problem with your account. This practice is known as "phishing" online or "pretexting" by phone.
- They may steal your credit or debit card numbers by capturing the information in a data storage device known as "skimming". They may swipe your card for an actual purchase, or attach a device to an ATM machine where they may enter or swipe your card.
- They may get your credit reports by abusing the authorized access that was granted to their employer; or by posing as a landlord, employer; or someone else who may have a legal right to your report.
- They may rummage through your trash, the trash of businesses, or public trash dumps in a practice known as "dumpster diving".
- They may steal personal information they find in your home.
- They may steal your mail, including bank and credit card statements, credit card offers, new checks and tax information.
- They may complete a "change of address form" to divert your mail to another location.

Once identity thieves have your personal information, they may use it to commit fraud or theft. For example:

- They may call your credit card issuer to change the billing address on your account. The imposter then runs up charges on your account. Because the bills are being sent to a different address, it may be some time before you realize there's a problem.
- They may open new credit card accounts in your name. When they use the credit cards and don't pay the bills, the delinquent accounts are reported on your credit report.
- They may establish phone or wireless service in your name.
- They may open a bank account in your name and write bad checks on the account.
- They may counterfeit checks or credit or debit cards, or authorize electronic transfers in your name and drain your bank account.
- They may file for bankruptcy under your name to avoid paying debts they've incurred under your name or to avoid eviction.
- They may buy a car by taking out an auto loan in your name.
- They may get identification such as a driver's license issued with their picture in your name.
- They may get a job or file fraudulent tax returns in your name.
- They may give your name to the police during an arrest. If they don't show up for the court date, a warrant for arrest is issued in your name.

How Can You Tell If You're A Victim of Identity Theft?

If an identity thief is opening new credit accounts in your name, these accounts are likely to show up on your credit report. You can find out by ordering a copy of your credit report from the three nationwide consumer reporting companies. If you have lost any personal information – or if it has been stolen—you may want to check all your reports more frequently for the first year.

Monitor the balances of your financial accounts. Look for unexplained charges or withdrawals. Other indications of identity theft can be:

1. failing to receive bills or other mail. This could mean an identity thief has submitted a change of address.
2. receiving credit cards for which you did not apply.
3. denial of credit for no apparent reason
4. receiving calls from debt collectors or companies about merchandise or services you didn't buy.

To order your free annual credit report from one or all the national consumer reporting companies, visit: www.annualcreditreport.com; call toll free 1-877-322-8228 or complete the Annual Credit Report Request Form and mail it to: annual Credit Report Request Service, PO Box 105281, Atlanta, GA 30348-5281. You can print the form from www.ftc.gov/credit. Do not contact the three nationwide consumer reporting companies individually; they provide free annual credit reports only through www.annualcreditreport.com.

If Your Personal Information Has Been Lost or Stolen

If you've lost personal information or identification, or if it has been stolen from you, you can minimize the potential for identity theft if you act quickly.

- **Financial accounts:** Close accounts like credit card and bank accounts immediately. When you open new accounts, place passwords on them. Avoid using 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.
- **Social Security number:** Call the toll free fraud number of any of the three nationwide consumer reporting companies and place an **initial fraud alert** on your credit reports. An alert can help stop someone from opening new credit accounts in your name.
- **Driver's license/other government issued identification:** Contact the agency that issued the license or other identification document. Follow its procedures to cancel the document and to get a replacement. Ask the agency to flag your file so that no one else can get a license or any other identification document from them in your name.

Once you have taken these precautions, watch for signs that your information is being misused, and that your identity has been stolen. If your information has been misused, file a report about the theft with the police and file a complaint with the FTC as well. If another crime was committed – for example, if your purse or wallet was stolen or your house or car was broken into – report it to the police immediately.

For More Information

The FTC publishes a series of publications about the importance of personal information privacy. To request free copies of brochures, visit ftc.gov or call 1-877-FTC-HELP (1-877-382-4357).

Information provided by the Federal Trade Commission