ACCESS Education Systems

DOLLARS & Sense

Family Financial Education Foundation

Edition 1, Volume 5

# Identity Theft—Are You at Risk?

Identity theft. Chances are you're familiar with the term. But what is it really all about, and are you at risk of becoming a victim?

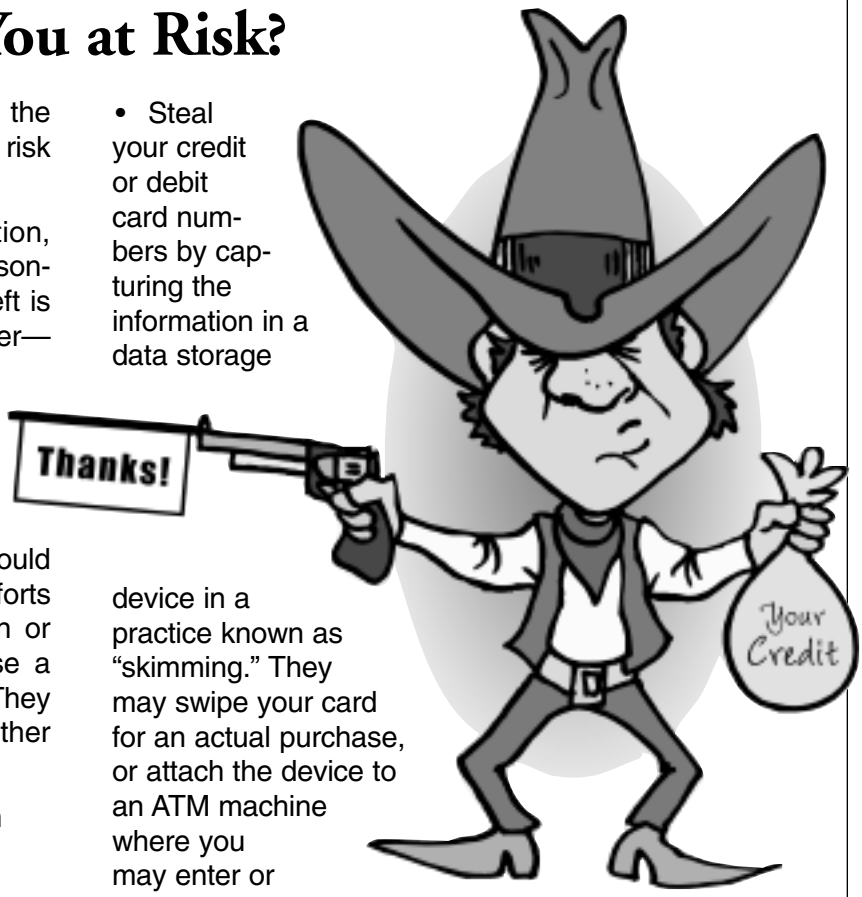
According to the Social Security Administration, identity theft occurs when a criminal uses your personal information to take on your identity. Identity theft is much more than misuse of a Social Security number—it can also include credit card and mail fraud. The Federal Trade Commission (FTC) says identity theft occurs when someone uses your personal information without your permission to commit fraud or other crimes.

So how does someone steal your identity? It could happen in a number of ways. Despite your best efforts to manage the flow of your personal information or to keep it to yourself, skilled identity thieves use a variety of methods to gain access to your data. They can obtain information from businesses or other institutions by:

- Stealing records or information while they're on the job;
- Bribing an employee who has access to these records;
- Hacking into computer records or other devices;
- Conning information out of employees.

**Thieves might also:**

- Steal your mail, including bank and credit card statements, credit card offers, new checks, and tax information;
- Go through trash, or the trash of businesses, or public trash dumps in a practice known as "dumpster diving;"
- Obtain your credit reports by abusing their employer's authorized access to them, or by posing as a landlord, employer, or someone else who may have a legal right to access your report;
- Steal your credit or debit card numbers by capturing the information in a data storage device in a practice known as "skimming." They may swipe your card for an actual purchase, or attach the device to an ATM machine where you may enter or swipe your card.




**In addition, identity thieves could:**

- Steal your wallet or purse;
- Complete a "change of address form" to divert your mail to another location;
- Steal personal information they find in your home;
- Steal personal information from you through e-mail or phone by posing as legitimate companies and claiming that you have a problem with your account. This practice is known as "phishing" online, or pretexting by phone.

**More about Pretexting**

Pretexting is the practice of getting your personal information under false pretenses, and is against the law.

*Continued on page 2*

ARTICLES

# Identity Theft–Are You At Risk?

*Continued from page 1*

Pretexters sell your information to people who may use it to get credit in your name, steal your assets, or to investigate you or try to take legal action against you under false pretenses.

According to the FTC, pretexters use a variety of tactics to get your personal information. For example, pretexters may call, claiming they're from a survey firm, and ask you a few questions. When pretexters have obtained the information they want, they use it to call your financial institution and pretend to be you or someone with authorized access to your account.

A pretexter might claim that he's forgotten his checkbook and needs information about his account. He may be able to obtain personal information about you such as your Social Security number, bank and credit card account numbers, information in your credit report, and the existence and size of your savings and investment portfolios.

Keep in mind that some information about you may be a matter of public record, such as whether you own a home, pay your real estate taxes, or have ever filed for bankruptcy. It is not pretexting for another person to collect this kind of information.

**But remember, it's illegal for anyone to:**

- Use false, fictitious, or fraudulent statements or documents to get customer information from a financial institution or directly from a customer of a financial institution;
- Use forged, counterfeit, lost, or stolen documents to get customer information from a financial institution or directly from a customer of a financial institution;
- Ask another person to get someone else's customer information using false, fictitious, or fraudulent statements or using false, fictitious, or fraudulent documents or forged, counterfeit, lost, or stolen documents.

**What Are the Effects of Identity Theft?**

Once identity thieves have your personal information, they use it in a variety of ways. They may call your credit card issuer to change the billing address on your credit card account. The imposter then runs up charges on your account. Because your bills are being sent to a different address, it may be some time before you realize there's a problem.

Thieves 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. Or they might:

- Establish phone or wireless service in your name;
- Open a bank account in your name and write bad checks on that account;
- Create counterfeit checks or credit or debit cards, or authorize electronic transfers in your name, and drain your bank account;
- File for bankruptcy under your name to avoid paying debts they've incurred under your name, or to avoid eviction;
- Buy a car by taking out an auto loan in your name;
- Obtain identification such as a driver's license issued with their picture, in your name;
- Get a job or file fraudulent tax returns in your name;
- Give your name to the police during an arrest. If they don't show up for their court date, a warrant for arrest is issued in your name.

So how can you tell if you're a victim of identity theft? Read the "Take Action Now" section on the next page.

**Did You Know? —**
**Facts and Stats about Identity Theft**

Consumer Sentinel, the complaint database developed and maintained by the Federal Trade Commission, compiled "Consumer Fraud and Identity Theft Complaint Data" from January through December 2005. Here are some of the key findings:

- Credit card fraud (26%) was the most common form of reported identity theft, followed by phone or utilities fraud (18%), bank fraud (17%), and employment fraud (12%). Other significant categories of identity theft reported by victims were government documents/benefits fraud (9%) and loan fraud (5%).
- "Electronic Fund Transfer" related identity theft was the most frequently reported type of identity theft bank fraud during calendar year 2005.
- The major metropolitan areas with the highest per capita rates of reported identify theft are Phoenix-

*Continued on page 3*

*Continued from page 2*

Mesa-Scottsdale, Arizona; Las Vegas-Paradise, Nevada; and Riverside-San Bernardino-Ontario, California.

- Between January and December 2005, Consumer Sentinel received more than 685,000 consumer fraud and identify theft complaints. Consumers reported losses from fraud of more than $680 million.

*Source: Data from Consumer Sentinel and the Identity Theft Data Clearinghouse, "Consumer Fraud and Identity Theft Complaint Data, January – December 2005, Federal Trade Commission, January 2006*

**Have You Fallen Prey to ID Theft? Take Action Now.**

So, just how can you tell if you're a victim of identity theft, and what can you do about it?

If an identity thief is opening credit accounts in your name, these accounts are likely to show up on your credit report. Contact FFEF who can provide you with a Credit Score Review. This service will help you identify suspicious accounts that you have not opened or debts you cannot explain. FFEF will pull your scored, 3-in-1 credit report, analyze it, and assess the positive and the negative items listed.

If there is any incorrect information on the report, FFEF will instruct you on how to correct these items. Remember, it's important to check your credit reports periodically to make sure no fraudulent activity has occurred.

**Stay alert for other signs of identity theft, like:**

- Failure to receive bills or other mail. 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.
- Receipt of credit cards that you didn't apply for.
- Denial of credit, or being offered less favorable credit terms (like a high interest rate) for no apparent reason.
- Calls or letters from debt collectors or businesses about merchandise or services you didn't buy.

**How Long Can the Effects of Identity Theft Last?**

It's tough to predict how long the effects of identity theft may linger because it depends on many factors, such as the type of theft, whether the thief sold or passed your information on to other thieves, whether the thief is caught, and problems related to correcting your credit report.

If you're a victim, you should monitor your credit reports and other financial records for several months after you discover the crime. You should review your credit reports once every three months in the first year of the theft, and once a year thereafter. Stay alert for other signs of identity theft. Also, don't delay in correcting your records and contacting all companies that opened fraudulent accounts. The longer the inaccurate information goes uncorrected, the longer it will take to resolve the problem. ■

# Take the Identity Theft Pop Quiz

Answer the following True or False questions to test your knowledge of identity theft and what to do if you fall victim. You'll find the answers on page 4.

1. _____ True or false? One of the best ways to protect your identity is by using online passwords only you would know—like your mother's maiden name or the last four digits of the Social Security Number.
2. _____ True or false? The best way to get a free copy of your credit report is to file a Freedom of Information Act (FOIA) Request.
3. _____ True or false? If someone has stolen information about your financial accounts, it's best to wait for several weeks to see what they do with it before taking any action.
4. _____ True or false? If the stolen information includes your driver's license or other government-issued ID, all you need to do is create a facsimile using a recent color photo.
5. _____ True or false? If the stolen information includes your Social Security Number, you can place an "initial fraud alert" by calling one of the three nationwide consumer reporting companies.
6. _____ True or false? Identity theft refers only to the theft of drivers' licenses or name badges.

# The First Steps to Take Should You Fall Victim to Identity Theft

If you become victimized by identity theft, take the following four steps as soon as possible, and keep a record with the details of your conversations and copies of all correspondence.

**1. Place a fraud alert on your credit reports, and review your credit reports.**

Fraud alerts can help prevent an identity thief from opening any more accounts in your name. Contact the toll-free fraud number of any of the three consumer reporting companies below to place a fraud alert on your credit report. You only need to contact one of the three companies to place an alert. The company you call is required to contact the other two, which will place an alert on their versions of your report, too.

**Equifax:** 1-800-525-6285; www.equifax.com; P.O. Box 740256, Atlanta, GA 30374-0241

**Experian:** 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013

**TransUnion:** 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834

**2. Close the accounts that you know, or believe, have been tampered with or opened fraudulently.**

Call and speak with someone in the security or fraud department of each company. Follow up in writing, and include copies (NOT originals) of supporting documents. It's important to notify credit card companies and banks in writing. Send your letters by certified mail, return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures.

When you open new accounts, use new Personal Identification Numbers (PINs) and passwords. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your Social Security number or your phone number, or a series of consecutive numbers.

If the identity thief has made charges or debits on your accounts, or on fraudulently opened accounts, ask the company for the forms to dispute those transactions.

**3. File a report with your local police or the police in the community where the identity theft took place.**

Then, get a copy of the police report or at the very least, the number of the report. It can help you deal with creditors who need proof of the crime. If the police are reluctant to take your report, ask to file a "Miscellaneous Incidents" report, or try another jurisdiction, like your state police. You also can check with your state Attorney General's office to find out if state law requires the police to take reports for identity theft. Check the Blue Pages of your telephone directory for the phone number or check www.naag.org for a list of state Attorneys General.

**4. File a complaint with the Federal Trade Commission.**

By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves and stop them. The FTC can refer victims' complaints to other government agencies and companies for further action, as well as investigate companies for violations of laws the agency enforces.

You can file a complaint with the FTC by calling the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261; or write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. ■

**Answers to the Identity Theft Pop Quiz:**
**1. False.** Crooks can often find this type of information about you—and then, it's "so long, identity!" It's better to use random numbers and letters, and commit them to memory. **2. False**. The Fair Credit Reporting Act allows you to ask for and receive one free credit report from each of the three nationwide credit reporting companies every 12 months. **3. False**. Your best first step is to contact your credit card companies and close your accounts. Also, talk with your bank about whether to close other accounts or take other steps. **4. False**. You should immediately contact the agency that issued the document, and follow its procedures to cancel the stolen document and get a replacement. **5. True.** Placing such an alert can help stop someone from opening new credit accounts in your name. **6. False.** While stealing drivers' licenses or name badges are types of identity theft, the term refers to a broad variety of criminal misuses of your name, Social Security Number, and financial information.

**Family Financial Education Foundation**
ACCESS EDUCATION SYSTEMS

724 Front Street, Suite 340
Evanston, WY 82930
(307) 789-2010, toll-free (888) 292-4333
www.accesseducation.org