FAMILY FINANCIAL EDUCATION FOUNDATION

DOLLARS & Sense

Family Financial Education Foundation

Edition 7, Volume 6

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;
- Rummage through your trash, 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.

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.

(Continued on page 2)

Identity Theft—Are You at Risk?

(Continued from page 1)

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" article.

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.

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 for 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.

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 2011. For the twelfth year in a row, identity theft complaints topped the list. Of more than 1.8 million complaints, 15% (279,156 complaints) were identity theft complaints. More than 27% this type of complaint was related to Government Documents or Benefits Fraud followed by credit card fraud (14%), phone or utility fraud (13%), bank fraud (9%), and employment fraud (8%). Other significant categories of identity theft reported by victims were loan fraud (3%) and Other (23%). In 2011, 12% of all identity theft complaints included more than one type. The states having the most Identity Theft Complaints per 100,000 population include Florida, Georgia, California, Arizona, and Texas.

"FTC Article: Fight back against Identity Theft.

(NAPS) Identity theft is a serious crime that costs American consumers billions of dollars and countless hours each year. It occurs when someone uses your personal information without your permission to commit fraud or other crimes.

While you can't entirely control whether you will become a victim, there are steps you can take to minimize your risk. The Federal Trade Commission (FTC), the nation's consumer protection agency, encourages consumers to Deter, Detect, and Defend to help cut down identity theft.

Deter

Deter identity thieves by safeguarding your information.

- Shred financial documents and paperwork with personal information before you discard them.
- Protect your Social Security number. Give it out only if absolutely necessary or ask to use another identifier.
- Don't give out personal information via the phone, mail or the internet unless you know who you are dealing with.

Detect

Detect suspicious activity by routinely monitoring your financial accounts and billing statements. Be alert to signs that require immediate attention, such as: bills that do not arrive as expected; unexpected credit cards or account statements; denials of credit for no apparent reason; and calls or letters about purchases you did not make.

Defend

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

1. Contact the fraud departments of any one of the three consumer reporting companies (Equifax, Experian, TransUnion) to place a fraud alert on your credit report. The fraud alert tells creditors to contact you before opening any new accounts or making any changes to your existing accounts. You only need to contact one of the three companies to place an alert.

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

3. File a report with your local police or the police in the community where the theft took place. Get a copy of the report or, at the very least, the number of the report, to submit to your creditors and others who 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 officials learn more about identity theft and the problems victims are having so that they can better assist you.

To learn more, visit ftc.gov/idtheft.

Used with permission from the FTC. "FTC Article: Fight back against Identity Theft. (ftc.gov/idtheft)

Identity Theft Checklist

1. Plan some time in your schedule to take care of the problem. The longer you wait the worse it can get

2. Alert your bank, the DMV and the credit bureaus. Cancel any credit cards and store cards you may have and put a temporary hold on all accounts. Make sure you also file a police report on the stolen items.

3. Go beyond the obvious. What other items were stolen that thieves could use? House and car keys, medical insurance card, club memberships, online passwords, phone numbers that could be used to run up charges.

4. Monitor the situation. Make regular calls to financial organizations and review your credit report. This is a good time to invest in a credit monitoring program.

Tip: Make a copy of all cards and other contents in your wallet and numbers to call for cancellation. Only carry what you need to in your wallet, and leave your Social Security card in a safe place at home.

Disposing of Your Old Home Computer

Your home computer may hold a lot of personal and financial information about your family such as passwords, account numbers, license keys or registration numbers for software, phone numbers, addresses, tax returns, etc. If you are planning on getting rid of your old computer, save the files you want to keep to a USB, CDRom, a new computer, etc. and then make sure that you either physically destroy your hard drive or use a program that overwrites or wipes the hard drive many times. You can dispose of your computer by recycling, donating, or reselling it. Remember, that most computers contain hazardous materials that should not be placed in a landfill. Check with your local health and sanitation agencies for ways to dispose of electronics safely.

ARTICLES

TIPS & TRICKS

Protecting Your Child's Personal information at School

NAPS) – During the school year, parents are asked to sign many forms. In the wrong hands, the personal information on these forms can be used to commit fraud in your child's name—to apply for government benefits, open bank and credit card accounts, apply for a loan or rent a place to live.

The Federal Trade Commission (FTC), the nation's consumer protection agency, cautions that when children are victims of identity theft, the crime may go undetected for years.

There are laws that help safeguard your child's and your family's personal information. For example, the federal Family Educational Rights and Privacy Act (FERPA), enforced by the U.S. Department of Education, protects the privacy of student records. It also gives parents the right to opt out of sharing contact information with third parties, including other families.

If your child is enrolled in school, the FTC suggests that you:

- Find out who has access to your child's personal information, and verify that the records are kept in a secure location.
- Pay attention to materials sent home asking for personal information. Before you reveal information about your child, find out how it will be used, whether it will be shared and with whom.
- Read the notice schools must distribute that explains your rights under the FERPA.
- Ask your child's school about is directory information policy. FERPA requires schools to notify parents and guardians about their school directory policy, and gives you the right to opt out of the release of directory information to third parties.
- Ask for a copy of your school's policy on surveys. The Protection of Pupil Rights Amendment (PPRA) gives you the right to see such materials before they are distributed to students.
- Take action if your child's school experiences a data breach. Contact the school to learn more. Talk with teachers, staff, or administrators about the incident and their practices. Keep a written record of your conversations. Write a letter to the appropriate administrator, and to the school board, if necessary. The U.S. Department of Education takes complaints about these incidents. Contact the Family Policy Compliance Office, U.S. Department of Education, 400 Maryland Ave., SW, Washington, DC 20202-5920 and keep a copy for your records.

To learn more about FERPA and PPRA, visit www2.ed.gov/policy/gen/guid/fpco/index.html. For information about identity theft, visit ftc.gov/idtheft. To file a complaint or get free information on consumer issues, visit ftc.gov or call toll-free, (877) FTC-HELP (1-877-382-4357). Watch a video, "How to File a Complaint," at ftc.gov/video to learn more.

Used with permission from the FTC. "FTC Article: Fight back against Identity Theft. (ftc.gov/idtheft)

Find more ways to protect your identity on our web site, FFEF.org

Do you have concerns about identity theft and how to protect yourself and your family? FFEF has all of the information and tools to help you review your credit report.

Don't forget to share your wealth of knowledge with friends and family. Our budget planning programs and credit counseling are available to everyone. Call today for more information.

www.ffef.org
www.accesseducation.org

(877) 789-4175

Business Hours!

Monday-Friday: 7:00 a.m.-7:00 p.m.
Saturday: 8:00 a.m.-12:00 noon

Family Financial Education Foundation

ACCESS EDUCATION SYSTEMS
724 Front Street, Suite 340
Evanston, WY 82930
contact: (877) 789-4175
www.ffef.org | info@ffef.org

If you know of someone who would benefit from this information, please pass this newsletter along.