

Identity Theft



By: Mark Larsen

Department of Homeland Security-Operation Security Program
DHS-OPSEC

Identity theft is the fastest growing crime in America. According to a study commissioned by the Federal Trade Commission over 9.9 million Americans learned they'd been victims of identity theft, at a total cost of nearly \$50 billion-an average of almost \$5,000 per victim. Identity theft or identity fraud is the taking of a victim's identity to obtain credit and credit cards from banks and retailers, steal money from a victim's existing accounts, apply for loans, file for bankruptcy, rent an apartment, or obtain a job using the victim's name. Thousands of dollars can be stolen without the victim knowing about it for months or even years.

Imposters obtain your Social Security number, your birth date, and other identifying information such as your address and phone number. With this information and a fake driver's license, they can apply in person for instant credit or through the mail posing as you. Imposters often claim they have moved and provide their own addresses. Once the first account is opened, they can continue to add to their credibility.

They can get information from your doctor, lawyer, school, health insurance carrier, and many other places. Be careful what you throw in the trash. Information may be obtained from utility bills, credit card slips, and other documents.

For further information, visit the Federal Trade Commission's web site at <http://www.consumer.gov/idtheft/>

The Washington Post recently ran an article entitled "ID Theft Scam Hits D.C. Area Residents," regarding ChoicePoint, Inc. Here is a brief synopsis of that article.

ChoicePoint has evolved into an information giant that has more than 100,000 customers and over 19 billion records. Customers include many Fortune 500 companies, local, state, and federal law enforcement, and every major federal government agency. Currently, as many as 4,500 residents in the District, Maryland and Virginia were among 145,000 people whose names, addresses, Social Security numbers and, in some cases, credit files were electronically shipped to people posing as business officials. Investigators believe the number of victims will continue to rise as officials learn more about the scheme.

To control the damage to consumers, ChoicePoint will offer victims free credit reports and credit-monitoring services for the next year: ChoicePoint officials said they expect to finish sending out notices by the end of the week. For further information regarding ChoicePoint, visit their website at <http://www.choicepoint.com/>

To prevent identity theft from happening to you.....

Do not give out personal information over the phone, through the mail, or over the Internet unless you have initiated the contact or know with whom you're dealing. Identity thieves will pose as bank representatives, Internet service providers, and even government officials to get you to reveal identifying information.

Shred all documents, including pre- approved credit applications received in your name, insurance forms, bank checks and statements you are discarding, and other financial information.

Do not use your mother's maiden name, your birth date, the last four digits of your social security number, or a similar series as a password for anything.

Minimize the identification information and the number of cards you carry. Carry what you actually need. Do not carry your Social Security card, birth certificate, or passport, unless it is absolutely necessary.

Do not put your Social Security number on your checks or your credit receipts. If a business requests your Social Security number, give them an alternate number and explain why. If a government agency requests your Social Security number, there must be a privacy notice accompanying the request.

Do not put your telephone number on checks.

Be careful using ATMs and phone cards. Someone may look over your shoulder and read your pin numbers, thereby gaining access to your account. Be cognizant of persons around you that may have electronic or surveillance style equipment (e.g., cameras, cell phones etc.).

Make a list of all your credit card account numbers and bank account numbers with customer service phone numbers and keep it in a safe place.

Do not put your credit card number on the Internet unless it is encrypted on a secured site and you can positively identify the business that is receiving your personal information. When entering a secured site you will receive a pop up message, "You are about to view pages over a secure connection." You will see this message unless you have chosen not to get this message in the future. Additionally, the site address will begin with "https:" and you will see a locked padlock in the lower right hand corner of the monitor. Clicking on the padlock will provide you with the site certificate information.

Pay attention to your billing cycles. Follow up with creditors if bills do not arrive on time. A missing credit card bill could mean an identity thief has taken over your credit card account and changed your billing address.

Cancel all credit cards that you have not used in the last six months. Open credit is a prime target.

Order your credit report at least twice a year. Reports should be obtained from all three major sources.

Equifax
800-525-6285
P.O. Box 740241
Atlanta, GA 30374-0241
www.equifax.com

TransUnion -Fraud Victim Assistance Division
800-680-7289
P.O. Box 6790
Fullerton, CA 92864-6790
<http://www.transunion.com/>

Experian
888-397-3742
P.O. Box 9532 Allen, TX 75013
<http://www.experian.com/>

When you receive your credit reports, review them carefully. Look for inquiries you did not initiate, accounts you did not open, and unexplained debts on the accounts you did not open. If there are accounts or charges you did not authorize, immediately notify the credit bureau by telephone and in writing.

You should also confirm that information such as your Social Security number, address(es), first and last names, middle initial and employers are correct. Errors in this information are often the warning signs of identity theft, although some inaccuracies may be due to simple mistakes. If you discover inaccuracies in your report, you should also notify the credit bureau as soon as possible so the information can be investigated.

Finally, if you have discovered errors or suspicious activity on your credit report, you should consider immediately contacting any credit card companies with which you have accounts and inform them about the activity. You should make sure they have your correct information on file and that any changes to the account were made by you.

Correct all mistakes on your credit report in writing. Send the letters return receipt requested. Identify the problems item by item and attach to a copy of the credit report and send back to the credit-reporting agency. You should hear from the agency within 30 days.

For further information, go to <http://www.consumer.gov/idtheft/>.