

Barbara E. Kerr | PRESIDENT
 David A. Sanchez | VICE PRESIDENT
 Dean E. Vogel | SECRETARY-TREASURER
 Carolyn Doggett | EXECUTIVE DIRECTOR
 Carole Anne Luckenbach | MANAGER,
 RISK MANAGEMENT
 AND MEMBER BENEFITS

Produced for CTA members by CTA's Risk Management and Member Benefits Department.

*To order additional copies of this issue, or if you would like to submit a topic for consideration in a future issue, please contact:
 CTA Risk Management and Member Benefits Department
 P.O. Box 921
 Burlingame, CA 94011-0921
 or email: member_benefits@cta.org*

IN THIS ISSUE

Protecting Yourself Against Identity Theft	1
Adding Up The Losses	1
Common Ways To Commit Identity Theft	2
Identity Theft IQ Test - Are You At Risk For Identity Theft? Test Your "Identity Quotient"	2
How To Protect Yourself From Identity Theft	3
What To Do If You Are A Victim Of Identity Theft	4
Resources	4

PROTECTING YOURSELF AGAINST IDENTITY THEFT

Identity theft is a serious crime. It involves the theft and unlawful use of another person's personal data to commit fraud or deception, typically for monetary gain. In the last 5 years, 27.3 million people were victims of identity theft.

Adding Up the Losses

Identity theft inflicts substantial costs on individuals and businesses. This is illustrated below for the year ending April 2003.

- Average loss per victim of identity theft: \$4,800
- Average amount victims spent to resolve problems associated with identity theft: \$500
- Average amount of time spent by victims to clear up affairs: 30 hours
- Total annual cost of identity theft to victims: \$5 billion
- Average value of money or goods obtained by criminals using a victim's personal information : \$10,200
- Total annual loss to businesses, including financial institutions, from identity theft: \$48 billion

Source: Federal Trade Commission

This issue of the *Benefits Update* is intended to explain why you need to protect yourself from identity theft, provide you with prevention tips as well as offer guidance regarding your course of action in the event that you become a victim of identity theft.

With the advent of the Internet and advanced communications technology, identity thieves have become more sophisticated in gathering personal data about you. Still, many consumers become victims of identity theft simply because of a lack of awareness. For example, how many times have you given your driver's license number, date of birth, or even your Social Security number, merely because a person asked? Many people provide personal information without thinking twice, totally unaware of the damaging consequences of such action.

When an identity thief obtains personal data about you, especially your Social Security number, your bank account or credit card number, and other valuable personal information, that person becomes equipped with the perfect tools to personally profit at your expense. Many people have reported that unauthorized persons have taken funds out of their bank accounts and used their credit cards to run up vast debts. What is even worse than the monetary loss is the fact that thieves can use your identity to commit criminal actions.

In response to the growing number of identity theft victims, Congress, in 1998, passed the Identity Theft and Assumption Deterrence Act. This legislation treated identity theft as a felony, which carries a maximum term of 15 years imprisonment, a fine and criminal forfeiture of any personal property used to commit the offense.

Common Ways to Commit Identity Theft

There are many ways to commit identity theft and many people do not realize how their behaviors make them easy prey.

- In public places, criminals scout their victims by listening in on your conversations as you provide credit card information to hotel or rental car companies.
- Closer to home, criminals may search your trash and retrieve discarded "pre-approved" credit card offers and try to activate them for their use.
- If you are a regular Internet user, you need to know that the Internet has become a haven for identity thieves to obtain personal data, such as passwords or even banking information. The next time you respond to "spam" or unsolicited e-mail, be aware that thieves could be sending these "spam" with the intention of obtaining personal data about you for fraudulent use.

Identity Theft IQ Test - Are You at Risk for Identity Theft? Test Your "Identity" Quotient**

Many people engage in activities that could potentially make them victims of identity theft. To determine your potential, take the test below and rate your answers as instructed. Add your score and determine if you are vulnerable to identity theft.

- _____ I receive several credit card pre-approved offers every week. (5 points)
- _____ Add 5 points if you do not shred them before putting them in the trash.
- _____ I carry my Social Security card in my wallet. (10 points)
- _____ I do not have a locked, secured mailbox. (5 points)
- _____ I use an unlocked, open box at work or at my home to drop off my outgoing mail. (10 points)
- _____ I carry my military ID in my wallet at all times. (10 points)
- _____ I do not shred or tear banking and credit information when I throw it in the trash. (10 points)
- _____ I provide my Social Security number (SSN) whenever asked, without asking questions as to how that information will be safeguarded. (10 points)
- _____ Add 5 points if you provide your SSN verbally without checking to see who might be listening
- _____ I am required to use my SSN at work as an employee ID. (5 points)
- _____ My SSN is printed on my employee badge that I wear at work or in public, or it is posted on other documents frequently seen by others in my workplace. (10 points)
- _____ I have my SSN and/or driver's license number printed on my personal checks. (10 points)
- _____ I am listed in a "Who's Who" guide. (5 points)
- _____ I carry my insurance card in my wallet with my SSN printed or that of my spouse. (10 points)
- _____ I have not ordered a copy of my credit reports for at least 2 years. (20 points)
- _____ I do not believe that people would dig in my trash looking for credit or financial information or look for documents containing my SSN. (10 points)

Understanding Your Score:

- 100+ points Recent surveys indicate that 7-10 million people were victims of identity theft last year. You are at HIGH RISK. It is recommended that you purchase a paper shredder, become more security-aware in document handling and start to question why people need your personal data.
- 50 - 100 points Your odds of being victimized are about average; higher if you have good credit.
- 0 - 50 points Congratulations. You have a high identity theft "IQ". Keep up the good work and do not let your guard down.

*Reprinted with permission from the Privacy Rights Clearinghouse.

How To Protect Yourself From Identity Theft

In spite of various innovative ways identity thieves use to illegally obtain personal information about you, there are, in turn, many proactive steps consumers can take to prevent the theft of personal data. Here are some suggestions:

Do not release your personal information on the phone, through the mail or the Internet unless you have initiated the call or inquiry and that you are confident that you have a trusted business relationship with that organization.

Be especially careful about releasing your Social Security number. Your Social Security number is the key to your credit and banking accounts and is the prime target of criminals.

If you do not have a secured mailbox at your residence, think about installing one in order to deter mail theft. When you are away from home for an extended amount of time, have the post office hold your mail or ask someone you trust to collect and hold the mail while you are away.

Keep track of your monthly bill statements and review them thoroughly. Report any unauthorized charges to your credit card company promptly. In general, you are liable for no more than the first \$50 of the loss, and in many cases, you will not be required to pay any part of the loss. If you are not receiving monthly statements for any accounts you know you have and expect statements for, call the financial institution or credit card company immediately and ask why.

Shred mail containing pre-approved credit card offers and other sensitive information such as credit card receipts, bank and investment account statements. Shredders are available at many office supply stores. Consider a cross-cut shredder rather than a straight-cut shredder, which may leave some data readable. Shredders cost as low as \$15.

List or photocopy all your credit cards, bank accounts and investment accounts including the account number, expiration dates and telephone numbers of your banks and credit card providers. This way, in the event your wallet is stolen, you can contact the banks and credit card providers immediately.

Review your credit reports at least once per year from each of the three credit bureaus (Experian, Equifax and TransUnion). In November 2003, Congress approved a law that allows consumers to receive a free credit report from each of the three credit-monitoring agencies every 12 months. The free credits reports are available from the Annual Credit Report Request Service by visiting www.AnnualCreditReport.com or calling (877) 322-8228. Your credit report lists all bank and financial accounts under your name. Be sure to review the report thoroughly to ensure that any inactive accounts are in fact, inactive. If someone has used your identity, reviewing your credit report is one way to catch the theft early. Each credit bureau offers credit-monitoring services with an annual fee of approximately \$50-120. With this service, the credit bureau notifies you when there is any activity on your credit report, thus alerting you to possible fraud.

If you have a computer and use the Internet regularly, install a firewall on your computer to prevent hackers from obtaining personal information and financial data on your hard drive. This is especially important if you connect to the Internet via DSL or cable modem. Install a current version of virus protection software to prevent a "worm" or virus from collecting information from your computer.

When purchasing merchandise on the Internet, conduct business only with those merchants that provide transaction security protection and that have strong privacy and security policies. If in doubt, do not conduct a transaction with a suspicious company. It is not worth the risk.

Consider putting a fraud alert or security freeze on your credit file. A fraud alert places a statement on your credit file requesting creditors to call you before issuing credit. A fraud alert is normally in place only for a few months but you can request placement of a fraud alert for seven years by sending a written request to the three credit bureaus. A security freeze means that your credit file cannot be shared with potential creditors, insurance companies or employers, thus preventing thieves from

What To Do If You Are A Victim Of Identity Theft

In the event you become a victim of identity theft, you must begin a long and laborious process to correct your records. In order to prevent further damage to your credit and reputation, you must act quickly and assertively. Here are a few suggestions:

- **Law Enforcement** - Report the crime immediately to your local police. Get a copy of the police report and keep the name and phone number of the investigator handy. File a complaint with the Federal Trade Commission (FTC) by calling (877) ID THEFT. The FTC is responsible for receiving and processing complaints from victims of identity theft.
- **Credit Bureaus** - Immediately contact the fraud units of each of the three credit reporting agencies. Report that you are a victim of identity theft and ask that your file be flagged with a fraud alert as well as a "victim statement". A fraud alert is a signal to creditors to contact you before opening any new accounts or making a change to your existing accounts.
- **Creditors** - Contact by phone and in writing the credit grantors with whom your name has been used fraudulently. You may be asked to file an affidavit. Close any accounts that have been tampered with or opened fraudulently. Document all conversations diligently including the dates, contact names and a short summary of the discussion. Keep a log of time and expenses incurred in the event that you are able to secure restitution from the thief through a court judgment or conviction.
- **Debt Collectors** - It will be very likely that debt collectors or collection agencies will be contacting you for payment on your fraudulent accounts. If so, tell them that you are a victim of identity theft and are not responsible for payment of the fraudulent accounts. If requested, complete the debt collector's affidavit. Follow up with the debt collector in writing that you have been a victim of identity theft and ask them to confirm in writing that you do not owe the debt. Send all correspondence by certified mail, return receipt requested.
- **Stolen Checks and ATM checks** - In the event that your bank checks or ATM cards have been stolen, report it to the issuing banks immediately and request a fraud affidavit. Get a new card, account number and password. When creating passwords, do not use words or numbers that could be easily guessed such as your maiden name, last four digits of your Social Security number or birth date. Use a combination of words and letters and never write your password down - commit it to memory.
- **Legal Assistance** - Consult an attorney if credit grantors, debt collectors and/or credit bureaus are not cooperative in removing fraudulent entries in your credit report.

Resources

As a first step in preventing identity theft, request a free copy of your credit report from the following credit monitoring agencies. Since you are entitled to a free copy every 12 months, stagger your requests so that you obtain copies of your credit report every four months.

Name	Address	Phone	Web Site Address
Equifax	P. O. Box 105069, Atlanta, GA 30348	(800) 685-1111	www.equifax.com
Experian (formerly TRW)	P. O. Box 9532, Allen, TX 75013	(888) EXPERIAN	www.experian.com
TransUnion	P. O. Box 6790, Fullerton, CA 92834	(800) 888-4213	www.transunion.com
Annual Credit Report Request Service	P.O. Box 105283, Atlanta, GA 30348	(877) 322-8228	www.AnnualCreditReport.com

There is a wealth of resources available on identity theft. Listed below are useful resources provided by various non-profit organizations.

Name	Phone	Web Site Address
Federal Trade Commission	(877) 438-4338	www.consumer.gov/idtheft
Privacy Rights Clearinghouse	(619) 298-3396	www.privacyrights.org
Identity Theft Resource Center	(858) 693-7935	www.idtheftcenter.org
California Office of Privacy Protection	(866) 785-9663	www.privacy.ca.gov
FBI Internet Fraud Complaint Center	N/A	www.ifccfbi.gov
U.S. Department of Justice, Identity Theft	N/A	www.usdoj.gov/criminal/fraud/idtheft.html
Identity Theft Survival Kit	(800) 725-0807	www.identitytheft.org
California Senate (for legislative information on identity theft)		www.leginfo.ca.gov/calaw.html.