Protecting Yourself from Identity Theft

All information was acquired from the United States Trade Commission

Technological advances in the 1990s gave rise to a new type of theft: identity theft.

WHAT IS IDENTITY THEFT?
Identity theft occurs when an unauthorized individual acquires some of your personal information -- your bank and/or credit card numbers, your income, your social security number, or even something as simple as your name, address, and telephone numbers -- and uses it to commit fraud or theft.

Specifically, the Identity Theft and Assumption Deterrence Act of 1998 makes it a federal crime when someone "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law."

According to Bankrate.com, in 2001 there were approximately 500,000 identity theft victims. Identity theft cost banks and credit-card companies about $5 billion and the average consumer spent $1,375 and 175 hours cleaning up their credit card reports.

HOW DO IDENTITY THIEVES GET MY INFORMATION?
Identity thieves may use a variety of methods to secure personal information about another individual, including:

- Stealing wallets and purses containing your identification and credit and bank cards.
- Stealing your mail, including your bank and credit card statements, pre-approved credit offers, telephone calling cards and tax information.
- Completing a "change of address form" to divert your mail to another location.
- Rummaging through your trash, or the trash of businesses, for personal data in a practice known as "dumpster diving."
- They fraudulently obtain your credit report by posing as a landlord, employer or someone else who may have a legitimate need for -- and a legal right to -- the information.
- Obtaining your business or personnel records at work or in your home.
- Using personal information you share on the Internet.
• Buying your personal information from "inside" sources. For example, an identity thief may pay a store employee for information about you that appears on an application for goods, services or credit.

HOW DO IDENTITY THIEVES USE MY INFORMATION?

• They call your credit card issuer and, pretending to be you, ask to change the mailing address on your credit card account. The imposter then runs up charges on your account. Because your bills are being sent to the new address, it may take some time before you realize there's a problem.
• They open a new credit card account, using your name, date of birth and SSN. When they use the credit card and don't pay the bills, the delinquent account is reported on your credit report.
• They establish phone or wireless service in your name.
• They open a bank account in your name and write bad checks on that account.
• They file for bankruptcy under your name to avoid paying debts they've incurred under your name, or to avoid eviction.
• They counterfeit checks or debit cards, and drain your bank account.
• They buy cars by taking out auto loans in your name.
• They give your name to the police during an arrest. If they're released from police custody but don't show up for their court date, an arrest warrant is issued in your name.

WHAT IS THE IMPACT OF IDENTITY THEFT ON THE VICTIM?
Victims could be refused loan (car, housing, education) and employment opportunities, be denied credit cards, or be arrested for crimes they did not commit -- these incidents may be the first clue that you've become a victim.

HOW CAN I PROTECT MYSELF FROM IDENTITY THEFT?
Manage your personal information cautiously and wisely by taking the following steps:

• Order a copy of your credit report from each of the three major credit bureaus once a year. By checking your report on a regular basis you can catch mistakes and fraud before they wreak havoc on your personal finances.
• Pay attention to your billing cycles. Follow up with creditors if your bills don't arrive on time. A missing credit card bill could mean an identity thief has taken over your account and changed your billing address to cover his tracks.
• Don't give out personal information on the phone, through the mail or over the Internet unless you've initiated the contact or are sure you know who you're dealing with. Identity thieves may pose as representatives of banks, Internet service providers (ISPs) and even government agencies to get you to reveal your SSN, mother's maiden name, account numbers and other identifying information.
• Place passwords on your credit card, bank and phone accounts. Avoid using easily available information like 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.
• Secure personal information in your home, especially if you have roommates, employ outside help or are having service work done in your home.
• Carry only the identification information and the number of credit and debit cards that you'll actually need.
• Don't carry your SSN card; leave it in a secure place.
• Ask about information security procedures in your workplace. Find out who has access to your personal information and verify that records are kept in a secure location. Ask about the disposal procedures for those records as well.
• Deposit outgoing mail in post office collection boxes or at your local post office, rather than in an unsecured mailbox. Promptly remove mail from your mailbox. If you're planning to be away from home and can't pick up your mail, call the U.S. Postal Service at 1-800-275-8777 to request a vacation hold.
• To thwart an identity thief who may pick through your trash or recycling bins to capture your personal information, tare or shred your charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards that you're discarding, and credit offers you get in the mail.
• The next time you order checks, omit your first name and have only your first initials and last name on them. If someone takes your checkbook, they will not know if you sign your checks with just your initials or your first name, but your bank will know how you sign your checks. Also, NEVER put your social security number on your checks.
• When you are writing checks to pay on your credit card accounts, DO NOT put the complete account number on the "For" line. Instead, just put the last four digits. The credit card company knows the rest of the numbers and anyone who might be handling your check as it passes through all of the check processing channels will not have access to it.
• Keep your purse or wallet in a safe place at work.

WHAT CAN I DO IF I SUSPECT I AM A VICTIM OF IDENTITY THEFT?
The U.S. Federal Trade Commission has set out the following steps to take if you suspect you are a victim of identity theft.

Contact the fraud departments of each of the three major credit bureaus, report the theft, and ask that a "fraud alert" be placed on their file and that no new credit be granted without their approval.
Equifax: 1.800.525.6285
Social Security Admin. Fraud Line: 1.800.269.0271
Experian (formerly TRW): 1.888.397.3742
Trans Union: 1.800.680.7289
1. For any accounts that have been fraudulently accessed or opened, contact the security departments of the appropriate creditors or financial institutions. Close these accounts. Put passwords (not mother's maiden name or Social Security number) on any new accounts they open.

2. File a report with local police or the police where the identity theft took place. Get the report number or a copy of the report in case the bank, Credit Card Company or others need proof of the crime later.

3. Call the ID Theft Clearinghouse toll-free at 1.877.ID.THEFT (1.877.438.4338) to report the theft. Counselors will take their complaint and advise them on how to deal with the credit-related problems that could result from ID theft. The Identity Theft Hotline and the ID Theft Website (http://www.ftc.gov/bcp/edu/microsites/idtheft/) give consumer's one place to report the theft to the federal government and receive helpful information.