THE FASTEST GROWING CRIME IN AMERICA!

Identity theft is on the rise, affecting almost 10 million victims in 2008 (22% increase from 2007), and continued to rise in 2009. Driving that increase was new accounts fraud, which showed longer periods of misuse prior to detection.

WHAT IS IDENTITY THEFT?

Identity theft occurs when a person unlawfully obtains and uses the identity of another person to commit a fraud, theft or deception. By wrongfully acquiring another's personal data such as social security number, mother's maiden name, bank account number or credit card number, identity thieves can perform many acts, most commonly opening bank or credit card accounts in the victim's name. Identity thieves are both creative and bold . . . they have even secured auto loans in the victim's name.

Identity theft is usually perpetrated for economic gain, but there are many other reasons for committing the crime. For example, there are cases where thieves have provided the victim's identity to the police during an arrest. When the identity thief was released from police custody, and did not show up for a court date, an arrest warrant was issued in the victim's name. There are even cases where the victim was actually arrested in his/her place of employment.

But the most common identity theft problem involving financial losses has resulted from intercepted unsecure on-line communications using sensitive information such as your credit card number. The thieves then call your credit card issuer and, pretending to be you, ask to change the mailing address on your credit card account. The identity thief then makes purchases as well as large cash advances on your account. Because your bills are being sent to the new address, it may take some time before you realize there is a problem.

HOW IDENTITY THIEVES GET YOUR PERSONAL INFORMATION

All an identity thief needs to open a new credit card account is your name, date of birth and Social Security Number . . . information easily found in junk mail you have tossed in the garbage or in e-mails abandoned on servers. Identity thieves are always coming up with new ways to gather information they are not supposed to have, but typically:

- They steal wallets containing your identification, credit cards and bank cards.
- They steal your mail, including your bank and credit card statements, pre-approved credit offers, new checks, and tax information.
- They file a "change of address form" to divert your mail to another location.
- They find personal information in your home or in your trash.
- They steal files out of offices where you are a customer, patient or student.
- They listen in on your conversation if you give your credit card number over the telephone when placing an order.
- They get your information from the personnel files in the workplace.
- They **"hack"** into electronic files kept by your healthcare providers, banks, health clubs, universities . . . just think of all the institutions that have your private information.

MINIMIZE YOUR RISKS

First of all and most importantly, be very careful who you give information to, and NEVER EVER share your password. Your bank, hospital or any other institution will NEVER ask you for your computer or online password. No legitimate company will EVER send you an e-mail asking you to verify account information. Become aware of current scam techniques such as phishing. Follow good password practices and never use your network login password for any other system or website.

You should ALWAYS look at the "URL" or website address on your browser. When you must give sensitive information over the internet, check the URL to be sure there is a 'HTTPS' at the beginning of it. Then, go to File: Properties. Be sure the web address listed there is the same as the web address on your browser. Beyond that:

- Always shred bank statements, credit card statements, pay stubs, insurance claim or payment forms, and other financial documents and credit reports before throwing them away. Most identity thieves find the information they need to perpetrate crimes by going through people's trash.
- Regularly review your bank, credit card, and phone statements for accuracy.
- Be wary of anyone calling to "confirm" personal information. Ask to call them back at their legitimate telephone number.
- Eliminate pre-approved offers of credit . . . opt-out of pre-approved credit offers by calling (888) 5-OPT-OUT.
- At least once a year, order a copy of your credit report from each of the three credit bureaus. To order your report online, visit the Web sites of the three major credit bureaus:
    - Experian (www.experian.com) / (888) 397-3742
    - Equifax (www.equifax.com) / (800) 525-6285
    - TransUnion (www.tuc.com) / (800) 680-7289

  Add a statement to your credit file that prohibits the granting of credit without calling you to confirm the application. This may thwart identity thieves' attempts to access your credit history and purchase goods at various retail establishments that grant credit on-site.
- Reduce the number of credit cards you carry. Keep good records of all your credit cards and the phone numbers to call in the event you lose one. Sign your new credit cards - before someone else does!
- Write "Always check ID" in black marker on the back of your credit card. This encourages retail clerks to ask for your ID any time that credit card is used, and may deter a potential thief from using the card.
- Do not provide credit card information over the telephone.
- Refrain from discussing financial matters on wireless or cellular phones.
- Remove your Social Security Number from your checks, driver's license, or other forms of ID.
- Send mail in U.S. Postal Service collection boxes rather than in unsecured mailboxes.
- Remove Social Security and other unnecessary identifying information from your wallet or purse.
- Arrange for somebody to pick up your mail when you are going to be gone for more than a few days.
- Never leave receipts behind at ATM machines, bank counters or gasoline pumps.
- Watch anyone who asks to "swipe" your credit or debit card. Devices known as "skimmers" are sometimes used by counterpersons to copy the identifying information off a magnetic strip of a credit or debit card and later added to a fake card with a blank magnetic strip.

IF YOU BECOME A VICTIM

- Immediately call all credit card issuers and let them know you have been a victim of identity theft. Request your old cards be cancelled, your old accounts closed and new cards and accounts opened immediately. Determine if any charges on these accounts need to be disputed and begin that process.
- Immediately contact your local police department and file a report. Including a copy of your police report in correspondence with financial and credit processing institutions adds legitimacy to your communications and can speed up the process of absolving you of wrongful debts or removing inaccurate information from your credit reports.
- Fill out an ID Theft Affidavit. To get a blank copy of the affidavit, visit the ID Theft website at www.consumer.gov/idtheft or call 1-877-IDTHEFT. You can use this form to report information to many different organizations, thus simplifying the process of disputing charges with companies where a new account was opened in your name.
- Contact the fraud department (by phone and in writing) at each creditor, bank or utility/service that provided the identity thief with unauthorized credit, goods or services. Request copies of all application documents the identity thief filed with that credit grantor. Begin the dispute process.
- Report identity theft to one of the major credit bureaus listed above. You only need to report to one of them as they now share a common database. Send a written request to place a "Fraud Alert" notification in your credit file. Include a copy of one of your utility bills and a copy of your driver's license for this purpose. Request either a freeze of your credit report (renewable for 90 days).
- Contact the Federal Trade Commission's Identity Theft Hotline at (877) 438-4338. Counselors will take your complaint and help you resolve financial and other problems that can result from the crime.
- Contact the Social Security Administration at (800) 269-0271 if you suspect fraudulent use of your Social Security Number. Visit www.ssa.gov.
- Contact your local Postal Inspection Service office if you suspect that someone has used your mail to steal your identity. Visit www.usps.com/postalinspectors to find the local office.
- Document all correspondence with the police department, credit grantors and credit reporting agencies.
- Keep copies of all your correspondence. Use this to create a quick summary report that you can give to future creditors as you explain your situation when trying to secure new credit.
- When the thief who stole your identity is arrested, engage in regular contact with your local district attorney and ask for information about the case. Keep documentation pertinent to the case to help prove your position in ongoing disputes.
- If your case is not resolved to your satisfaction, contact the Federal Trade Commission by filling out a complaint on their Web site: www.ftc.gov.

Keep Your Identity Secure!