Identity Theft: What Can I Do?

Past or Potential Victim: Learn How to Protect Yourself

If you think your identity may have been stolen one of the first things that may cross your mind is, "How did someone get my personal information?"

Although companies have an obligation to do their best to keep your information confidential, accidents do happen. Sometimes it occurs via an accidental disclosure from an institution that has your information, such as a financial center or data resource center, that unfortunately ends up in the hands of a criminal. Other times it is deliberately stolen.

Stolen information can be obtained via an intrusion into a company's customer information through computer hacking; dishonest employee assistance; mail theft (including pre-approved credit card offers and mortgage documents); credit card "skimming" (the use of a "look- alike" card-swiping machine that fits seamlessly over the real ATM card reader and records your card's information for the thief); and SPAM schemes in the form of "Phishing" (telephone fraud and bank fraud carried out through email).

IMPORTANT FIRST STEPS: INITIALIZING A FRAUD ALERT, CLOSING ACCOUNTS, FILING A COMPLAINT

If the stolen information includes your social security number, or if you are unsure exactly what information has been stolen, call any one of the three credit reporting agencies immediately and place an initial fraud alert on your credit report. A fraud alert can help stop someone from opening new accounts in your name by ensuring that you are contacted by phone for verification and confirmation prior to each new account opening.

The contact information for the three main credit reporting agencies is:

Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241

Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 2002, Allen, TX 75013

TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

It is important to close any compromised credit card accounts and to consult with your financial institution about changing your passwords on your accounts. Ask your financial insitution to monitor your accounts with them for possible fraud. Place unique and different passwords on any new accounts that you open.

Depending on the nature of the crimes committed under your identity, file a report with your local police, the Internet Crime Complaint Center (IC3) or the Federal Trade Commission (FTC).

IC3 works to address crime committed over the internet and provides a convenient and easy method to alert authorities of suspected violations. It also serves as a central repository for law enforcement and regulatory officials that allows more easily networked and shared data, including statistical data and current trends. Visit the IC3 website at www.ic3.gov for more information or to file a complaint online. You can also file a complaint by phone by dialing the toll free complaint line at (800) 251-7581.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad. For more information about the FTC, visit www.ftc.gov or call toll free: (877) FTC-HELP (382-4357).

It is very important to continue to read your financial account statements carefully and monitor your credit reports every few months in the first year of the theft, and at least once a year with each of the three major credit reporting agencies thereafter .

MOVING FORWARD WITH PROACTIVE PREVENTION

Although consumers may never be able to completely protect themselves from being a victim of this theft, there are protective measures you can and should take to decrease your likelihood of becoming a victim...

BE AWARE OF THE STATUS OF YOUR CREDIT REPORT

One of the most important measures to take in spotting identity theft is to be aware of your credit report. Check it often and, at the very least, once a year. The western two-thirds of the U.S. population are now able to do this for free with all three major credit

reporting agencies simultaneously by visiting the website www.annualcreditreport.com. By September 2005, the entire U.S. will be eligible for this free service. If anything appears fraudulent or counterfactual, call the reporting agency immediately to put an initial fraud alert on your report. This alert will remain on your credit for 90 days and will prevent anyone else from opening a new account in your name unless it is verified by you over the phone.

WATCH FOR SIGNS

In addition to keeping an eye on your credit report, watch for these other signs that your information is being misused: missing bills or other mail, receiving credit cards you did not apply for, being denied credit or receiving unfavorable terms for no apparent reason, and receiving phone calls from bill collectors or businesses regarding products or services you did not purchase.

USE PASSWORDS ONLY YOU WILL KNOW

Although it has been said many times, it bears repeating: Do not use your mother's maiden name, your birth date, the last four digits of your Social Security number (SSN) or your phone number, or a series of consecutive numbers as your password for any account you open or maintain.

This type of information is typically what identifies you with your credit and financial centers, and also - as stated earlier - where your information can sometimes be accidentally put in to the wrong hands.

Finally, if you have information about an identity theft incident or criminal activity and wish to submit a tip, please help officials in the fight against identity theft by visiting www.fbi.gov and clicking on the "Submit a Tip" link.

Resource: *Reprint of this article authorized by the National White Collar Crime Center (NW3C). The article appeared in the NW3C magazine "Informant" Vol.1, No.2, Jul-Oct 2005.*