

Identity crisis: Has your name been stolen?

Identity theft—the unauthorized use of an individual’s name or personal information to obtain money or credit—is the fastest-growing white-collar crime. The “e-world” of buying and selling by using phones, faxes and computers in various combinations offers opportunities to cybercrooks on a vastly expanded scale compared to the purse snatchers and pickpockets of the past—or present. The more involved one is in this world—say as a busy executive, professional, entrepreneur or investor—the more opportunities for today’s clever thieves, if proper precautions are not taken. Consider some recent incidents:

- A man had more than \$287,000 taken from his online brokerage account by a thief working with a woman who had access to confidential employee information at the man’s workplace. Over 100 other people also were victimized by this pair.

- Several people acquired the names and Social Security numbers of high-ranking active-duty and retired military officers through a public Internet Web site and obtained credit cards and bank and corporate credit in the officers’ names.

- Using Web-enabled cell phones, a public library’s computer, business magazines with information about tycoons, and a knack for guessing passwords, a busboy broke into accounts of 217 of the richest people in America. He was caught only when he began to transfer \$10 million from one of those accounts to an offshore bank.

How can identity theft be combated? The U.S. Department of Justice suggests that a winning strategy involves steps summed up by the word “SCAM.”

S.C.A.M.

Stingy is the way to be with information about yourself. Never give out more than the bare minimum necessary for the transaction that you want to make—whether on your phone, on your computer, on your checks, on forms and applications, or in a place of business. Most especially, never give out your credit card number except to a trusted merchant or vendor when you have initiated the contact. Memorize information rather than carry it in your wallet or purse. Opt out of information sharing. Cover your hand movements at ATMs and public phones. Consider installing a locked mailbox or using a post office box. Do not let mail accumulate at home while you are away.

Check your financial information regularly and closely, looking both for what should be there and what should not be. If you do not receive your monthly bank or credit card account statement, or if something seems “off” about a statement, contact the financial institution immediately. Be vigilant about disputing anything strange. If you shop online, make sure that the Web site is secure and reliable. Make sure that either “https://” (note the “s”) appears in connection with the site or that a locked padlock icon appears on your Internet browser. Also make sure that the Web site advertises a physical business address, a customer service phone number and a privacy policy.

Ask periodically for a copy of your credit report. Three national bureaus--Equifax, Experian (formerly TRW) and Trans Union--collect financial information about you and disseminate it to anyone with a “legitimate business

need.” You ought to see what’s in your reports in order to know who has been requesting data about you and whether any unauthorized transactions have been recorded. You also will have the opportunity to correct erroneous entries. You can obtain a copy of your report from each bureau for a small fee. You also can direct that your name be removed from their marketing lists, thereby limiting the number of preapproved credit card offers that you receive.

If you’ve had trouble—a stolen card, an unauthorized charge, a credit application in your name that you did not initiate—you can request a *fraud alert* on your account, requiring the bureaus to call you to verify all applications. Although you can report frauds by telephone, a written request establishes a record in case of later problems.

Maintain careful records of your banking and other financial accounts for at least a year, if not longer. And use a shredder for personal records before throwing them in the trash.

Your allies

If you think that you’ve become a victim of identity theft or fraud, act *immediately* to minimize the damage to your personal funds and financial accounts, as well as your reputation and credit standing. Here are some allies in that effort that you should contact: your financial institution, the fraud units of the principal credit agencies, your local police or the police in the community where the identity theft took place, the Federal Trade Commission, and—possibly, depending on the situation--the Better Business Bureau, the Postal Inspection Service, the Social Security Administration, the Internal Revenue Service. Also contact relevant creditors concerning any accounts that have been tampered with or opened fraudulently. Follow up telephone calls with letters.

If you take these steps, you’ll have a fighting chance against those who would steal your good name.

© 2007 M.A. Co. All rights reserved.

Any developments occurring after January 15, 2007, are not reflected in this article.