

## The Basics

### Protect yourself from identity theft

By [Susan Okula](#)

Although it's well over a billion-dollar-a-year racket, most people don't lose any sleep over credit card fraud.

If bogus charges show up on your bill, or if your card is lost or stolen, you simply call the credit card issuer. Getting things straightened out takes a little time, but usually it doesn't cost you anything. Visa or MasterCard or American Express eats the losses -- not you, the customer.

Of course, we all ultimately pay for credit card fraud -- it's part of the reason for those sky-high interest rates. But as long as you check your statements, you're not going to be personally hurt by a credit thief. Right?

Wrong.

Two types of credit fraud can hit individuals very hard. The first is debit-card theft, which takes a direct hit on your bank account, and not on the hefty coffers of Visa or MasterCard.

The second, and most serious, is outright identity theft. A swindler assumes your credit identity and embarks on a spree that can last for years, even decades.

#### Living large on your good name

Last August, Marvin Young Jr. of Oakland, Calif., received a letter from Sears, Roebuck & Co., denying his credit application. The only trouble was that Young had not applied for a Sears card. Sensing trouble, Young obtained a copy of his credit report and found that more than 30 new credit cards had been issued in his name in the previous 90 days. "I almost had a heart attack," says Young, who hadn't asked for any of those accounts.

He had a pretty good idea of who did open those accounts, however. In 1990, a former roommate had obtained Young's Social Security number and birth date and subsequently opened a checking account, a business and at least one credit account in Young's name.

Apparently, the warning Young placed on his credit report seven years ago expired. Now he is busy supplying stores such as Bloomingdale's and J.C. Penney with notarized affidavits to prove he is not responsible for the thousands of dollars in bills charged by the impostor.

What's most infuriating is that Young, like all identity-theft victims, has to notify every single credit issuer of the fraud. That one mistake by the credit bureau can take years to untangle. "It's not easy when someone takes over your life like this," Young says, a common lament of victims of identity theft.

No agency keeps statistics on identity theft, but law enforcement agencies agree the problem is growing, with thousands of new cases being reported each month. MasterCard reported that credit card losses from identity theft in 1996 were four times greater than in 1995; Visa doesn't keep such statistics. However, the Federal Reserve Board reported to Congress in March 1997 that, overall, identity theft losses to the U.S. financial system are comparatively small. Of course the Fed, like most of America, has a major stake in easy credit. But if Fed Chairman Alan Greenspan is ever victimized, we wonder what the official reaction would be.

### **Names in the trash**

Make no mistake: An identity thief can ruin your life. Thieves, who may work individually or as part of large international crime rings, obtain identifying information about their victims in many ways, says Beth Givens, director of the Privacy Rights Clearinghouse, a nonprofit consumer information and advocacy program in San Diego.

They may be roommates, relatives, friends, estranged spouses or household workers with ready access to their victims' personal papers. Or they get the information by stealing a wallet or a purse, going through your trash and picking out financial statements or credit card slips, or taking your mail. Sometimes they even switch the addresses of victims to their own post office boxes and wait for the credit applications and card renewals to come to them.

They also get essential information -- including the quality of prospective victims' credit -- by illegally accessing the huge databases of the three credit reporting bureaus. All have thousands of computer terminals in places like car dealerships or real estate agencies. They can shop for victims at will.

They can also get information through your employer. "We learned of a case where a member of a Nigerian crime ring was employed temporarily at a very large corporation," Givens says. "He downloaded the employee list containing Social Security numbers and then one by one the employees' identities were used for fraudulent purchases."

Identity thieves can even photocopy your vital credit information legally at the local courthouse, says Joseph Seanor, a private investigator in Alexandria, Va. If you've been divorced, the transcripts of your case, including the financial and credit account information you divulged as part of the proceedings, as well as your Social Security number, are part of the public record. "Why go dumpster diving?" asks Seanor.

### **Finding victims through the Internet**

The Internet provides another opportunity for identity thieves to glean personal information, Seanor says. Thieves can design very official-looking e-mail messages that imply they are from a major company, and successfully obtain personal information from trusting individuals.

Once the crooks have some of your personal information, they can start applying for credit cards in your name, often giving an address that is different from yours. Sloppy credit-granting procedures give thieves plenty of opportunities. "A lot of credit granters are not checking records," Givens says. "They are more interested in new applicants than in verifying the authenticity of the applicants."

Identity thieves may buy a car or rent an apartment in your name. Some may even commit crimes in your name. Givens relates one case where the impostor was a major drug dealer using the identity of a highly ranked corporate executive. When traveling overseas, the executive has to carry an official letter that explains he is not the drug dealer. Still, cops recently broke into the man's house and into his bedroom with guns drawn.

While this is an extreme case, many identity theft victims have been denied student loans, mortgages, credit accounts and even jobs. Some wrongly have had their telephone service disconnected and their driver's licenses suspended, or been harassed by collection agencies.

The sad part is, it is next to impossible to stop a determined identity thief. Who is going to apprehend him?

Occasionally law enforcement agencies, including the Secret Service, bust up identity theft crime rings that involve many victims and millions of dollars. But they don't chase down single crooks who commit "victimless" crimes.

While victims may not be liable for the credit bills an identity thief runs up, they still are compelled to spend time, effort and money to clear up the mess. "They spend hours and hours filing expensive legal affidavits and writing letters and making telephone calls to clear their good names," says Ed Mierzwinski, consumer program director for PIRG.

### Looking out for yourself

Mierzwinski believes that both the credit-granting institutions and the credit bureaus need to improve verification systems to help prevent identity theft. But there's little chance of anything meaningful being done to make it harder for anyone to get credit. You have to look out for yourself.

"The most important thing that consumers can do is to order their credit reports once a year so they are not caught by surprise," Givens says. You can order a copy of your report online from Equifax (in most states), Experian and Trans Union. Cost: \$8 in most states, unless you have recently been denied credit. Then the reports are free.

Givens and other experts also suggest the following:

- Don't carry unneeded credit cards, your Social Security card, your birth certificate or other personal documents in your purse or wallet.
- Keep track of all your ATM, credit card, debit card and other receipts. Either store them in a safe place or destroy them before putting them in the trash.
- Cancel all your unused credit card accounts.
- Keep a list of your credit card account numbers and the companies' telephone numbers in a safe place so you can cancel them quickly and easily in case they are stolen or lost. A handy way of doing this is to use a copying machine. Just be careful where you leave the hard copy.
- Protect your Social Security number as much as you can. Do not give it out to any person or company unless you are familiar with them and you have initiated your communication with them.

If you become an identity fraud victim, PIRG suggests that you take three steps immediately:

- Report the identity theft to local law enforcement authorities, including the police, postal inspectors and Secret Service.
- Contact all banks and others where your name has been used fraudulently, sending a copy of a police report or other documentation to show that you are a fraud victim.
- Call the fraud departments of the three major credit bureaus to get copies of your credit report and to have fraud flags and statements added to your report saying that all potential creditors should contact you to verify credit applications.

If the first three steps fail to resolve the problem, we would add a fourth: Call a lawyer. Credit issuers and reporting agencies are sometimes slow in responding to complaints from consumers. The threat of lawsuits can provide some incentive (see the sidebar on advice).

For a more complete discussion of the precautions, as well as the steps to take if you become a victim of identity theft, visit the Privacy Rights Clearinghouse and PIRG Web sites.

“You ultimately cannot prevent identity theft from happening to yourself,” Givens says, “but you can reduce the odds.”