



Stop thief — that's MY identity you're using!

Byron Beck

Day and Zimmermann Protection Technology Hanford

This is the first of a series of articles that cover identity theft. Look for the continuation of this article in upcoming issues of the Hanford Reach.

In the course of a busy day, you may write a check at the grocery store, charge tickets to a ball game, rent a car, mail your tax return, call home on your cell phone, order new checks or apply for a credit card. Chances are you don't give these everyday transactions a second thought. But someone else may.

Identity theft is one of the fastest-growing crimes in America. Washington state ranked eighth in the nation in identity theft last year. Federal officials and consumer groups estimate there are between 500,000 and 700,000 cases of identity theft each year, costing victims over \$765 million annually. Last year, identity theft was the number-one consumer complaint to the Federal Trade Commission. Unfortunately, the electronic age has helped the identity thief immensely.

Hundreds or thousands of records or files are only a few keystrokes away. In addition, the sluggish economy might be driving more people to commit such theft, crime experts say.

Identity thieves' stock in trade is your everyday transactions. Many transactions require you to use personal information: your bank and credit-card account numbers; your Social Security number; or your name, address and phone numbers. An identity thief can co-opt pieces of your personal information and appropriate it without your knowledge to commit fraud or theft. An all-too-common example is an identity thief using your personal information to open a credit-card account in your name.

Close to home

Can you completely prevent identity theft from occurring? Probably not, but you can minimize your risk by managing your personal information wisely and cautiously, and with heightened sensitivity.

We have all heard horror stories about identity theft. Unfortunately, two Day and Zimmermann Protection Technology Hanford employees have first-hand knowledge of this activity. Someone applied for, received and

Continued on page 11.

Stop thief — that's MY identity you're using, cont.

used a credit card in each of their names. Both cards had the maximum amount allowed charged against them. Both employees received calls seven months after the incident. One employee was called to ascertain if an identity theft had occurred, and the other employee was called by an angry collection agency demanding payment on an overdue bill. As soon as the employees realized what had happened, they began the frustrating task of trying to clear their credit records and have the bad debts expunged.

What they learned

Both employees learned a great deal about how to limit the damage an identity thief can create:

- You, the victim, are responsible for clearing up the mess. It can take months or years to resolve.
- Cancel your credit cards immediately. Keep the credit-card companies' toll-free numbers where you can find them easily.
- File a police report immediately with your local police and the police in the jurisdiction where the card was stolen and used. A police report can help prove to creditors that you were diligent and it is the first step toward an investigation (if there is one). Also, get a copy of the police report in case the bank, credit-card company or others need proof of the crime.
- Call the three national credit reporting organizations immediately and place a fraud alert on your name and Social Security number (and call the Social Security number fraud line). These organizations issue an alert that warns companies that your information was stolen and requires them to call you before authorizing new credit. The national credit reporting agencies and their numbers are: Equifax (800) 525-6285, Experian (formerly TRW) (888) 397-3742; and Trans Union (800) 680-7289.

The two PTH employees also suggest, that everyone check his or her credit standing at least yearly, because they found inconsistencies in all three credit reports. Since they took the actions listed above, no additional damage has been done. It seems to have stopped further fraudulent activity.

How ID crime occurs

Despite your best efforts to manage who has access to your personal information, skilled identity thieves use a variety of methods, both low-tech and high-tech, to gain access. The following scenarios demonstrate how imposters can gather information and take over your identity.

Scenario 1: Dumpster diving

During the early-morning hours, there is no activity, except for a van driving slowly along the trash-can-lined street. The van stops, the passenger jumps out, grabs trash bags and tosses them into the van. Back at their "safe house," they dump the trash on the floor and begin sorting through their treasures. They might find the following:

- **Credit-card receipts** showing the card number, expiration date and signature. Even if the card has expired, they can simply add two years to the date when making telephone transactions.
- **Earning statements** with your work location, Social Security number, date of birth and earnings.
- **Receipts** showing where you eat, shop, go for entertainment or travel.
- **Bank statements** including the account number and ATM activity.
- **Empty packet of checks** that still has deposit slips. Thieves can change the address and send it to the

Continued on page 12.

Stop thief — that's MY identity you're using, cont. 2

bank requesting more checks.

- **Car service receipts** that show the make, model and identification number. With that information, someone can request a replacement for a "lost" title.
- **Everything about you**, which can be gathered over a long period of time.

Recycle bins may also provide information. Not all documents are reviewed before they're discarded, and sometimes they include information that is thought to be out of date or poor copies of sensitive documents. Always be sure that documents placed in recycle bins do not contain sensitive information.

Scenario 2: It's almost tax time

Some taxpayers have received e-mail from a non-IRS source indicating that the taxpayer is under audit and needs to complete a questionnaire within 48 hours to avoid the assessment of penalties and interest. The e-mail refers to an "e-audit" and references IRS form 1040. The taxpayer is asked for his or her Social Security number, bank-account numbers and other confidential information.

The IRS *does not* conduct e-audits, nor does it notify taxpayers of a pending audit via e-mail. Such a message is *not* from the IRS and you should not provide the requested information. It could be an attempt at identity theft.

Scenario 3: Job hunting

It was just the job lead Jim needed — a marketing-manager position with a leading international insurance broker. And only days after Jim responded to the job-posting on Monster.com, a human resources director sent along a promising e-mail. "We're interested in you," the note said. "The salary is negotiable, the clients big. In fact, the clients are so valuable and sensitive that you'll have to submit to a background check as part of the interview process."

Eager for work, Jim complied and sent just about every key to his digital identity including his age, height, weight, Social Security and bank-account numbers — even his mother's maiden name.

It was an elaborate identity-theft scam designed to prey on some of the most vulnerable potential victims, the unemployed. Job seekers don't have much leverage when they are asked to jump through hoops by a prospective employer.

In many online scams, bad spelling, grammatical errors and awkward sentence structure are often tips that something is amiss. A red flag might be that the area code and address where the information is to be sent differs from what's on the letterhead or the Web site. ■