

# What do you do when you are the victim of identity theft?

Byron Beck, *Day and Zimmerman Protection Technology Hanford*

*Last week's Operations Security article, "Stop thief – that's MY identity you're using!" explained identity theft and how an identity thief gathers information about you. Here, we discuss how the identity thief uses that stolen information and how you can protect yourself.*

Identity thieves can get your personal information by:

- stealing wallets and purses with your identification, credit and bankcards
- stealing your mail, which could contain your bank and credit-card statements, preapproved credit offers, telephone calling cards and tax information
- completing a "change of address" form to divert your mail
- rummaging through your home and business trash or recycle bins
- fraudulently obtaining your credit report
- obtaining your business or personal information at work
- stealing personal information from your home
- using personal information you share on the Internet — it's easy, quick and cheap
- requesting that you complete a personal survey
- monitoring automated teller machines
- stealing a security badge (from a car), changing the photo and using it as identification for facility access
- posing as a bank or credit-card company representative requesting information over the phone that your bank or credit-card company should already have
- buying your personal information from an "insider."

## How information can be used

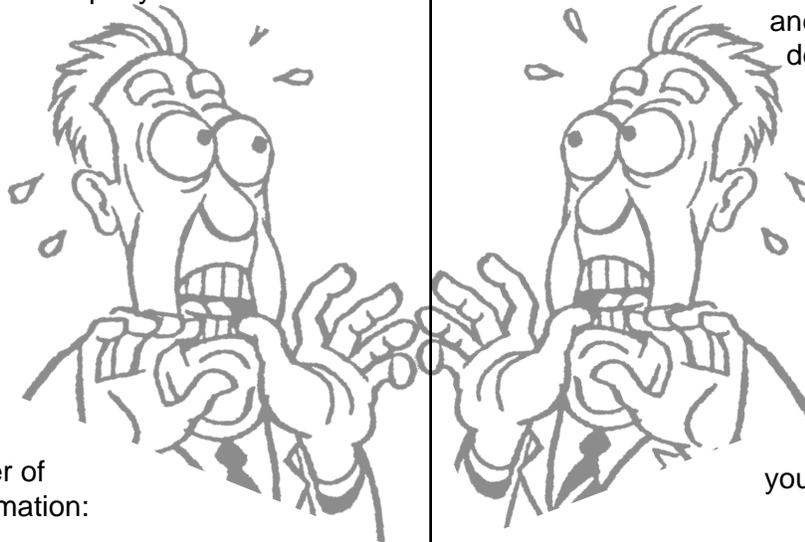
Once they have your personal information, identity thieves have a number of ways to use that information:

- They may call your credit-card issuer and, pretending to be you, ask to change the mailing address on your credit-card account. The imposter then runs up charges on your account. Because your bills are being sent to the new address, it may take some time before you realize there's a problem.
- The identity thieves may open a new credit-card account using your name, date of birth and Social Security number. They use the credit card, don't pay the bills, and the delinquent account is recorded on your credit report.
- They establish phone or wireless service in your name.
- They open a bank account in your name and write bad checks on that account.
- They file for bankruptcy under your name to avoid paying debts they've incurred under your name, or to avoid eviction.
- They counterfeit checks or debit cards, and drain your bank account.
- They buy cars by taking out auto loans in your name.

## Protect yourself

While you probably cannot prevent identity theft entirely, you can minimize your risk. By managing your personal information wisely, cautiously and with an awareness of the issue, you can help guard against identity theft.

- Before you reveal any personal identity information, find out how it will be used and whether it will be shared with others. Ask if you have a choice about the use of your information and if it can be kept confidential.
- Pay attention to your billing cycles. Follow up with creditors if your bills don't arrive on time. A missing credit-card bill could mean an identity thief has taken over your credit-card account and changed your billing address.



*Continued on page 17.*

## What do you do when you are the victim of identity theft, cont.

- Guard your mail from theft. Deposit outgoing mail in post-office collection boxes or at your local post office. Promptly remove mail from your mailbox after it has been delivered. If you're planning to be away from home, ask a trusted person to pick up your mail or call the U.S. Postal Service to request they hold your mail until you return.
- Put passwords on your credit-card, bank and phone accounts.
- Minimize the identification information and the number of credit cards you carry.
- Do not give out personal information on the phone, through the mail or on the Internet unless you have initiated the contact or know with whom you're dealing. Identity thieves may pose as anyone seeking personal information.
- Shred all receipts, copies of credit applications, insurance forms, physician statements, bank checks, expired credit cards, credit offers and statements that you are discarding.
- Be cautious about where you leave personal information at work or at home.
- Give your Social Security number only when absolutely necessary. Ask to use other types of identifiers when possible.
- If you place financial information on your personal computer, consider having all of the sensitive data stored on removable media such as a floppy disk or CD and not on your hard drive. Then, when you decide to sell your computer or send it in for servicing, unauthorized persons cannot gain access to your data.
- Thank the store clerks who ask for your identification; they are helping to protect you and your account.

### What can you do?

Sometimes an identity thief can strike even if you've been very careful about keeping your personal information private. If you suspect that your personal information has been hijacked and misappropriated to commit fraud or theft, take action immediately, and keep a record of your conversations and correspondence.

Contact the police department and the Federal Trade Commission. Contact the Social Security Administration at (800) 269-0271 if you suspect your

SSN is being fraudulently used. Through the toll-free Identity Theft Hotline at (877) 438-4338, the FTC collects complaints about identity theft from consumers who have been victimized. Although the FTC does not have the authority to bring criminal cases, it can help victims of identity theft by providing information to assist them in resolving the financial and other problems that can result from this crime. The FTC also refers victim complaints to other appropriate government agencies and private organizations for further action.

You can minimize your risk by managing your personal information wisely, cautiously and with heightened sensitivity. If you would like to learn more, we encourage you to use the Internet at home or at your local library. Just use your favorite Internet search engine and type in "identity theft."

Here are some Web sites that may be useful:

- Federal Bureau of Investigation at <http://www.fbi.gov/>
- Federal Deposit Insurance Corporation at <http://www.fdic.gov>
- Federal Trade Commission at <http://www.ftc.gov>
- United States Postal Inspection Service at <http://www.usps.gov/>
- United States Secret Service at <http://www.treas.gov/usss/>.

This list does not constitute an endorsement or approval of content by Day and Zimmermann Protection Technology Hanford. ■