

Safeguarding Your IDENTITY



Oprah Winfrey, Tiger Woods, Martha Stewart, Steven Spielberg and Robert DeNiro all have been targeted. It happens every 79 seconds. Hundreds of thousands of people are victims of it every year. And if you don't take care, some day you may be, too.

and Your WEALTH

A well-dressed man strolls down a tree-lined street of a nice neighborhood, apparently getting some fresh air. Casually, the man opens a mailbox with a raised red flag, indicating mail is awaiting pickup. He removes the envelopes. At the next house, he does the same thing. After he has emptied the mail, he sorts through and opens bills and anything else that might contain Social Security numbers and other personal information.

This man is stealing more than just mail — he's taking these people's identities. He has chosen this neighborhood because he knows these Social Security numbers are likely tied to excellent credit histories. He uses this stolen information to open lines of credit and new credit card accounts online, where there is less scrutiny. He also initiates a change of address for an existing account and orders new checks, which he uses to make purchases. He is able to siphon thousands of dollars from these accounts before anyone notices. The longer he goes undiscovered, the more he steals.

TACKLING A GLOBAL PROBLEM

Identity theft has been the fastest-growing crime in the United States in the past five years, says Thomas Roberts, Northern Trust's division head of corporate fraud prevention and investigations. Consumers reported fraud-related crimes of more than \$680 million in 2005, according to the Federal Trade Commission (FTC). And the FTC says that roughly 5% of the population has reported being victims of identity theft.

Everyone, regardless of their net worth, should be aware of the pervasiveness of the crime, Roberts says.

"The problem is huge and getting bigger every day, and you really need to protect yourself because no one else is going to do it," he says. "You can't look to the police to protect you."

You need to understand the latest identity theft schemes coming over the Web, keep up with the latest protection software and specifications, and use some common sense, he says.

UNDERSTANDING IS KEY

Years ago, identity theft was primarily a local crime, Roberts says, with thieves stealing mail, purses or wallets, or using other low-tech means of appropriating someone's identity. Thanks to the Internet, however, identity fraud has become a global issue.

In addition to the well-publicized incidences of someone hacking into an institution's computer system and stealing information, thieves use a variety of methods to steal identities over the Internet. One of the more common schemes today is "phishing" — when thieves send fraudulent e-mails posing as legitimate companies asking for the recipients' passwords or other personal information to resolve a problem with their accounts.

Other identity theft schemes range from sophisticated to simple and include:

- Skimming credit or debit card information from ATM machines with data storage devices.
- Burglarizing your home or "dumpster diving" for bank and credit card statements, etc.
- Using change of address forms to divert mail.
- Posing as authorized personnel with legal access to credit information.
- Getting the information from friends, family or coworkers.

After the thieves have obtained your information, they generally assume your identity to open new credit card accounts or lines of credit, or write checks against existing accounts. And affluent households may be uniquely vulnerable for a number of reasons.

ATTRACTIVE TARGETS

Identity thieves often target affluent individuals because they are unlikely to be turned down for credit when they open new accounts and are frequently able to use an affluent individual's identity longer without detection.

Protecting your information is key to safeguarding your identity. Shred financial documents, bills, statements or anything that contains personal information. "Be stingy with your Social Security number," Roberts says. That means revealing your personal information

only when it's absolutely necessary. In many cases, you're not required to give your Social Security number, he says. Also, take care when disclosing personal information over the phone, mail or Internet.

RAPID DETECTION LESS LIKELY FOR SOME

The higher balances in the bank and investment accounts of wealthy individuals can make detecting criminal activity more difficult. For instance, if someone writes a \$5,000 check against an average account, that check is likely to bounce and the account holder will be notified. However, high account balances can mask these fraudulent transactions and make rapid detection less likely.

To protect yourself, monitor your financial accounts for suspicious activity. "Be aware of when your bills and statements should be showing up in the mail," Roberts says. Signs that could point to identity theft: skipped billing statements, unsolicited credit cards or account statements, credit denials for no apparent reason, or calls or letters about purchases you didn't make.

If you split your time between two or more homes, ensure your mail is properly routed to you and have a trusted neighbor check your mailbox regularly. These measures could help minimize your chances of overlooking a skipped statement or bill.

MORE PEOPLE, MORE VULNERABILITY

Employing multiple people to handle your investments and other personal affairs also may provide additional

opportunities for theft. To avoid inadvertently giving an unscrupulous person access to your accounts, be sure to hire reputable people and conduct background checks, Roberts says.

"Make sure the people you hire are as careful as you are with your identity," Roberts says. "Ask them what controls they have in place to prevent fraud. Are there locks on your information in their computers? Have all the documents been shredded before being discarded? If they don't give you the right answers, they might not be the appropriate people to handle your money."

Take the time to review the privacy policies of any company that has access to your personal or financial-related information and be sure you are comfortable with their policies.

IF YOU SUSPECT A PROBLEM

Finally, if you suspect you might be a victim of identity theft, take the appropriate steps to stem the damage. Dealing with a stolen identity can be incredibly time-consuming. But acting quickly can help minimize the damage — it can deter the identity thief from continuing to use your identity, and in many cases, the amount of personal liability you face is directly related to how long it takes you to report the problem.

While identity theft is a growing problem, it does have an upside. "People are now much more savvy," Roberts says. "They're questioning things they might not have noticed several years ago. That's a very good thing." ■

Seven Ways to PROTECT Your IDENTITY

1. Open all bank, credit card and investment statements promptly and scan for suspicious activity.
2. Shred all documents that contain account or personal information, including credit card applications and other "junk" mail, before putting in the garbage or recycling.
3. Be careful when giving out your Social Security number, account information or passwords over the phone or by e-mail. If someone calls or sends an e-mail claiming
4. Once a year, review a copy of your credit report to monitor activity.
5. Beware of the latest identity theft scams. The Federal Trade Commission maintains a Web site with resources to help you "deter, detect and defend" against
6. Minimize the possibility of spyware on your computer. Establish a firewall and keep your virus protection software up to date.
7. Question anyone who handles finances on your behalf or has access to your personal information to ensure they are taking precautions to safeguard your identity.

identity theft. For more information, go to ftc.gov/bcp/edu/microsites/idtheft.