MORNINGSTAR®
PracticalFinance℠

June 2009
Volume 5
Number 6

Protect Yourself from Identity Theft

I like to think I'm pretty scrupulous about avoiding identity theft. I try to shred anything that comes into my house with my name on it, I'm on my guard when conducting transactions online, and I ask questions before I give anyone personal information they may not need. (This is more of a privacy point than one about identity theft, but is anyone but me stunned at the number of people who blurt out their phone numbers when a random retail salesperson asks them for it?)

I recently attended an identity-theft seminar, however, and was surprised at how much I learned. That's because identity thieves are constantly evolving their practices. Just as soon as we consumers get up our guard against one type of identity theft, criminals seem to come up with a workaround.

For that reason, I'm devoting part of this month's issue to making sure you're staying one step ahead of the identity thieves. Not only are identity thieves using new methods that you need to be aware of, such as "skimming" and "pretexting," but identity theft has been spiking amid the faltering economy. Reported cases of identity theft increased to nearly 10 million in 2008, according to Javelin Strategy & Research, up 22% from 2007. Scammers steal personal information to rent apartments, open new credit cards, obtain health insurance or health care, establish utilities, or even obtain employment and loans. That fraud, in turn, exacts an enormous financial and emotional toll on those who are scammed. On the plus side, the amount of dollars ripped off in each incident has dropped sharply, to roughly $500 per incident, in part because consumers have become far more vigilant about staying alert for signs of identity theft and promptly reporting cases to authorities.

In the pages that follow, I've provided you with a comprehensive set of strategies for safeguarding your identity, whether you're at home, online, or out and about.

Track Your Statements

One of the best ways to be pre-emptive about identity theft is to scrutinize the transactions on your bank and credit card statements to ensure that they're in line with the transactions you've made. And if you identify a discrepancy, notify the financial institution immediately, first via phone call and then by certified mail, requesting a return receipt.

If you identify unauthorized charges on your credit card bill and notify your card company within 60 days of receiving the statement, your liability will be limited to $50 per card. If you identify unauthorized transactions involving your debit or ATM card, time is of the essence. Your liability will be limited to $50 if you notify your bank within two days of discovering the unauthorized transaction; if you notify the bank between two and 60 days of discovering the discrepancy, your liability jumps up to $500. If it takes you more than 60 days to notify your bank of the unauthorized debits, you're on the hook for any losses in your account.

Note that if your ATM or debit card carries the Visa or Mastercard logo, and many of them do, your liability is in most cases limited to $50 per card,

Continued on Next Page

Christine Benz,
Director of Personal Finance

regardless of how long it takes you to report the fraud to your bank. Still, for everyone's sake, it's best to report a problem as soon as you identify it.

In addition to combing your statements to make sure that all of your debits and credits are truly yours, I'd also recommend tracking the dates you receive your statements for the next month. That will give you an idea of when to expect them in future months. If you don't receive a credit card, bank, or other financial statement within two or three days of when you normally receive it, contact the bank or credit card company to let them know. Identity thieves have been known to steal financial statements out of the mail to obtain personal information, and if they've stolen your identity they may divert mail to another address. They may also steal newly issued credit or debit cards from the mail.

Reduce Your Reliance on Snail Mail

There's something comforting about receiving paper statements in the mail. For financial assets, that paperwork may seem like black-and-white, tangible proof that you truly own what you own.

That sense of security provided by paper is largely illusory, however. In fact, provided you've taken steps to secure your at-home network (more on this in a minute), conducting your financial transactions online is safer than using paper statements and checks. The reason is simple: When your financial transactions are passing from mailbox to the postal service back out to another mailbox, identity thieves have more opportunities to put their hands on your personal information. And unless you shred everything that comes into your house, identity thieves can also sift through your trash in search of documents with your personal information and account numbers.

It's hard to eliminate snail mail from your life entirely, though, and some of you simply may not be ready to make the leap to online banking and bill-paying. Thus, it pays to take precautions when sending financial information through the mail. If you're receiving checks from your employer or a financial institution, use direct deposit rather than having checks mailed to your house. If you're ordering blank checks, arrange to pick them up at the bank rather than having them sent to your home. Always put your outgoing mail in a U.S. Postal Service mailbox rather than in your own home mailbox or the outgoing mailbox at your office. I also recommend that you skimp on putting extra identifying information like phone numbers and account numbers on your envelopes, even if the financial institution or utility asks you for it.

Set Up a Secure Online Security System

As I noted, managing your financial transactions online can be safer than doing so via the mail. The essential ingredient, however, is an up-to-date security system for your home computer network, including anti-virus and anti-spyware software as well as firewalls. A good spam filter can also help ensure that you don't receive a lot of scam e-mails. Although these programs have gotten easier to use, they can still be cumbersome and require that you update them periodically. If you're not comfortable

---

To stop Windows from "remembering" your passwords:

1. In Internet Explorer, click on the **Tools** menu from the top of your screen. Then click on **Internet Options** in the dropdown menu.
2. Click on the **Content** tab. Click on the **Auto-Complete** button and the **AutoComplete Settings** screen appears.
3. Uncheck the box that says **User names and passwords on forms**, then click **OK**.

To password-protect Microsoft Excel and Word documents:

1. With a Word or Excel document open, click on the **Tools** tab.
2. Next click **Options** in the dropdown menu. Click on the **Security** tab and enter your password, then click **OK**.

Watch Out for These Common Types of Identity Theft

Dumpster Diving
WHAT IT IS_ Thieves steal personal information from garbage, recycling bins.
AVOID IT_ Shred account statements, bills, credit card solicitations.

Medical Identity Theft
WHAT IT IS_ Thieves steal your identity to obtain insurance, medical care in your name.
AVOID IT_ Safeguard your insurance card, review health-insurance claims carefully.

Phishing
WHAT IT IS_ Legitimate-looking e-mail or Web site asks you to supply personal information.
AVOID IT_ Never supply personal information when solicited via e-mail or online.

Pretexting
WHAT IT IS_ Scammer lies about identity in an effort to obtain your personal information.
AVOID IT_ Don't give out personal information unless you've initiated the contact.

Skimming
WHAT IT IS_ Applies to theft of credit or debit card numbers for fraudulent purposes.
AVOID IT_ Stay alert at point of sale; watch out for unusual devices attached to ATM machine, gas pump.

Pharming
WHAT IT IS_ Secretly directs you from a legitimate Web site to a scammer's site.
AVOID IT_ Look for padlock icon, "https" in the URL; keep security software up to date.

Shoulder Surfing
WHAT IT IS_ Thieves obtain PINs, account numbers by looking over your shoulder.
AVOID IT_ Shield ATM machine with your body, conceal credit card number from others in store line.

setting up these systems and doing what you need to do to keep them up to date, hiring a computer consultant to come into your home to do it for you can be well worth the money you'll spend.

Because you can't be sure about the quality of the security software on computer systems that aren't your own, be careful about accessing financial information when you're away from home. And never, ever log on to any of your financial accounts using a public or unsecured network.

Be Password-Savvy

Also be careful with the passwords you use, particularly on sites where you conduct transactions or provide personal financial information. Don't use obvious passwords, such as the name of your spouse or pet, or your birthday; that makes it easy for identity thieves to guess at yours. Also don't use the same password again and again. The hardest-to-hack passwords are gibberish or use a combination of numbers and letters.

Windows will ask you whether you want it to "remember" your passwords, and then it will populate the password field automatically. That makes it a lot easier to surf online, but be careful when using this feature. Use it only when you're on sites that don't store sensitive information, such as your local newspaper's site, rather than on sites where you actually execute business transactions. You can also shut off the Windows feature that asks you whether you want it to remember your passwords. I've included details on how to change this feature on Page 2.

Using "password manager" software is another way to guard against phishing and other online scams. These programs store your user names and passwords and encrypt your information so it's not accessible to hackers; however, these programs may not be able to handle some of the more complicated password formats that some banks require.

If you manage your various user names and passwords on your own, perhaps by maintaining a Microsoft Word or Excel document on your computer, take care to ensure that document's safety. If your workstation doesn't require a password to log on, take the step of password-protecting your document. I've included details on how to password-protect Microsoft Word documents and Excel spreadsheets on Page 2.

Shop Safely

In addition to keeping your home computer's security system up to date, you should take steps to help prevent fraud while shopping online. Make sure you have the latest version of your Internet browser, because newer versions often incorporate the latest in encryption technology. In addition, there are a couple of signals to look for to indicate that you're shopping safely. On any screen where the vendor requests that you input passwords, your name and address, credit card number, or any other identifying information, the URL in your browser window should read "https" rather than "http." In addition, you should see a small yellow padlock icon toward the bottom right corner of your screen. If you're not sure your information is adequately protected, call the company and tell it about your concerns.

Once you make an online purchase, print out the confirmation and be sure you have the vendor's name, address, and phone number. Also be on high alert if a vendor you've never heard of has a price on an item that's far below the selling price everywhere else. You may indeed have found the deal of the century, but it could also be a red flag that the merchandise is counterfeit or the vendor isn't legitimate. Do a little more research before supplying your credit card number.

In addition, you're usually better off, from a security standpoint, using a credit card rather than a debit card when transacting online or in a store. As I mentioned above, debit card holders who don't report the problem within two days of discovering it could be on the hook for as much as $500. On a more basic level, credit card holders whose accounts have been tampered with have an important lever that debit card holders do not have. If someone has made a fraudulent transaction on your credit card, you may simply refuse to pay the bill until the problem gets resolved. But if someone has taken money out of your account or made a purchase using your debit card, the onus is on you to get the money back.

If you're shopping in stores or dining out, you also need to take steps to protect your sensitive financial information. Guard your credit card number when standing in line at a store, and make sure your credit card doesn't leave your sight for an extended period of time (though it's inevitable that restaurant servers take your credit card away from the table to process your transaction). Also be leery of hand-held card-processing machines, which can be devices to "skim"—meaning that the store employee makes a copy of your account number with an eye toward fraudulently using it later on.

Carry as few credit cards as you'll need, hold on to your receipts when you return home, and shred them. As an additional safeguard, write "Check ID" alongside your signature on the back of your credit card. You'll have to produce your driver's license each time you transact with that card, but the ID check will provide an additional safeguard that you're the only one who can use the card.

Don't Call Us, We'll Call You

Also be on high alert if someone saying they're from a bank, government agency, or law enforcement calls you and requests personal or financial information. These entities don't typically do this. Ask the caller to send you more information in writing, or, if you're concerned there's a problem with one of your accounts, look up the financial institution's phone number in your files or on the back of your credit card and place the call yourself. Don't use a phone number supplied by the person who called you, and don't assume the call is legitimate simply because your caller ID readout matches where the person says they're calling from. (Identity thieves can mock up their caller ID readouts.)

Also avoid making charitable donations over the phone. Instead, go to the charity's Web site or request that the information be sent to you in the mail.

Take Care with Health Care

Medical identity theft can take a number of different forms, and that's partly why it's a "growth" area of the identity-theft world. Criminals can pilfer your insurance information to obtain treatment or prescription drugs, or they may file fake claims to obtain payouts from insurers. Not only can this type

Ten Ways to Protect Yourself from Identity Theft Today

	What You Can Do	Why You Should Do It
1	**Switch to online banking.**	Less personal information in the mail means thieves have fewer chances to obtain your information.
2	**Check your computer security: Spyware, firewalls, antivirus, and spam filters.**	Online transactions are only safe if your security system is up to date.
3	**Track the dates when you typically receive bills, statements.**	If a bill or statement hasn't arrived, you can alert the issuer promptly.
4	**Use direct deposit for checks.**	Identity thieves target mailed items that look like checks.
5	**Turn off the "Remember Your Password" feature in Windows.**	Makes it harder for identity thieves to click through for your personal information.
6	**Password-protect sensitive documents.**	Protects you in case someone improperly gains access to your computer.
7	**Use credit rather than debit when shopping.**	Consumer protections are generally greater for credit cards than debit.
8	**Write "Check ID" on the back of credit card.**	Vendor will have to ask for photo ID before accepting your card.
9	**Scrutinize health-care statements.**	Medical identity thieves can masquerade as you, obtain treatment or insurance.
10	**Carry a copy of your Medicare card.**	Original cards carry your Social Security number; you can black it out on copy.

of fraudulent activity muck up your finances and credit report, but if a criminal's medical history is commingled with your own, there's a chance you could receive the wrong type of medical treatment.

All of that makes it essential that you safeguard your health-care records and insurance information as closely as you guard other personal financial information. As with your credit and debit cards, keep close tabs on your insurance card at all times. In addition, review your health-care transaction statements as closely as you scrutinize your credit card and bank statements. If you spot anything out of the ordinary, notify your health-care provider and insurance company as soon as possible. As with financial statements, receiving claims and other medical information online is preferable to having these statements pass through the mail.

Also be careful with Medicare cards, which include Social Security numbers. One idea is to make a copy of your card, then use black marker on the copy to cover up the last four digits of your Social Security number. If you're a new patient, health-care providers may still require that you bring your original card to the office so they can make a photocopy, but after that your safer copy should be sufficient.

Mind the Home Front

Also take care when storing sensitive documents in your house. Even if you don't have a lot of people coming and going in your home, I recommend a locking file cabinet to hold any paperwork that includes your account numbers or Social Security numbers. And if you keep a master directory with your financial account numbers, by all means keep that under lock and key—either at home, in a safety-deposit box, or in a password-protected electronic version. Identity-theft experts also say you only court problems by carrying your Social Security card in your wallet; your safety-deposit box is the best place for it.

Finally, be careful about what you throw away. Good old-fashioned dumpster diving is still a popular form of identity theft; by putting all of our paper recyclables together and on the curb, many of us make it even easier for identity thieves to sort through our paperwork. That's not to suggest you shouldn't recycle but rather that you should invest in a good-quality cross-cut shredder and make liberal use of it.