

# 10 Things to Know About Identity Theft

Identity theft is often in the news, but there are a lot of misconceptions swirling around about how to best protect yourself.

While some identity thieves focus on getting your credit cards and maxing them out before you even realize they're missing, an increasing number are using one piece of information about you — often a credit card number — in order to steal your entire identity.

Though many folks worry about keeping their credit card information secure when shopping online, the top methods that identity thieves use to steal personal data are still low-tech, according to Justin Yurek, president of ID Watchdog, an identity theft-monitoring firm. “Watch your personal documents, be careful to whom you give out your data over the phone, and be careful of mail theft,” he says.

Indeed, a recent study by Javelin Strategy & Research found that of the 9.9 million identity-theft cases reported in 2008 — resulting in a loss of \$48 billion — online theft only accounted for 11 percent of incidents. Stolen wallets, checkbooks, and credit and debit cards made up almost half.

No one is immune to identity theft, but armed with a little knowledge about how identity thieves operate — and a little

common sense — you can stay one step ahead of them.

**1. Thieves don't need your credit card number in order to steal it.** Conversely, they don't need your credit card in order to steal your identity. Identity thieves are crafty; sometimes all they need is one piece of information about you and they can easily gain access to the rest. As a result, says Heather Wells, recovery manager at ID Experts, an identity protection company, today it's crucial to lock up important documents at home. “Secure birth certificates, Social Security cards, passports, in a safe deposit box or in a safe hidden at home,” she says. “And that includes credit cards when not in use.”

**2. The non-financial personal information you reveal online is often enough for a thief.** Beware of seemingly innocent personal facts that a thief could use to steal your identity. For example, never list your full birthdate on Facebook or any other social-networking Web sites. And don't list your home address or telephone number on any Web site you use for personal or business reasons, including job-search sites.

**3. Be careful with your snail mail.** “Follow your billing cycles closely,” says Lucy Duni, vice president of consumer education at TrueCredit.com. “If a credit

card or other bill hasn't arrived, it may mean that an identity thief has gotten hold of your account and changed your billing address." Al Marcella, professor at Webster University's School of Business and Technology in St. Louis, and an expert on identity theft, suggests when you order new checks, you pick them up at the bank instead of shipping them to your home. "Stolen checks can be altered and cashed by fraudsters," says Duni. And never place outgoing mail in your post office box or door slot for a carrier to pick up. Anyone can grab it and get your credit card numbers and other financial information. Bring it to the post office yourself.

**4. Review all bank and credit card statements each month, preferably once a week.** Watch for charges for less than a dollar or two from unfamiliar companies or individuals. Thieves who are planning to purchase a block of stolen credit card numbers often first test to check that the accounts haven't been cancelled by aware customers by sending a small charge through, sometimes for only a few pennies. If the first charge succeeds, they'll buy the stolen data and make a much larger charge or purchase. They're guessing — often correctly — that most cardholders won't notice such a tiny charge. In addition, many of the fraud alerts you can set on your accounts aren't triggered by small dollar amounts. Reviewing your credit report on a regular basis is also a good idea, but usually by the time a fraudulent transaction reaches your credit report, it's too late.

**5. If an ATM or store terminal looks funny, don't use it.** "Make sure there is no device attached to any ATM card slot you use," says Wells. "As a general rule, the mouth of a card receptacle on an ATM machine should be flush with the machine or have only a very slight lip." If it looks or feels different when you swipe your card, or has an extra piece of plastic sticking out from the card slot, it may be a skimmer, an electronic device placed there by thieves that captures your credit card information when you swipe it. If you notice it after you've already inserted your card, you should alert your bank so they can watch for any fraudulent charges to your account.

**6. Identity thieves love travelers and tourists.** Scott Stevenson, founder and CEO of Eliminate ID Theft, an ID theft protection company, cautions travelers to be alert to strangers hovering around whenever you use a credit card at an ATM or phone, and to avoid public wireless Internet connections unless your laptop or PDA has beefed-up security protection. However, he also suggests watching for little-known methods of lifting your identity. "Cut up your used hotel key cards when you check out," Stevenson advises, since these keys contain important information about you and your finances, including your name, address, phone, and the credit card you used to pay for your room. "When you toss them out or leave them lying in the hotel room, anyone can pick them up and use them to steal your identity," he adds.

**7. Identity thieves are sneaky; you**

**need to be sneaky, too.** There are a few simple things you can do to protect your credit card in case it falls into the wrong hands. “Sign your credit card with a Sharpie so your signature can’t be erased and written over,” suggests Echo Montgomery Garrett, a writer in Marietta, Ga. Consultant Sarah Browne of Carmel, Calif., had all but one credit card stolen from a hotel room. The card that was spared still had the “Please Activate” sticker on it. Though Browne had activated the card, she forgot to remove the sticker. “The thieves must have known that you have to activate a new card from the phone number listed with the credit card company, so they didn’t bother with it,” she said, and since then, she leaves the activation stickers on all of her cards. Indeed, when a thief struck a second time at a public function, Browne’s stickered cards were again left untouched.

**8. Pay attention at the checkout line.** If a cashier or salesperson takes your card and either turns away from you or takes too long to conduct what is usually a normal transaction, she may be scanning your card into a handheld skimming terminal to harvest the information. But they don’t need a handheld scanner to capture your information. According to Mark Cravens, the Anti-Scam Doctor and author of “The Ten Commandments of Investing,” they can take a picture of the front and back of your card with a cell phone or merely swap out cards. “Look at your card when they hand it back and make sure it’s yours, and not another gold, silver, or blue card that looks like

yours,” he says. “You may not notice they swapped your card for days.”

**9. Go paperless in as many ways as possible.** Sandy Shore, training manager with Novadebt, a nonprofit, New Jersey-based credit-counseling agency, suggests clients cut back on the mail they receive from banks and financial institutions by discontinuing paper bills and statements. “Access your financial statements at the issuer’s Web site instead,” she says. This strategy has the added bonus of an environmental benefit. Similarly, Vaclav Vincalek, president of Pacific Coast Information Systems, an IT security firm, recommends that whatever paper receipts and financial statements you do receive go through the shredder instead of into the wastebasket. “Never throw away a credit card slip,” he says. “Instead, shred anything that has any number, name, address on it.”

**10. Identity theft insurance can pay off, but you need to read the fine print.** Several companies offer identity theft insurance, which covers the money you shell out to repair your identity. This includes whatever you spend on phone calls, making copies of documents and mailing them, hiring an attorney, and in some cases, lost wages. However, the insurance — which costs about \$50 a year — does not reimburse you for funds you lost. Your current homeowner policy may include identity theft insurance in your package, so check first before signing up with an outside company. Also, some companies are starting to offer identity theft insurance as an employee

benefit.