22 WAYS TO FOIL CREDIT CARD THIEVES

You probably won't end up paying the bill, but a stolen credit card can still cost you big in time and aggravation. Here's how to protect yourself online and off.

By Liz Pulliam Weston

In some ways, credit card fraud isn't the problem it's often made out to be.

VISA says fraud accounts for about 7 cents of every $100 spent on its credit cards, an all-time low and about half the rate of 10 years ago. Add to that the fact that the major credit card companies have "zero liability" policies, which means the vast majority of consumers who are victims don't wind up paying a dime out of their own pockets.

Why, then, should you worry?

Well, for one, credit card fraud is a hassle. You often need to have your account closed and a new one opened, which can leave you without a card for a week or more. That's inconvenient, and it can mess up any automatic payments charged to that card.

That's if all goes well. Sometimes card issuers balk at removing charges or closing a bogus account.

Robert Allen of Simi Valley, Calif., fought with Capital One for seven months before the credit card company finally removed a disputed charge from an Internet retailer. (The retailer kept insisting it had sent the digital camera Allen ordered, but nothing ever arrived.) Allen said Capital One also closed his account and issued him a new card, which he worried might hurt him in other lenders' eyes.

"That was my oldest account at seven years," said Allen. Closing the account "makes my credit history look younger than it is."

Occasionally these disputes can escalate to the point where they show up as a late payment, charge-off or collection on your credit report. That can really trash your credit score, which is the three-digit number lenders use to help them gauge your credit-worthiness. Banks and insurers check your credit.

So should you.
So, better safe than sorry. Fortunately there's plenty you can do to reduce the odds of becoming a victim.

Guard your card online

☐ **Beware of "phishing" e-mails.** These are made to look as if they're coming from your bank or credit card issuer and usually urge you to take "immediate action" so that your card isn't deactivated. The link in the e-mail takes you to a criminal's Web site, where you're encouraged to input your credit card account number and other personal financial details. If you get an e-mail purporting to be from your card issuer, use the toll-free number on your card to call and ask what's up.

☐ **Be cautious shopping with unknown Web sites.** A quick trip to an evaluation site like Bizrate.com or the Better Business Bureau online could save you money. Also make sure you have multiple ways to contact the merchant, including a phone number, fax number, street address (not just a post office box) and e-mail address.

☐ **Make sure the transaction is secure.** Don't enter your card number unless the little padlock is showing on the lower part of your browser, and the Web site address starts with "https" rather than just "http."

☐ **Don't let Web sites "store" your cards.** The encryption technology used for transactions -- the information zipping back and forth between your computer and the merchant's -- may well be better than the security used to protect information stored in the merchant's databases. Besides, a big database of credit card numbers is a juicy target for hackers.

Guard your card offline

This is really basic, but: Don't forget your card. You might be rushed, or distracted by your kids, or involved in an interesting little chat with the clerk. Whatever. Keep an eye on your card and make sure it goes back in your wallet. I typically leave my wallet on the counter or restaurant table, with my hand on top of it, until the card goes back in. This can be a little awkward sometimes, but it helps remind me not to leave the store without my plastic. The one time I forgot is the time, of course, someone swiped my card.

☐ **Shield your card.** Think how many people these days carry around camera phones -- and think how easy it would be to snap a picture of your card if it were left in plain view.

Don't give your number out to solicitors. This includes telemarketers who contact you by phone to offer you a "great deal" on magazine subscriptions, vacations or any other purchase. If you ever get anything, you're likely to pay a lot more for it than agreed, and some of these scamsters fight tooth and nail against your attempts to have the charges removed.

☐ **Consider carrying fewer cards.** Reduce your exposure by limiting the number of cards a thief could potentially steal.

☐ **Copy what you carry.** Every once in a while, empty your wallet onto a copier and zap an image of the front and back of your cards. Keep this info in a secure place (not in your purse or wallet) so you know which issuers to call to report stolen cards.

Watch your statements

☐ **Know when your statements should arrive.** Missing statements could indicate that someone has stolen your mail or redirected it to a new address. Check your most recent statements for the account closing dates; most close around the same time each month, and should land in your mailbox a week or so later.

☐ **Review the charges.** The more fastidious among you can compare your statement with receipts you've collected during the month. The rest of us should, at the very least, scan each charge to make sure we recognize the merchant and the amount and have some recollection of making the purchase.

☐ **Report suspicious or unauthorized charges.** Call the issuer promptly and follow up in writing. Yes, sometimes you'll make a donkey of yourself, as I did in the sleep-deprived days after our daughter was born. I insisted to the customer service rep that I couldn't possibly have made a certain charge -- only to realize after her gentle questioning that, yep, I actually had. The rep was very gracious. I suspect such things happen all the time.

Police your paperwork

☐ **Beware of "mistakes."** If a merchant makes an error processing your card, tear up the incorrect receipt or at least write "void" all over it. When presented with a receipt that has blank lines before the total, draw a line through them so that additional charges can't be added.

☐ **Collect, collect, collect.** Gather up your "flimsies" -- credit card receipts -- rather than leaving them where any thief could copy down your account number and expiration date. (In a few years, merchants will be required by federal law to truncate numbers on receipts, but it's not the law yet in most places.)

☐ **Shred, shred, shred.** Cross-cut shredders are the best, but even a $20 version will do the job. Feed it all your old credit card receipts, applications and anything else that includes sensitive financial information, such as your Social Security number.

Secure your mail

☐ **Opt out of credit card solicitations.** Reduce the volume of pre-approved credit card offers (which can be swiped and used by thieves) by calling 1-888-5OPT OUT, which will take your name off marketing lists sold by the credit bureaus. You'll need to input your Social Security number as an identifier. Signing up for this service didn't eliminate but did significantly reduce the number of offers coming into our home.

☐ **Ask your issuers not to send "convenience checks."** Good luck with this one. Some issuers will abide by your wishes (although it may take a while -- often these things are printed up months in advance). Others will ignore you. Be persistent.

☐ **Get a locking mailbox.** And don't leave your outgoing mail where it can be swiped by anyone passing by; drop it off at the post office.

Other ideas:

☐ *Keep and maintain a file of each and every credit card you have. Copy of the original offer and contract, contact names, telephone numbers what to do if card is stolen, etc. Never know when you may need this information in hurry.*

☐ *Review your credit history report periodically*.

☐ _____

☐ _____

☐ _____

☐ _____

☐ _____

☐ _____

☐ _____

☐ _____

If you're a victim:

Despite your best efforts, you may still become a victim. Here's what you need to know:

Your liability for fraud on existing accounts is limited. Technically, you could owe $50 if the thief has a chance to use a stolen card before you call the issuer to report it. But typically issuers waive that fee, particularly if you report the theft promptly. (If the thief steals your account number, rather than the card itself, you have no liability under federal law.) You may have to fill out an affidavit the issuer sends you to confirm that fraud occurred, but typically the bogus charges are removed without too much hassle.

If the fraud involves a billing dispute, you'll want to notify the issuer in writing within 60 days of when the statement containing the charges was mailed to you.

(Since you probably won't pick up the tab for credit card fraud, you may wonder who does. The answer depends on whether the merchant got an actual signature. If so -- if the transaction happened in a brick-and-mortar store, for example -- the credit card issuer is usually the one who eats the cost. If not -- if the transaction happened online or over the phone -- the merchant typically pays. Given that credit card fraud is at least 15 times more common on the Web than offline, at least according to research firm Gartner Inc., you can see why some Internet merchants are a little paranoid.)

You may be in for a bigger fight with new-account fraud. If someone steals your identity to open a new credit card, you may face more skepticism from the card issuer. Lenders often require a police report before they agree to remove the account from your credit report. (Needless to say, that can create problems if the thief is someone you know -- as I touched on in "The newest identity thieves: parents.")

Keep good records. Call your issuer as soon as you spot the fraud, but then follow up in writing. Use the company's address for "billing inquiries," which you'll find printed on your statement or in your account agreement; it's usually different from the place you send your payment. Keep copies of all correspondence with the issuer and any merchants involved.

Keep pushing. Like Robert Allen, you might run into a recalcitrant merchant or card issuer. You don't have to give up. Ask for another investigation, take your case to arbitration, contact regulators, even give your representative in Congress a call.

Get help if you need it. Resources like the Identity Theft Resource Center offer tools and advice for dealing with persistent credit card fraud problems.