

## In general

Whether they're snatching your purse, diving into your dumpster, stealing your mail, or hacking into your computer, they're out to get you. Who are they? Identity thieves.

Identity thieves can empty your bank account, max out your credit cards, open new accounts in your name, and purchase furniture, cars, and even homes on the basis of your credit history. If they give your personal information to the police during an arrest and then don't show up for a court date, you may be subsequently arrested and jailed.

And what will you get for their efforts? You'll get the headache and expense of cleaning up the mess they leave behind.

## Protect yourself against identity theft

There are really two types of identity theft:

- Account takeover--this is what happens when a thief gets your existing credit or debit cards (or even just the account numbers and expiration dates) and goes on a shopping spree at your expense
- Application fraud--this is what happens when a thief gets your Social Security number and uses it (along with other information about you) to obtain new credit in your name

You may never be able to completely prevent either type of identity theft, but here are some steps you can take to help protect yourself from becoming a victim.

## Check yourself out

It's important to review your credit report periodically. Check to make sure that all the information contained in it is correct and there is no fraudulent activity. Every consumer is entitled to a free copy of his or her credit report once a year from each of the three national credit reporting agencies: Equifax, TransUnion, and Experian. You can visit [www.annualcreditreport.com](http://www.annualcreditreport.com) for more information.

## Secure your number

Your most important personal identifier is your Social Security number (SSN). Guard it carefully. Never carry your Social Security card with you unless you'll need it. The same goes for other forms of identification (for example, health insurance cards) that display your SSN. If your state uses your SSN as your driver's license number, request an alternate number.

Don't have your SSN preprinted on your checks, and don't let merchants write it on your checks. Don't give it out over the phone unless you initiate the call to an organization you trust. Ask the three major credit reporting agencies to truncate it on your credit reports. Try to avoid listing it on employment applications; offer instead to provide it during a job interview. Don't leave home with it

Most of us carry our checkbooks and all of our credit cards, debit cards, and telephone cards with us all the time. That's a bad idea; if your wallet or purse is stolen, the thief will have a treasure chest of new toys to play with.

Carry only the cards and/or checks you'll need for any one trip. And keep a written record of all your account numbers, credit card expiration dates, and the telephone numbers of the customer service and fraud departments in a secure place--at home.

### **Keep your receipts**

When you make a purchase with a credit or debit card, you're given a receipt. Don't throw it away or leave it behind; it may contain your credit or debit card number. And don't leave it in the shopping bag inside your car while you continue shopping; if your car is broken into and the item you bought is stolen, your identity may be as well.

Save your receipts until you can check them against your monthly credit card and bank statements, and watch your statements for purchases you didn't make.

### **When you toss it, shred it**

Before you throw out any financial records such as credit or debit card receipts and statements, cancelled checks, or even offers for credit you receive in the mail, shred the documents, preferably with a cross-cut shredder. If you don't, you may find the panhandler going through your dumpster was looking for more than discarded leftovers.

### **Keep a low profile**

The more your personal information is available to others, the more likely you are to be victimized by identity theft. While you don't need to become a hermit in a cave, there are steps you can take to help minimize your exposure:

- To stop telephone calls from national telemarketers, list your telephone number with the Federal Trade Commission's National Do Not Call Registry by registering online at [www.donotcall.gov](http://www.donotcall.gov).
- To remove your name from most national mailing and e-mailing lists, as well as most telemarketing lists, register online with the Direct Marketing Association at [www.dmaconsumers.org](http://www.dmaconsumers.org).
- To remove your name from marketing lists prepared by the three national consumer reporting agencies, register online with the Direct Marketing Association at [www.optoutprescreen.com](http://www.optoutprescreen.com).
- When given the opportunity to do so by your bank, investment firm, insurance company, and credit card companies, opt out of allowing them to share your financial information with other organizations.
- You may even want to consider having your name and address removed from the telephone book and reverse directories.
- Never provide any personal information via phone, letter, or e-mail unless you initiated the transaction. Legitimate businesses should already have your information on file, and will not call you or e-mail you to ask for it.

### **Take a byte out of crime**

Whatever else you may want your computer to do, you don't want it to inadvertently reveal your personal information to others. Take steps to help assure that this won't happen.

Install a firewall to prevent hackers from obtaining information from your hard drive or hijacking your computer to use it for committing other crimes. This is especially important if you use a high-speed connection that leaves you continuously connected to the Internet. Moreover, install virus protection software and update it on a regular basis.

Try to avoid storing personal and financial information on a laptop; if it's stolen, the thief may obtain more than your computer. If you must store such information on your laptop, make things as difficult as possible for a thief by protecting these files with a strong password--one that's 6 to 8 characters long, and that contains letters (upper and lower case), numbers, and symbols.

"If a stranger calls, don't answer." Opening e-mails from people you don't know, especially if you download attached files or click on hyperlinks within the message, can expose you to viruses, infect your computer with "spyware" that captures information by recording your keystrokes, or lead you to "spoofs" (websites that replicate legitimate business sites) designed to trick you into revealing personal information that can be used to steal your identity.

If you wish to visit a business's legitimate website, use your stored bookmark or type the URL address directly into the browser. If you provide personal or financial information about yourself over the Internet, do so only at secure websites; to determine if a site is secure, look for a URL that begins with "https" (instead of "http") or a lock icon on the browser's status bar.

And when it comes time to upgrade to a new computer, remove all your personal information from the old one before you dispose of it. Doing so by using the "delete" function isn't sufficient to do the job; overwrite the hard drive by using a "wipe" utility program. The minimal cost of investing in this software may save you from being wiped out later by an identity thief.

## Recovering from identity theft

Suddenly your bank account is empty, your credit card bills are through the roof, and you're getting late notices for accounts you don't own. Despite your best efforts, your identity has been stolen. What now?

### Time is money

To minimize your losses, act fast. Contact, in this order:

1. Your credit card companies
2. Your bank
3. The three major credit bureaus
4. Local, state, or federal law enforcement authorities

### Your credit card companies

Credit card companies are getting better at detecting fraud; in many cases, if they spot activity outside the mainstream of your normal card usage, they'll call you to confirm that you made the charges. But the responsibility to notify them of lost or stolen cards is still yours.

If you do so in a reasonable time (within 30 days after you discover the loss), you won't be responsible for more than \$50 per card in fraudulent charges. Ask that the accounts be closed at your request, and open new accounts with password protection.

If an identity thief opens new accounts in your name, you'll need to prove it wasn't you who opened them. Ask the creditors for copies of application forms or other transaction records to verify that the signature on them isn't yours.

Whether the identity thief compromises an existing account or opens a new one fraudulently, the creditor involved may want you to fill out a fraud affidavit. Most will accept the uniform affidavit form available from the Federal Trade Commission (FTC); you may obtain it from the FTC at [www.ftc.gov](http://www.ftc.gov).

Follow up your initial creditor contacts with letters indicating the date you reported the loss or theft. Watch your subsequent monthly statements from the creditor; if any fraudulent charges appear, contest them in writing.

### **Your bank**

If your debit (ATM) card is lost or stolen, you won't be held responsible for any unauthorized withdrawals if you report the loss before it's used. Otherwise, the extent of your liability depends on how quickly you report the loss:

- If you report the loss within two business days after you notice the card is missing, you'll be held liable for up to \$50 of unauthorized withdrawals. (If the card doubles as a credit card, you may not be protected by this limit.)
- If you fail to report the loss within two days after you notice the card is missing, you can be held responsible for up to \$500 in unauthorized withdrawals.
- If you fail to report an unauthorized transfer or withdrawal that's posted on your bank statement within 60 days after the statement is mailed to you, you risk unlimited loss.

If your checkbook is lost or stolen, stop payment on any outstanding checks, then close the account and open a new one. Dispute any fraudulent checks accepted by merchants in order to prevent collection activity against you. You may also want to contact a check-guarantee bureau for additional assistance.

### **The three major credit bureaus**

If your credit cards have been lost or stolen, call the fraud number of any one of the three national credit reporting agencies:

1. Equifax (888) 766-0008
2. Experian (888) 397-3742
3. TransUnion (800) 680-7289

You only need to contact one of the three; the one you call is required to contact the other two.

Next, place a fraud alert on your credit report. If your credit cards have been lost or stolen, and you think you may be victimized by identity theft, you may place an initial fraud alert on your report. An initial fraud alert entitles you to one free credit report from each credit bureau, and remains on your credit report for 90 days. If you become a victim of identity theft (an existing account is used fraudulently or the thief opens new credit in your name), you may place an extended fraud alert on your credit report once you file a report with a law enforcement agency. An extended fraud alert entitles you

to two free credit reports within 12 months from each credit bureau, and remains on your credit report for 7 years.

Once a fraud alert has been placed on your credit report, any user of your report is required to verify your identity before extending any existing credit or issuing new credit in your name. For extended fraud alerts, this verification process must include contacting you personally by telephone at a number you provide for that purpose.

If you live in one of the handful of states that allow you to "freeze" your credit report, do so. Once you do, no one--creditors, insurers, and even potential employers--will be allowed access to your credit report unless you "thaw" it for them.

If your state allows you to freeze your credit report, you must contact all three major credit reporting agencies. In some cases, victims of identity theft are not charged a fee to freeze and/or thaw their credit reports, but the laws vary from state to state. Contact the office of the attorney general in your state for more information.

If you discover fraudulent transactions on your credit reports, contest them through the credit bureaus. Do so in writing, and provide a copy of the identity theft report you file. You should also contest the fraudulent transaction in the same fashion with the merchant, bank, or creditor who reported the information to the credit bureau. Both the credit bureaus and those who provide information to them are responsible for correcting fraudulent information on your credit report, and for taking pains to assure that it doesn't resurface there.

## **Law enforcement agencies**

While the police may not catch the person who stole your identity, you should file a report about the theft with a federal, state, or local law enforcement agency. Once you've filed the report, get a copy of it; you'll need it in order to file an extended fraud alert with the credit bureaus. You may also need to provide it to banks or creditors before they'll forgive any unauthorized transactions.

When you file the report, give the law enforcement officer as much information about the crime as possible: the date and location of the loss or theft, information about any existing accounts that have been compromised, and/or information about any new credit accounts that have been opened fraudulently. Write down the name and contact information of the investigator who took your report, and give it to creditors, banks, or credit bureaus that may need to verify your case.

If the theft of your identity involved any mail tampering (such as stealing credit card offers or statements from your mailbox, or filing a fraudulent change of address form), notify the U.S. Postal Inspection Service. If your driver's license has been used to pass bad checks or perpetrate other forms of fraud, contact your state's Department of Motor Vehicles. If you lose your passport, contact the U.S. Department of State. Finally, if your Social Security card is lost or stolen, notify the Social Security Administration.

## Follow through

Once resolved, most instances of identity theft stay resolved. But stay alert: monitor your credit reports regularly, check your monthly statements for any unauthorized activity, and be on the lookout for other signs (such as missing mail and debt collection activity) that someone is pretending to be you.

As the grizzled duty sergeant used to say on the televised police drama, "Be careful out there." The identity you save may be your own.