**How to Protect Yourself from Identity Theft**

1. How many consumers were hit by identity theft?

2. What percentage of identity theft cases were the worst case scenario?

3. What is the most common form of ID theft?

4. What are three low-tech, common sense precautions you can take to help protect yourself?

5. How can you shut our ID thieves before they can cause damage?

6. What are prospective lenders supposed to do when they see a fraud alert on your credit file?

7. Besides your computer what other devices should you make sure are secure?

8. What should be in your ID theft file?

9. What should you check your credit report for periodically?

10. What do crooks steal from your mailbox?

11. Why should you sign up for online access to your accounts?

12. Why should you monitor your cell phone bill?

13. What are three things you should do if you suspect you have been a victim of identity theft?

14. *Critical Thinking*: Why do you think identity theft is so hard for law enforcement to stop?

**How to protect yourself from Identity Theft**

**ID theft is real but overhyped by companies selling pricey services. These eight steps can secure your identity for less.**

Consumer Reports Money Adviser: July 2010

1. Get serious, not scared   |  2. Place security freezes and fraud alerts   |  3. Secure your devices   |  4. Keep an ID-theft file   |  5. Review all your personal data files   |  6. Stop unsolicited credit-card offers   |  7. Monitor accounts often   |  8. Respond rapidly   |  Getting your files 

After trending downward for four years, identity theft is on the rise again. Last year more than 11 million consumers were hit by the crime. That's a record, according to Javelin Strategy and Research, a California company that has surveyed 5,000 adults on the subject every year since 2003. The jump is partly a result of the recession, Javelin says, when fraud tends to spike.

But you don't need to sign up for expensive services offered by credit-reporting bureaus and other companies to keep your identity safe. Most of their products are unnecessary or ineffective, or they duplicate things you can do yourself—free. Our own assessment of some two dozen identity-theft protection products crowding the market found dubious value. Here's how to protect yourself.

**1. Get serious, not scared**

Don't let the horror stories freak you out. The worst-case scenario—where someone opens new credit-card accounts or commits other crimes using your name, Social Security number, or other information—is relatively uncommon. That nightmare happened to less than 1 percent of all U.S. households in 2005, according to the latest data from the U.S. Department of Justice. Half of that group resolved the problem, usually in less than a day to two weeks.

The most common form of ID theft isn't even what most people think of as ID theft. It's old-fashioned credit-card fraud and check-kiting, with someone fraudulently accessing your credit- or debit-card account. It affects about 4 percent of households. What's more, in most cases, your liability is legally limited, and credit-card issuers or banks pay the direct losses, not you. Most victims suffered no out-of-pocket costs last year; those who did lost only $373 on average, half the amount lost in 2007, Javelin says. That's well below the $1 million to $2 million guarantees that many identity-theft protection services trumpet to suggest that your losses could be catastrophic.

You can protect yourself by taking these low-tech, common-sense precautions:

* Never give your Social Security number or other information to strangers who call, text, or send e-mail messages to you, even if they seem legitimate, as with phony "phishing" e-mail that looks like it comes from your bank. And don't write your Social Security number on checks (except those you send to the IRS), noncredit applications, or other forms.
* Never leave your wallet or purse unattended. Don't carry your Social Security card, rarely used credit cards, or written PINs or passwords.
* Store financial account statements, medical records, and tax filings in a secure place at home, especially if you let workers or others inside, and shred those documents when you no longer need them.
* Don't post your date of birth, mother's maiden name, first pet's name, or other personal information on websites like Facebook, Flickr, Friendster, LinkedIn, MySpace, or Twitter. They're often used to verify your identity and could allow an imposter electronic access to your accounts.
* If your bank or credit-card issuer offers free online or mobile alerts that will warn you of suspicious account activity as soon as it's detected, sign up for them. The alerts are different from the expensive credit-monitoring services that banks also sell. (You don't need those.)

**2. Place security freezes and fraud alerts**

You can shut out ID thieves before they cause damage by placing a security freeze on your credit reports at all three major credit bureaus: Equifax ([*www.equifax.com*](http://www.equifax.com/)); Experian ([*www.experian.com*](http://www.experian.com/)); and TransUnion ([*www.transunion.com*](http://www.transunion.com/)). It will prevent anyone from looking at your credit report except for the companies that already have a financial relationship with you, certain government agencies, and other exempt entities. To sign up for one, go to each bureau's home page and look for the security-freeze link.

If a lender can't pull your credit report, it isn't likely to grant new credit to someone else in your name. So a security freeze is an excellent deterrent against fraud. But like all deterrents, it isn't fail-safe. "Some creditors, such as payday lenders, will give credit without getting a credit report," says Rebecca Kuehn, assistant director of the Federal Trade Commission's division of privacy and identity protection.

If you haven't placed a security freeze and you spot a sign of identity theft, put an initial fraud alert on your credit report immediately. That's fast, free, and stays in place for 90 days. It also gives you additional legal protection. After that, request a security freeze.

Prospective lenders are supposed to see a fraud alert on your credit file and call you to find out whether the application is legitimate. Filing a fraud alert is appropriate anytime your identity information is compromised, such as when your wallet, cell phone, or computer is lost or stolen, or if your home or car is broken into. But you should also do it after more-subtle warning signs, such as finding unauthorized charges on your credit-card statement (even if quickly resolved) or failing to receive expected bills or mail.

Fraud alerts are free; security freezes typically cost $5 to $10 per person per credit bureau each time you place or temporarily lift one. Prices range from free to $20 depending on state law. But if you're a victim of ID fraud, freezes are usually free. You can initiate a freeze online directly with each credit bureau; for fraud alerts, you only need to inform one bureau, which will pass the request on to the other two.

**3. Secure your devices**

If you access the Internet on your computer, you probably already know about the need for a firewall; regularly updated anti-virus, anti-spyware, and anti-phishing software; and strong passwords with upper- and lower-case letters, numerals, and symbols like #, &, and $. But you might not think about other wide-open doors to your identity. Make sure your smart phone, iPad, other mobile devices, and portable flash drives containing personal data have security applications and encryption in case they're lost or stolen.

**4. Keep an ID-theft file**

Because identity theft is now a fact of life, it's a good idea to set up a folder for certain documents and data and keep it in a secure place. Include credit reports, security-freeze documents and passwords, copies of annual privacy notices, security-breach notices, and potential ID-theft evidence, such as mail to your address in someone else's name. This is also the place to keep photocopies of the contents of your wallet—the front and back of your driver's license, credit cards, club membership cards, etc.—in case it's lost or stolen.

**5. Review all your personal data files**

Check your credit report periodically for items that you don't recognize—such as accounts, judgments, liens, collections, bankruptcies, and other possible footprints of identity theft—and dispute all erroneous and fraudulent information. Under the federal Fair Credit Reporting Act, you're entitled to one free copy of your credit report every year from each of the big three credit bureaus. Stagger your requests so that you'll get your file from one of them every four months.

You should order your free reports at [*www.annualcreditreport.com*](http://www.annualcreditreport.com/). You're also entitled to an additional free report from each bureau whenever you place an initial fraud alert on your credit report.

Other data brokers keep files on you. Irregularities could mean someone is using your ID to work, tap your health benefits, rent homes, or write bad checks. You have a right to free copies each year and to dispute errors in them (see box at right).

**6. Stop unsolicited credit-card offers**

One way crooks steal your name is by swiping preapproved credit offers from your mailbox to open an account. They can then watch your mailbox to lift the new card you didn't know was coming. You can stop credit bureaus from selling your name to lenders by going to [*www.optoutprescreen.com*](http://www.optoutprescreen.com/) or calling 888-567-8688. Opting out should stop most offers, and it's free.

Other credit offers might come from affiliates of financial services companies that already have a business relationship with you. You can stop them by paying attention to the annual privacy rights notices you get from banks, brokers, and other financial companies and exercising your right under federal law to prevent them from "sharing" (translation: "selling") your information with affiliates and others. Do the same with retailers and websites.

**7. Monitor accounts often**

It's no longer enough to wait for your monthly credit-card or checking account statement to look for suspicious activity. For added protection, sign up for online access to your accounts and check them regularly, even daily. "Almost a third of victims told us they became aware of an identity theft when they noticed missing money from an account," says Katrina Baum, acting division director and senior statistician at the National Institute of Justice. "What this tells me is that it really behooves consumers to be vigilant about checking their financial statements and paying attention to their account activity."

And don't assume that the paper checks listed are legit. Crooks can tap into your funds using fabricated checks with a fictitious name, address, and bank—as long as they use your real account number.

Monitor your telephone bills (landline and cellular) to find any unauthorized "cramming" charges for phony services and purchases. As cell phones increasingly become mobile payment devices, fraudulent charges are showing up there, too.

**8. Respond rapidly**

If you suspect you've been a victim of identity theft, act quickly. Immediately contact your creditors and financial institutions to report unauthorized charges or debits, and close any compromised accounts. Place fraud alerts and security freezes, and get your credit reports from all three credit bureaus so you can review them for irregularities. File a report with your local police and the FTC, and step up your own account monitoring. Chances are good that these actions will resolve the problem in relatively short order and at little or no cost.

Don't let the incident scare you into signing up for identity-theft protection or credit-monitoring services—unless they're free, which is often the case for a limited time after corporate or government data breaches. Make sure a breach notice is not an identity-theft trick itself, and remember to cancel the subscription when the free period runs out.

**Getting your files**

Here are the annual data reports you should check each year for signs of possible ID theft, and where to get them. Most are free.

* **ChoicePoint Full File Disclosure** includes a public-records search, auto and homeowner claims reports, pre-employment background checks, searches for criminal records and evictions, and address history. Go to [*www.choicetrust.com*](http://www.choicetrust.com/) and click on "Access Your Personal Information."
* **Social Security statements** show your earnings history and should match your own earnings records. The government mails the statement annually, but if you've misplaced it or haven't received one, you can order a copy online by going to [*ssa.gov*](http://ssa.gov/) and clicking on "Your Social Security Earnings Statement."
* **Annual statement of medical benefit** is a record of your health-insurance claims and medical treatment. Contact your health insurer to find out how to get this information.
* **MIB consumer file** has coded listings of medical conditions and tests, hazardous hobbies, and driving records. It's used by U.S. and Canadian life insurers to decide whether to issue a policy. Call 866-692-6901 or go to [*www.mib.com/html/request\_your\_record.html*](http://www.mib.com/html/request_your_record.html).
* **Prescription drug history** has information about the medications you've taken over the last five years, including dosages, your refill record, and the doctors who prescribed them. Call Intelliscript at 877-211-4816 and Medpoint at 888-206-0335.
* **Driving record** has your history of moving violations, points, your physical description, address, license status, and other details. Contact your state department of motor vehicles directly to get a copy for a fee. Beware of online middlemen selling the same information at higher costs.
* **Chex Systems and TeleCheck reports** have information about mishandled and overdrawn checking accounts. For Chex Systems, go to [*www.consumerdebit.com*](http://www.consumerdebit.com/) and click on "Order Consumer Report." For TeleCheck, go to [*www.firstdata.com/telecheck/telecheck-request-file-report.htm*](http://www.firstdata.com/telecheck/telecheck-request-file-report.htm).
* **Rental history reports** have information on your rent payments, references, and evictions. For information on getting your report from First Advantage SafeRent, call 800-815-8664 or go to [*www.fadvsaferent.com/consumer\_relations/index.php*](http://www.fadvsaferent.com/consumer_relations/index.php). For your RentBureau report, go to [*www.rentbureau.com/multifamily*](http://www.rentbureau.com/multifamily) and click on "Consumers."

*This article appeared in*[*Consumer Reports Money Adviser*](https://ec.consumerreports.org/ec/ma/order.htm?INTKEY=IW8CMNBA)*.*