



## Parenting

# Identity theft

**How to protect yourself—and your kids** by Jennifer Abbasi

In the U.S. each year, about 9 million people fall victim to identity theft—from a few hundred dollars charged to your credit card to someone posing as you to get a job. A growing concern: It's happening to kids, even babies. What you need to know now:

## Children: the perfect target

Child victims make up only a small percentage of reported cases, but when it happens to kids, it's often the most serious type of theft. Why?

- **It can go undetected for years** (since your baby won't apply for credit anytime soon).
- **It will affect your child's credit and employment history** when the thieves, usually family members, obtain credit cards, and even get jobs.
- **If the thieves are arrested for another crime**, it will go on your child's record, too.

### To protect your child:

- **Don't give out her social security number (SSN)—to anyone.** Though they may ask for it, her doctor and school don't need it unless she's receiving a government service, like free lunch. At the doctor's office, only give out her insurance-card number. Teach her that her SSN is her secret.
- **Opt her out of mailing lists** if you sign her up for a financial account so you'll be able to spot any unusual mailings quickly.

## Lower your risk

According to the Federal Trade Commission (FTC), every American now in his or her 20s or 30s will likely become a victim at some point if identity theft continues at its current rate.

### To protect yourself:

- **Carry only one or two credit cards**—and nothing that lists your SSN—to save yourself some hassle if your wallet is stolen.
- **Keep a photocopy of the front and back of all of your cards** at home so you can quickly call and cancel anything that's missing. If you keep copies at work, make sure they're locked up.
- **Substitute your driver's license for your SSN** whenever possible, such as at a doctor's office. (You will have to give it out sometimes, like when you apply for a job or authorize a credit check in order to get a loan, an apartment rental, or new utilities.)
- **Check your bank statements and credit card bills carefully** for activity you don't recognize.



## 3 red flags that your identity has been stolen:

1. **Withdrawals on your bank-account statement** that you didn't make
2. **On your credit report: an address you don't recognize**, accounts (especially overdues) that aren't yours, and applications you didn't fill out (credit card applications stay on your report for only two years)
3. **Calls from stores or vendors that you never visited**, or calls and mailings about accounts and purchases you don't know anything about



## 3 red flags that your child's identity has been stolen:

1. **Suspicious mail**, like preapproved credit cards and other financial offers normally sent to adults, starts coming in her name.
2. **You try to open a financial account** for her but find one already exists, or the application is denied because of a poor credit history.
3. **A credit report already exists in her name.** If she has one she's probably been targeted, since only an application for credit starts a report.

## If you think you or your child might be a victim:

**STEP 1** Call one of the three national credit-reporting agencies to place a fraud alert (one call will activate the other two). The agency will then verify that it's you if anyone tries to authorize new credit within 90 days. If you request a permanent alert in writing, you'll be notified directly regarding requests for new credit for the next seven years. If your child was the victim, the agencies must remove all suspicious activity from her report once you prove

she's a minor. To place a fraud alert, call Equifax, 800-525-6285; Experian, 888-397-3742; or Trans Union, 800-680-7289. It's an automated call.

**STEP 2** Cancel lost or stolen credit and ATM cards, and close accounts that have been tampered with or, worse, opened. To dispute new accounts with financial institutions, you'll need to provide an ID Theft Affidavit, which is available on the Federal Trade Commission (FTC) website.

**STEP 3** File an incident report with the police, even if it's just for a lost wallet. If you know someone is misusing your info, file an identity-theft report and make sure you keep copies of all police documents.

## To protect yourself in cyberspace:

- Buy a firewall program to block your computer from being monitored and hacked into. Try Norton Internet Security (\$70).
- If you have cable or DSL, turn off your computer when you're not using it so hackers have limited time to do their thing.
- Complicate your passwords by mixing numbers and letters, and don't let sites "remember" your password.
- Never give out personal information (like your SSN) over e-mail.
- Only shop at secure sites, meaning a padlock icon in the lower-right-hand corner of the screen, a "VeriSign" logo (a big checkmark), or "https" in the URL of the check-out page, not just "http."
- Log off (don't just close the window) after banking or shopping.

## How identity is stolen:

30%	Lost or stolen wallet, checkbook, or credit card
15%	By friends, relatives, and acquaintances
15%	By an employee at a business where your info's on file, like the doctor's office
9%	Online
8%	stolen mail
7%	By an employee who processes a purchase you make
7%	Other
6%	From a company that handles your financial data, like your bank or employer
1%	Dumpster diving

### What to do today:

#### Get a free credit report

Each of the three credit bureaus is required to send you a copy of your report once a year at your request. Go to [AnnualCreditReport.com](http://AnnualCreditReport.com) or call 877-322-8228. Tell them to include only the last four digits of your SSN when they send your report. **Tip:** Stagger your requests to the three agencies over the year to set up your own credit-check system.

### HAVE QUESTIONS? (And want to talk to a real live person?)

Contact the FTC or the Identity Theft Resource Center (ITRC). The ITRC can answer questions about child identity theft—for example, what to do if the thief is a family member.

FTC: 877-438-4338 or [consumer.gov/idtheft](http://consumer.gov/idtheft)  
ITRC: 858-693-7935 or [idtheftcenter.org](http://idtheftcenter.org)

SOURCES: Joanna Crane, manager of the identity theft program of the Federal Trade Commission; Linda Foley, Identity Theft Resource Center; Javelin Strategy & Research's 2006 Identity Fraud Survey Report