

# Protect Yourself from Identity Theft

**12 million** Americans were victims of identity theft in 2011.

Source: Reuters



Nineteen people each minute become victims of identity theft.\* It can take months to undo the damage done to your identity and credit. Don't become a wily thief's next victim—follow these tips to protect your identity.

\*Source: TransUnion

## 7 ways to keep your information secure

- 1 Guard your privacy.** Don't share personal information (e.g., your address, phone numbers, Social Security number, date of birth or birth place) on social networks. And, don't fall prey to scams that ask for personal information over email.
- 2 Install security features.** If you keep personal or financial documents on your computer, install a firewall, use anti-virus and anti-spyware software, use a secure wireless network and make sure your browser is always up-to-date.
- 3 Keep your personal and financial information secure.** Whether you keep it in a filing cabinet or online in the cloud, make sure you secure it with a key or a strong password.
- 4 Always use strong passwords online,** and change them periodically.
- 5 Shred what you don't need.** Destroy documents, bills, receipts and junk mail that you don't need, especially if it contains your personal information.
- 6 Check your mail.** Never leave mail in your mailbox for a long period of time. If you're going on vacation, request a hold from the U.S. Postal Service to stop mail delivery until you return.
- 7 Keep an eye out for unauthorized activity** in your bank and credit card accounts. Online banking makes it easy to check your activity as often as you wish. Also, be sure to check the information on your credit report to make sure it is correct.



Your homeowner's insurance policy may have coverage for identity theft. Call your agent to find out.

# What to do if your identity has been stolen

Having your identity stolen can be a scary experience, but if you act quickly, you can limit the impact on your credit. Here's how:

- **Place a fraud alert on your account** through the three credit reporting companies—**Equifax, TransUnion** and **Experian**. Fraud alerts are active for 90 days; after that, you'll have to reactivate the alert if you feel that it's necessary.
- **File a report** with your local police department.
- **File an Identity Theft Report** using the tools available on the Federal Trade Commission's website at [www.consumer.ftc.gov](http://www.consumer.ftc.gov).
- **Contact your bank, credit card companies and loan companies** to place a fraud alert on your account or close your existing accounts.

If a thief has stolen your wallet or purse, he can get your address from your identification. **Change the locks on your home** to be on the safe side.

## *If your credit, ATM or debit card is lost or stolen:*

- **Report your loss immediately to the card issuer.** Once you report it, you won't be responsible for unauthorized purchases made thereafter.
- **Get a copy of the transaction history** associated with the lost or stolen card, and look for unauthorized charges.
- **Follow up with your card company.** Write a letter to the card issuer to confirm that you reported the card lost or stolen.
- **File a police report.**

**If your identification has been lost or stolen, contact the DMV for a replacement.** Ask them to note the loss or theft in your file, or ask for a new identification or driver's license number.

Credit or financial fraud comprises **28%** of identity fraud cases. Fraud concerning phone, utility, bank and employment comprises more than **50%** of identity theft cases.

Source: TransUnion

## 3 ways to protect your information on your smartphone

1. Protect your home screen with a password.
2. Only download apps through a trusted website that monitors the apps.
3. Don't reveal too much personal information on social media sites.

Smartphone users are **33%** more likely to be victims of identity theft.

Source: Reuters

