



Identity Theft

If You Become a Victim

- Contact these three major credit bureaus and request that a fraud alert be placed on your credit report:
Equifax, 800-525-6285;
Experian, 888-397-3742; and
TransUnion, 800-680-7289.
- Close the accounts that may have been tampered with or opened fraudulently.
- File a report with your local police or the police in the community where the identity theft took place.
- Report the theft to the Federal Trade Commission at **ftc.gov/idtheft** or 877-438-4338.

In identity theft, criminals get hold of personal information such as your social security number and use this to get credit cards and even car and home loans in your name. Sometimes, victims' only warning that this has happened is a collection agency's call, demanding payment on a purchase or loan. To fight identity theft, banks use a combination of safeguards, including employee training, strict privacy policies, rigorous security standards and encryption systems. Legally, you are not liable for loans you did not agree to, but restoring your identity can be a huge inconvenience.

Be Aware of the Threat

Identity thieves use a number of methods to obtain personal data. Take these steps to protect yourself:

1. Tear up receipts, bank statements and unused credit card offers before throwing them away.
2. Keep your personal information in a secure place at home, especially if you have roommates, employ outside help or are having work done in your house.

3. Make sure that your mailbox is secure.
4. Protect your PINs and passwords; use a 10-digit combination of letters and numbers for your passwords, and change them periodically.
5. Monitor account activity on a regular basis. Sign up to view your financial accounts and billing statements online.
6. Don't give out personal information on the phone, through the mail or over the Internet unless you know who you are dealing with.
7. When conducting business online, make sure your browser's padlock icon is active.
8. Don't reply to e-mail or pop-up messages that ask for personal or financial information, and don't click on links in the message. Don't cut and paste a link from the message into your Web browser—fraudsters can make links look like they go one place, but that actually send you to a different site.
9. Use antivirus and antispyware software, as well as a firewall, and update them all regularly.
10. Be cautious about opening any attachment or downloading any files from e-mails you receive, regardless of who sent them.
11. Review your credit report to ensure accuracy. You may order free copies at **annualcreditreport.com**

Prevent Identity Theft

DETER — Minimize Your Risk by safe guarding your personal information

DETECT — monitor your accounts and bank statements each month, and check your credit report regularly

DEFEND — as soon as you suspect identity theft respond so that you can recover