

IDENTITY THEFT



SECTION 4: SAFETY AT HOME

Protect Your Personal and Electronic Information (Identity Theft)

Identity theft is a serious and costly crime. People whose identities have been stolen can spend months or years cleaning up the mess thieves have made of their good name and credit record. In the meantime, victims may lose job opportunities, be refused loans, housing or cars, or even get arrested for crimes they didn't commit.

Top 10 Tips for Identity Theft Prevention

The following tips can help you lower your risk of becoming a victim.

- 1. The best defense is a good offense.** Contact the fraud department of any of the three consumer reporting companies— Equifax, Experian and Trans Union—to place a fraud alert on your credit report. The fraud alert automatically lets credit card companies and other creditors know they must contact you before opening any new accounts or making any changes to your existing accounts. You only need to contact one of the three companies to place an alert; that company will transfer the alert to the other two.

Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241

Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013

TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

- 2. Don't get caught by "phishing".** Scam artists "phish" for victims' information by posing as representatives of banks, stores or government agencies. This is done over the phone, through regular mail, and especially via e-mail. Don't respond to a request to verify your account number or password. Don't give out your personal information unless you made the contact. Legitimate companies will not request this kind of information in this way.
- 3. Keep your identity from getting trashed.** Invest in a paper shredder and shred all papers with personal information before you throw them away. Shred unwanted credit card applications and "convenience checks" that come in the mail, credit card receipts with your account number, outdated financial papers and papers containing your clients' personal information.

(continued)

IDENTITY THEFT



4. **Control your personal financial information.** Many states have laws requiring banks and other financial institutions to get your permission before sharing your personal financial information with outside companies. You also have the right to limit the sharing of your personal financial information with most of your companies' affiliates. Write to your companies that you want to "opt-out" of sharing your personal financial information with their affiliates.
5. **Shield your computer from viruses and spies.** Protect your personal information on your home computer. Use passwords with at least eight characters, including a combination of letters, numbers, and symbols. Use firewall and virus protection software and update it regularly. Download free software only from sites you know and trust, and don't install software without knowing what it is. Set Internet Explorer browser security to at least "medium." Don't click on links in pop-up windows or in spam e-mail, and don't download any file from an e-mail address you don't know.
6. **Click with caution** When shopping online, check out a Web site before entering your credit card number or other personal information. Read the privacy policy and look for opportunities to opt out of information sharing. (If there is no privacy policy posted, shop elsewhere!) Enter personal information only on secure Web pages with "https" in the address bar and a closed padlock symbol at the bottom of the browser window. These are signs that your information will be encrypted or scrambled, protecting it from hackers. If you don't see these signs, order by telephone. Also, you should always use a credit card rather than a debit card to make online purchases.
7. **Check your bills and bank statements.** Open your credit card bills and bank statements right away. Check for any unauthorized charges or withdrawals and report them immediately. Call if bills don't arrive on time. It may mean that someone has changed contact information to hide fraudulent charges.
8. **Stop pre-approved credit offers.** Stop most pre-approved credit card offers by calling toll-free 888-5OPTOUT (888-567-8688) to have your name removed from credit bureau marketing lists. These mail packages are valuable for identity thieves, who steal your mail and fill out the applications in your name.
9. **Ask questions.** Ask questions whenever you are asked for personal information that seems inappropriate. Ask how the information will be used and if it will be shared. Ask how it will be protected. Explain that you're concerned about identity theft. If you're not satisfied with the answers, consider going somewhere else.

(continued)

IDENTITY THEFT



- 10. Check your credit reports — for free.** One of the best ways to protect yourself from identity theft is to monitor your credit history. You can get one free credit report every year from each of the three national credit bureaus. Request all three reports at once, or order from a different bureau every four months. (More comprehensive monitoring services from the credit bureaus cost from \$44 to over \$100 per year.) Order your free annual credit reports by phone, toll-free, at 877-322-8228, or online at www.annualcreditreport.com.

If you think your identity has been stolen, here's what to do now:

1. Contact the fraud departments of any one of the three major credit bureaus to place a fraud alert on your credit file. The fraud alert requests creditors to contact you before opening any new accounts or making any changes to your existing accounts. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will be automatically notified to place fraud alerts. Once the alert is placed, you may order a free copy of your credit report from all three major credit bureaus.
2. Close the accounts that you know or believe have been tampered with or opened fraudulently. Use the ID Theft Affidavit when disputing new unauthorized accounts.
3. File a police report. Get a copy of the report to submit to your creditors and others that may require proof of the crime.
4. File your complaint with the Federal Trade Commission. The FTC maintains a database of identity theft cases used by law enforcement agencies for investigations.

(Sources: The Federal Trade Commission, The Office of Privacy Protection in the California Department of Consumer Affairs)