

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

ExperianSM: 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.

CONTINUED

SECTION 4: SAFETY AT HOME Protect Your Personal and Electronic Information CONT.,**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credit card applications and “convenience checks” that come in the mail, credit card receipts with your account number, outdated financial papers and papers containing your clients’ personal information.

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 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.

CONTINUED

SECTION 4: SAFETY AT HOME Protect Your Personal and Electronic Information CONT.,**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.

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:**1. Report the fraud to the three major credit bureaus.**

You can report the identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system, which will ask you to enter your Social Security number and other information to identify yourself. The automated system allows you to flag your file with a fraud alert at all three bureaus. This helps stop a thief from opening new accounts in your name. The alert stays on for 90 days. Each of the credit bureaus will send you a letter confirming your fraud alert and giving instructions on how to get a free copy of your credit report.

Experian 1-888-397-3742 Equifax 1-800-525-6285 TransUnion 1-800-680-7289

2. Report the crime to the police.

Ask the police to issue a police report of identity theft. Give the police as much information on the theft as possible, including copies of your credit reports showing the items related to identity theft. (Black out items not related to identity theft.) Give the police any new evidence you collect to add to your report. Be sure to get a copy of your police report. You will need to give copies to creditors and the credit bureaus.

CONTINUED

SECTION 4: SAFETY AT HOME Protect Your Personal and Electronic Information CONT.,**3. Request information on fraudulent accounts.**

When you file your police report of identity theft, the officer may give you forms to use to request account information from credit grantors, utilities or cell phone service companies. When you write to creditors where the thief opened or applied for accounts, send copies of the forms, along with copies of the police report. Give the information you receive from creditors to the officer investigating your case.

4. Call creditors.

Call creditors for any accounts that the thief opened or used. When you call, ask for the security or fraud department. Examples of creditors are credit card companies, other lenders, phone companies, other utility companies, and department stores. Tell them you are an identity theft victim. Ask them not to hold you responsible for new accounts opened by the thief. If your existing credit accounts have been used fraudulently, ask the credit issuers to close those accounts and to report them to credit bureaus as "closed at consumer's request." If you open a new account, have it set up to require a password or PIN to approve use. Don't use your mother's maiden name or the last four numbers of your Social Security number as your password. Ask the creditors to give you copies of documentation on the fraudulent accounts.

5. Review your credit reports carefully.

When you receive your credit reports, read them carefully. Look for accounts you don't recognize. Look in the inquiries section for names of creditors from whom you haven't requested credit. You may find some inquiries identified as "promotional." These occur when a company has gotten your name and address from a credit bureau to send you an offer of credit. Promotional inquiries are not signs of fraud. (By calling to report identity theft, your name will be automatically removed from the mailing list to receive unsolicited credit offers of this kind.) Also, as a general precaution, look in the personal information section to verify your Social Security number, address and name.

If you find anything you don't understand, call the credit bureau at the telephone number listed on the report. Tell them you want to block, or remove, any information on the report that is the result of identity theft. (You must send a police report of identity theft to support this request.)

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