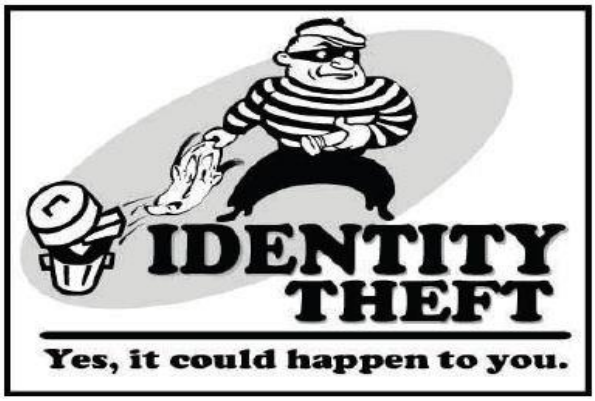
Identity Theft Prevention



How to Protect Yourself from Identity Theft

1. **Protect your Social Security number**. Don't carry your Social Security card or other cards that show your SSN.

2. **Use caution** when giving out your personal information. Scam artists "phish" for victims by pretending to be banks, stores or government agencies. They do this over the phone, in e-mails and in postal mail.

3. **Treat your trash carefully.** Shred or destroy papers containing your personal information including credit card offers and "convenience checks" that you don't use.

4. **Protect your postal mail**. Retrieve mail promptly. Discontinue delivery while out of town.

5. **Check your bills and bank statements**. Open your credit card bills and bank statements right away. Check carefully 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.

6. **Check your credit reports**. Review your credit report at least once a year. Check for changed addresses and fraudulent charges.

7. **Stop pre-approved credit offers.** Preapproved credit card offers are a target for identity thieves who steal your mail. Have your name removed from credit bureau marketing lists. Call toll-free 888-5OPTOUT (888-567-8688).

8. **Ask questions.** Ask questions whenever you are asked for personal information that seems inappropriate for the transaction. Ask how the information will be used and if it will be shared. Ask how it will be protected. If you're not satisfied with the answers, don't give your personal information.

9. **Protect your computer.** Protect personal information on your computer by following good security practices.

• Use strong, non-easily guessed passwords.

• Use firewall, anti-virus, and antispyware software that you update regularly.

• Download software only from sites you know and trust and only after reading all the terms and conditions.

• Don't click on links in pop-up windows or in spam e-mail.

10. Use caution on the Web. When shopping online, check out the website before entering your credit card number or other personal information. Read the privacy policy and take opportunities to opt out of information sharing. Only enter personal information on secure Web pages that encrypt your data in transit. You can often tell if a page is secure if "https" is in URL or if there is a padlock icon on the browser window.

<u>Steps to Take if Your Data is Compromised or Stolen</u>

1. Contact a Major Credit Bureau Agency to Place a **Fraud Alert on Your Credit Reports.** Fraud alerts can help prevent an identity thief from opening any more accounts in your name. Contact the toll-free fraud number of any of the three consumer reporting companies below to place a fraud alert on your credit report. *You only need to contact one of the three companies to place an alert.* The company you call is required to contact the other two, which will place an alert on their versions of your report.

2. **Close the accounts that you know, or believe, have been tampered with or opened fraudulently.** Call and speak with someone in the security or fraud department of each company with which you are closing an account. Follow up in writing, and include copies (NOT originals) of supporting documents. It's important to notify credit card companies and banks in writing. Send your letters by certified mail, return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures. If the identity thief has made charges or debits on your accounts, or on fraudulently opened accounts, ask the company for the forms to dispute those transactions.

3. **File a report with your local police or the police in the community where the identity theft took place.** It is important to report identity theft to your local police as soon as you become aware of being a victim. Get a copy of the police report. You may need copies of the police report when notifying creditors.

4. **Contact the Social Security Administration Fraud Hotline.** If you are the victim of a stolen Social Security number, the SSA can provide information on how to report the fraudulent use of your number and how to correct your earnings record. We encourage you to contact the Fraud Hotline immediately once you suspect identity theft. The web site also provides tips on using and securing your Social Security number. Visit the SSA web site for advice on keeping your number safe.

5. **File a complaint with the Federal Trade Commission.** By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves and stop them. The FTC can refer victims' complaints to other government agencies and companies for further action, as well as investigate companies for violations of laws the agency enforces.