

STOP IDENTITY THEFT

A DOZEN WAYS TO PREVENT IDENTITY THEFT

Shred all unnecessary documents containing personal information. Shred credit card offers and “convenience checks” that you do not use. Shred all credit cards and bank statements except the most current.

Do not carry your Social Security card with you. Minimize the identification information and the number of credit cards you carry with you. Give your Social Security number only when absolutely necessary.

Destroy old or expired credit cards. Close all inactive credit card and bank accounts.

For ATM and debit cards, choose a PIN different from your address, telephone number, date of birth, or the last four digits of your Social Security number.

Memorize your PIN. Do not write it on your ATM or debit card, or keep it written on a piece of paper somewhere in your wallet or purse.

Keep personal information in a safe place. If you employ outside help or are having service work done in your home, keep your personal information secure and out of sight.

Do not give out personal information over the telephone, through the mail, or over the Internet unless you have initiated contact or know the business with which you are dealing with.

Order a FREE copy of your credit report from one of the three major credit reporting agencies.

1. Equifax 800-685-1111 or online at www.equifax.com
2. Experian 888-397-3742 or online at www.experian.com
3. Trans Union 800-888-4213 or online at www.transunion.com

You can also order your free annual credit report by phone at 877-322-8228 or online at www.annualcreditreport.com.

Periodically check your ATM and debit card activity for unauthorized use. Check bank statements, canceled checks and credit cards for suspicious activity.

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. If you are not satisfied with the answers, **DO NOT** give out your personal information.

Identity theft thieves “phish” for victims by pretending to be banks, retailers, government agencies and charitable organizations. They do this over the phone, by regular mail and over the Internet. Don’t take the bait. Never give out personal information unless you initiate the contact. Do not respond to requests to verify your account number, PIN number or password.

Click with caution when shopping online. Only enter personal information on a secure web site and shield your computer from viruses and spies to block out hackers. Do not click on links in pop-up windows or in spam e-mail.

