ID Theft Prevention

1. Buy a cross-cut type shredder. Shred all your important papers and especially pre-approved credit applications received in your name and other financial information that provides access to your private information.

2. Watch out for *Dumpster Divers.* Don't throw anything away that someone could use to become you. Use that shredder!

3. Be careful at ATM's or anywhere you use your "pin number". *Shoulder Surfers* may be lurking nearby.

4. Have boxes of checks delivered to your bank or post office box – not to your home address.

5. Do not put checks in the mail from your home mailbox. Drop them off at a post office mail drop. Mail theft is common. It's easy to change the name of the recipient on the check with an acid wash.

6. When you are expecting a new credit or debit card in the mail, watch the calendar to make sure that you get the card within the appropriate time. If not received by a certain date, call the card grantor immediately and find out if the card was sent. Find out if a change of address was filed.

7. Cancel all credit cards that you do not use or have not used in 6 months. Thieves use these very easily – open credit is a prime target.

8. Put passwords on all your accounts and do not use your mother's maiden name. Don't carry a list of passwords in your wallet.

9. Get a post office box or a locked mailbox.

10. Ask all financial institutions, doctors' offices, etc., what they do with your private information and make sure they shred it and protect your information.

11. Empty your wallet of all extra credit or debit cards and social security numbers, etc. Do not carry any identifiers you do not need. Don't carry your birth certificate, social security card or passport, unless necessary.

12. Never give out personal information over the phone to someone you don't know. If they tell you they are a credit grantor of yours, call them back at the number that you know is the true number, and ask for that party to discuss personal information. Provide only information that you believe is absolutely necessary.

13. Do not put your social security number on your checks or your credit receipts. Businesses should not need your SS number to identify you. If a government agency requests your social security number, there must be a privacy notice accompanying the request.

14. Consider removing your telephone number from your checks.

15. Do not put your credit card account number on the Internet (unless it is encrypted on a secure site). Don't put account numbers on the outside of envelopes, or on your checks.

16. If your health insurance carrier, school, employer, or other institution uses your social security number for your identification number, ask if that can be changed.

17. Monitor all your bank accounts and credit card statements each month. Check to see if there is anything that you do not recognize. Call immediately if you suspect fraud.

18. Order your credit report from all three credit reporting agencies at least once a year. Review it carefully. If you see anything that appears fraudulent, immediately put a fraud alert on your report; correct any mistakes in writing.

19. Take your name off all promotional lists. Call the three credit reporting agencies numbers to opt out of pre-approved offers.

20. Consider making your phone an unlisted number or just use an initial.

21. Make a list of all your credit card account numbers and bank account numbers (or photocopy), along with customer service phone numbers; keep in a safe place. Do not keep it on the hard drive of your computer if you are connected to the internet.

# # # # # # # # # # # # #

Credit Reporting Agencies: www.annualcreditreport.com
Equifax: 1-800-525-6285; www.equifax.com
Experian: 1-888-397-3742; www.experian.com
TransUnion: 1-800-680-7289; www.transunion.com

To get off promotional lists, write to the following:

Direct Marketing Association
Mail Preference Service
P. O. Box 9008
Farmingdale, NY 11735

Direct Marketing Association
Telephone Preference Service
P. O. Box 9014
Farmingdale, NY 11735

To get off pre-approved credit card mailings, call 1-888-567-8688 or go to www.optoutprescreen.com.

Contact Creditors and Financial Institutions:
If a credit card or banking account has been tampered with, you should immediately contact their security or fraud department and close the account. If you open a new account, select a new password or PIN, and change passwords on all unaffected accounts as well. Follow up any telephone call with a certified letter, especially when it pertains to a credit card account.

File a Report

- Contact your local police department or sheriff's office; keep a copy for your records.
- Contact the Federal Trade Commission (FTC), which maintains the Identity Theft Data Clearinghouse and provides information to identify theft victims. Call toll-free 1-877-ID-THEFT (1-877-438-4338); send mail to Identify Theft Data Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580, or file an ID Theft Affidavit online at www.consumer.gov/idtheft.
- If your mail has been stolen, notify your local postal inspector at https://postalinspectors.uspis.gov. Mail theft is a federal crime.
- Notify the Social Security Administration if your Social Security Number has been misused. Call the SSA Fraud Hotline at 1-800-269-0271; fax: 410-597-0118; write: SSA Fraud Hotline, PO Box 17768, Baltimore, MD 21235; or e-mail: oig.hotline@ssa.gov.