IDENTITY THEFT

A thief can obtain information by:	**Here are some simple steps you can take to protect yourself:**
Stealing a wallet and purse containing your ID, credit, and bank cards.	Limit the amount of identification and the number of credit cards you carry. Carrying only the ID, insurance and credit cards you use often. Keep the rest in a secure location at home. Store your wallet or purse in a secure location while you are at work or other public places Do not have your Social Security or driver's license number printed on your checks.
Stealing your mail, including bank and credit card statements, pre-approved credit offers, new checks, and tax information.	Don't leave envelopes with checks inside in an unsecured mailbox. Try to use a sealed U.S. Post Office mailbox for your correspondence. If you have an "open" mailbox, make an effort to pick up your mail promptly. Don't leave mail in your mailbox overnight or on weekends Stop your mail while on vacation or have a friend pick it up for you. Promptly and thoroughly review financial statements, verify that account information is correct. Dispute anything that looks suspicious.
Completing a change-of-address form to divert your mail to another location.	Watch for unexplained interruptions in your mail service. If there is one, or your mail volume suddenly decreases, contact your local post office and verify that your address has not been changed without your knowledge.
Dumpster diving (searching) through your trash for personal data.	Shred documents that contain personal information before you throw them away.
Finding your personal information in your home.	Memorize your PINs and passwords. Do not write them down or store them anywhere in your home.

Using personal information you shared on the Internet.	Do not release personal information on online bulletin boards or in non-secure emails or chat rooms. When making transactions over the Internet, use only a secure site. Look for the "lock" icon on the Web page. Shop only through on-line sites you know and trust, or where you see encryption technology. Look for a padlock icon or “https” in the URL.
Posing as a representative from a company or government agency through bogus email or telephone contacts.	Protect your Social Security number and credit card account numbers. Don't give them to anyone over the telephone if they've called you. Hang up and call the company back using a telephone number you find (NOT ONE THEY GIVE YOU) to check that it was a legitimate inquiry. Never give your Personal Identification Numbers (PINs) to anyone, for any reason. Watch out for a scam that is known as "phishing," where someone calls or emails you and claims to be from one of your accounts (Internet provider, financial institution, credit card, etc.) and wants to "verify" your information by requesting that you give them your account number, Social Security number, etc. DO NOT GIVE OUT THIS INFORMATION. Immediately call those companies and notify them about these abuses.
“Shoulder surfing” at the Automated Teller Machine or telephone booth to watch you enter your PINS.	Make sure you are not being watched when you make withdrawals or access accounts over a public telephone.

Other action you can take:
Cancel unused credit cards.

Completely destroy or shred copies of credit card receipts, statements from financial institutions, tax returns and loan applications before discarding them. Keep the ones you need in a SECURE place.

Review a copy of your credit report at least once a year.

If you feel you have been a victim of identity theft notify the correct authorities.

Contact the three Credit bureaus and report the incident. Then provide written notification to confirm your telephone contact.

Credit Bureaus:

Trans-Union
P.O. Box 390
Springfield, PA 19064-0390
1-800-680-7289

Equifax
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-525-6285

Experian
P.O. Box 949
Allen, TX 75013-0919
1-888-397-3742

Contact the financial institution(s) where you have accounts. Obtain new account numbers and have a code word placed on your accounts.

File a report with your local law enforcement agency and obtain a report number for future reference.

Request new accounts and PINs if your credit cards or ATM cards have been compromised.

Close the account and ask your financial institution to notify the appropriate check verification service if your checks have been stolen or misused. You should also contact the major check verification companies yourselves:

- TeleCheck: **1-800-710-9898**
- Certegy, Inc.: **1-800-437-5120**

Call SCAN (1-800-262-7771) to find out if anyone has been passing bad checks in your name.

Report the fraudulent use of your Social Security Number to the Social Security Administration: Report Fraud — 1-800-269-0271.

Visit your state's motor vehicles office and advise them of the incident.

Obtain a new operator's license and number. NOTE: You do not have to use your SSN for your driver's license. YOU MAY request another number for your driver's license.

For more information, visit the Federal Trade Commission website at:
http://www.ftc.gov/bcp/edu/microsites/idtheft/