Best Practices to Help Protect Yourself from Identity Theft

- Never leave your wallet or bank statements lying around. Use caution even at home- most times the victim knows the identity thief.
- Sign new credit cards as soon as you receive them. Cut-up and throw away the old cards. Shred or tear up unwanted pre-approved credit applications.
- When signing receipts, draw a line through any blank spaces. Save receipts until you reconcile with your bank statements.
- Never give your social security number to anyone over the phone and never send this information by email.
- Always keep your PINs confidential. Don't write this info on anything that you keep in your purse.
- Review all monthly statements carefully and report any unusual charges immediately.
- Shred anything that has your social security or account information on it.
- On your home computer, install anti-virus and anti-spyware software. Also use a firewall and keep everything up to date.
- Beware of pretext calling or phishing scams. Legitimate businesses should not call and ask for your social security number and other important information. If you suspect fraud, get their number to call them back. Usually, the phone number will be disconnected or not a valid, working number.
- When making internet purchases, make sure that the page you are on is secure. You should see either a closed padlock or an unbroken key down in the bottom of the browser. This reflects that this site is secure. Another way to tell is also if the website address begins with "https".