Identity Theft

What To Do If You're a Victim
If you're a victim of identity theft, the Federal Trade Commission (FTC) recommends that you do the following:

• Contact the fraud department of the three major credit bureaus to place a fraud alert on your credit file. The fraud alert requests creditors to contact you before opening any new accounts or making any changes to your existing accounts.

• Close the accounts that you know or believe have been tampered with or opened fraudulently. Use the ID Theft Affidavit (available on the FTC website and accepted by the three major credit bureaus) when disputing new unauthorized accounts.

• File a police report. Get a copy of the report to submit to your creditors and others who may require proof of the crime.

• File your complaint with the FTC at www.consumer.gov/idtheft. The FTC maintains a database of identity theft cases used by law enforcement agencies for investigations. Filing a complaint also helps the agency learn more about identity theft and the problems victims are having so that it can better assist you.

Identity Theft
Identity theft is the fastest growing crime in America, affecting half a million new victims each year. Identity theft is the taking of another person's identity to obtain credit and credit cards, bank accounts, and other items. People steal identities for many reasons, such as to obtain personal information and use it for financial gain.

How To Prevent Identity Theft

• Do not give out personal information over the phone, through the mail, or online unless you initiated the contact. Always be aware of potential scams.

• Never give out your Social Security number, driver's license number, or any other information over the telephone unless you initiated the contact.

• Protect your personal information when using internet services. Always use secure websites and keep it up-to-date.

• Create hard-to-guess passwords that are not found in a dictionary. Select passwords with at least eight characters and that include a mix of numbers and both uppercase and lowercase letters.

• Minimize the identification information and the number of cards you carry. Take only what you'll actually need.

• Do not use the same password for all of your accounts. Use different passwords for different accounts.

• Be careful when using ATMs and long-distance phone cards. Someone may look over your shoulder and get your PIN numbers.

• Make a list of all your credit and bank account numbers and bank account numbers with customer service phone numbers, and keep it in a safe place.

• If you receive a new credit card and it doesn't arrive in an appropriate period of time, call to make sure someone has not filled a charge of address for you.

• Never submit your credit card number to a website unless it is encrypted on a secure site. Look at the bottom of the screen for a padlock symbol. Do not select to save your information on the site for future transactions.

• Pay attention to your billing cycles. Follow up with creditors if bills don't arrive on time. A missing credit card bill could mean an identity thief has taken over your credit card account and changed your address.

• Check your credit card accounts and bank accounts at least once a month.

• Order your credit report at least twice a year from the three major credit bureaus (Equifax: www.equifax.com), Experian (www.experian.com), and Trans Union (www.transunion.com). The Fair Credit Reporting Act allows you to get one free credit report from each of the three major credit bureaus once per year. Visit www.annualcreditreport.com.

• Correct mistakes on your credit report in writing. Send a letter to the credit reporting agency and identify the problem item by item, include a copy of the credit report, and send the letter return receipt requested.