Identity Theft Prevention:

What is identity theft?

Identity Theft occurs when someone uses your personally identifying information like your name, Social Security number, or credit card number without your permission to commit fraud or other crimes. According to the Federal Trade Commission, approximately 9 million Americans have their identity stolen each year. Identity thieves may use your personally identifying information to establish lines of credit, bank accounts, credit card accounts and other forms of credit. You may not find out your identity has been compromised until you receive a bill in the mail or are contacted by a debt collector.

Is identity theft a crime?

Identity Theft is a Crime in the State of New Jersey.

In New Jersey, Identity Theft is covered by the Wrongful Impersonation statute (N.J.S.A. 2C:21-17), which makes it an offense to impersonate another, assume a false identity, or obtain personally identifying information pertaining to another person and use that information or assist another in using that information to obtain a benefit, services or attempt to avoid a debt or avoid prosecution for a crime by using the name of the other person. New Jersey's Wrongful Impersonation ranges from a Disorderly Person's offense to a crime of the 2nd degree in cases where five or more identities have been used to obtain a benefit or service in the amount of $75,000 or more or the identities if five or more people have been used to obtain a benefit.

How does identity theft occur?

Your personally identifying information may be compromised through a variety of methods.

Dumpster Diving - Looking through your garbage for bills or other paper with your personal information on it.

Skimming - Skimmers are small electronic devices that can be easily concealed in a pocket and when your credit card is swiped through it, the device reads all of the information encoded on the magnetic strip on your card.

Phishing - Phishing scams are electronic mails sent from what appears to be a legitimate financial institution. They are devised to trick you into sending them account and password information. A common scam would be an email advising you that due to a security issue your bank would like you to confirm or reset your password.

Address Change - Your bills are diverted to another address where they are read or your mail is stolen from your mail box.

Theft - Your personally identifiable information is acquired through the theft of a wallet, purse, home burglary or car burglary.

Pretexting - Your are called or receive a text message from what appears and sounds like a legitimate financial institution in an attempt to trick you into revealing personally identifiable information.

Additional information can be found at:

http://www.ftc.gov/bcp/edu/microsites/idtheft/ consumers/about-identity-theft.html#Howdothieves stealanidentity

Preventing Identity Theft

Order a copy of your credit report every year from all three of the major credit reporting agencies in order to check for any fraudulent activity or discrepancies. In the State of New Jersey you are entitled to one free credit report every year from each of the credit reporting agencies.

Protect your mail by removing it from your mailbox as soon as possible, and consider utilizing a locked mailbox.

Shred any discarded paperwork that contains personal identifiers or financial information including pre-approved credit card and loan applications. If a vendor manually processes your credit card, ask for and destroy any carbon copies.

Stop pre-approved credit offers by calling the Credit Reporting Industry at 888-567-8688.

Know where your personal information is kept and ensure it is secure. Protect your wallet and purse and do not leave them unattended. There have been several cases where thieves access wallets and remove one credit card, but leave the rest of the contents undisturbed. Keep an eye on your credit card when using it to pay purchases.

Be aware of your surroundings when using ATM cards, making credit card purchases, and when using pin numbers and passwords. Several cases have been uncovered where skimmers are placed into ATM's capturing ATM data.

For computer use, make sure you install and keep updated anti-virus software as well as a software firewall to discourage hackers. Be aware that personal information you send over the internet could be viewed by others. Secure your wireless network, and look for the "https:" at the beginning of any web address when you are conducting financial transactions over the internet.

Carefully review your bills, bank statements, credit card statements and other financial accounts to ensure that your balances and debits match your records.

When disposing of digital devices such as phones, computers, and ipads, make sure your data has been wiped off of it — this includes modern copiers which may have an internal hard drive. If in doubt, destroy the devices.

The modern online scams are just updated versions of old con games — DO NOT give out personal information in response to unsolicited offers made in person, on the phone, or over the internet. Banks

and other legitimate financial businesses will not ask for your password or personally identifying information when they call you.

DO NOT fill out personal information on warranty cards and sweepstakes entries; it is often sold to others as a marketing tool.

DO NOT provide your social security number unless you have to.

What do I do if I become a victim?

Contact your local police department and file a report and obtain a case number. Most credit and financial institutions will require that you file a police report. Police departments in New Jersey are required to take a report when you reasonably believe or suspect you are a victim of identity theft notwithstanding the fact that jurisdiction for prosecution or investigation may lie elsewhere. (N.J.S.A. 2C:21-17.6)

Immediately call the fraud units of the three credit reporting companies: Equifax, Experian and TransUnion. Report the theft of your credit cards or identity to them. Request that your account be flagged and have a Fraud Alert/Victim Impact statement placed in your credit file asking that creditors call before granting credit. Obtain the names and phone numbers of businesses where fraudulent accounts have been opened, if any.

Credit Bureaus

Equifax

Experian

TransUnion

P.O. Box 105873

P.O. Box 949

P.O. Box 390

Atlanta, GA. 30348

Allen, TX. 75013

Springfield, PA. 19064

Credit Report:

800-997-2493

Credit Report:

888-397-3741

Credit Report:

800-916-8800

Fraud Alert:

800-525-6285

Fraud Alert:

888-397-3742

Fraud Alert:

800-680-7289

www.equifax.com

www.experian.com

www.transunion.com

Creditors:

Contact your creditors and those businesses who provided credit in your name fraudulently by phone and in writing to inform them of the problem. Ask for replacement cards, close out old and fraudulent accounts, and obtain new account numbers and create new pin numbers if the account(s) have been used fraudulently.

Federal Trade Commission (FTC):

Contact the FTC and file a report either through the FTC website at www.consumer.gov/idtheft or by telephone at 877-ID-THEFT (877-438-4338). The Federal Trade Commission serves as a clearinghouse for complaints by the victims of identity theft. The FTC assists victims by providing information to help resolve financial and other problems that can result from identity theft.

Obtain an “Identity Crimes Affidavit” from the FTC website and complete. It will be useful when notifying police, merchants, financial institutions, and credit bureaus.

Assisting Law Enforcement:

Set up a folder to keep a detailed history of the crime. Keep a log of all contacts and make copies of all documentation. Provide this information to the police and assist them in obtaining any additional information which may be required.

Gather all evidence and documentation of your financial loss and provide it to the police.

Obtain possible witness information — your salesperson, apartment managers, employers and any other person or institution who accepted the fraudulent application(s) or document(s). Provide this information to the police.

Complete the Federal Trade Commission's "Identity Crimes Affidavit" and provide it to the police.

Stolen Checks:

If you have had checks stolen or accounts set up fraudulently and you believe checks have been created for the fraudulent account, report it to the financial institution and close the accounts. Create new accounts and place stop payments on the outstanding fraudulent checks. You should also report the stolen checks to the check verification companies.

National Check Fraud Service

1-843-571-2143

SCAN

1-800-262-7771

TeleCheck

1-800-710-9898 or 927-0188

ChexSystems

1-800-428-9623

Equifax Check Systems

1-800-437-5120

ATM Cards:

If your ATM card is lost or stolen, contact the issuing financial institution, acquire a new card, account number and create a new PIN number.

Fraudulent Change of Address:

Notify the local US Postal Inspector if you suspect someone has fraudulently changed your address. Meet with your Postmaster to identify the new address and attempt to recover your fraudulently diverted mail. Contact information for US Postal Inspectors can be found at: www.usps.gov/postalinspectors.

Social Security Number:

If your social security number has been used fraudulently, contact the Social Security Administration at 1-800-269-0271 or through their website at www.ssa.gov/org.

Drivers License Fraud:

If you suspect your driver's license or registration was lost, stolen or fraudulently used, contact the State of New Jersey Motor Vehicle Commission at 1-866-TIPS-MVC (1-866-847-7682).

Passport Fraud:

If your passport has been lost or stolen, immediately contact the U.S. State Department at 1-877-487-2778, or visit their website at http://travel.state.gov/ passport/lost/lost_848.html.