Identity Theft

Identity theft happens when someone steals and uses your Social Security number or other personal information without your permission.

Protecting Your Identity

1. **Read your bank, credit card, and account statements, and the explanation of medical benefits from your health plan.** If an account statement contains errors, or it does not come on time, contact the business.

2. Shred it! - If you have paper bank documents or other financial documents, rather than simply throwing them away in the trash bin you should shred them into the smallest pieces that you can.

3.. Encrypt files and lock up documents - Any important records that need to be kept should be kept under lock and key, which means in a safe or lock box. Online documents and vital information should be password protected or stored in encrypted files.

4. Don't keep all of your critical information in one place - You should never carry your driver's license and social security card at the same time. If someone were to come by both of these cards, your identity could be easily stolen.

5. Secure your outgoing mail - When sending outgoing mail, you should use a secure mailbox. The same goes for online correspondence. You do not want anyone reading your mail that it was not intended for.

6. Keep your personal information private - You should never give out personal or vital information over the phone or over the Internet, unless you are absolutely sure that you are going through secure channels in the process.

7. Look for "https" - While purchasing items online is traditionally secure, you should always use caution to make sure that the businesses you deal with are legitimate. Always make sure that "https" appears at the beginning of the URL in the address bar before entering your credit card information online. This means that the website is secure and identity thieves will not be able to spy on you and steal your credit card number.

8. Sign up for a service that monitors your personal identity for you - You may want to pay a service to monitor your personal identity, giving you peace of mind in the process. Sophisticated methods will be used to prevent identity theft from occurring using your personal information, and you will be notified if any suspicious activity should happen to occur on one of your accounts.

WARNING SIGNS

- **You may receive a notice from the IRS that someone used your social security number.**
- **You notice errors or strange withdrawals from your bank account.**
- **You begin receiving bills or collection notices for products or services you never received or ordered.**
- **Calls from debt collectors about debts that do not belong to you.**
- **Regular bills or account statements do not arrive on time.**

What to do if Your Identity is Stolen

1. Call the companies where you know fraud occurred.

2. Flag Your Credit Reports-request a fraud alert be placed on your credit file. The company you call must contact the other two credit bureaus. A fraud alert last 90 days, after this period the bureau would need to be contacted again.

TransUnion	**1-800-680-7289**
Equifax	**1-800-525-6285**
Experian	**1-888-397-3742**

3. Report identity theft to the FTC at ftc.gov/complaint or call 1-877-438-4338. Once the complaint is completed you will receive an FTC Affidavit

4. Take this affidavit to your local police department and the department where the fraud occurred and file a report.