

Identity Theft & Fraud

Identity Theft occurs when someone uses your personal information, such as:

- Name
- Social Security Number
- Credit Card number or other identifying information without your permission to commit fraud or other crimes

Take action to minimize the chances of becoming a victim of identity theft.

Types of Identity Theft:

1. Dumpster Diving: Thieves rummage through trashcans for pieces of unshredded personal information that they can use or sell.
2. Mail Theft: Crooks seek out and steal from unattended/unlocked mailboxes to obtain pre-approved credit offers, bank statements, tax forms, and/or convenience checks.
3. ATM Theft, Skimming: Thieves secretly attach electronic devices on an ATM to capture numbers when customers swipe their cards. This may include a tiny camera to record the PIN number a customer enters for the transaction. The skimming device may be taped over the card reader.
4. Inside Sources: A dishonest employee.
5. Imposters: An individual who fraudulently poses as someone who has a legitimate or legal reason to access the victim's personal information (e.g., landlord, an employer, marketer, etc).
6. Direct Access to Personal Information in the Home: Unfortunately, there are identity thieves who can gain legitimate access into someone's home and personal information through household work, babysitting, healthcare, friends or roommates, etc.
7. Purse/Wallet Theft: Stolen purses and wallets usually contain plenty of bankcards and personal identification. A thief can have a field day using this information to obtain credit under the victim's name or to sell the information to an organized crime ring.

Types of Online Fraud:

Online Banking is generally safe, but it is good to be careful when you are online. Below are some types of online fraud.

1. Spyware/Malware: Cyber-thieves use a software application that can be remotely installed on your computer without you knowing. This is special snoopware lets the thief access everything you do online. Be wary of e-mail attachments and Web sites you don't know.
2. Online Data: Thieves have purchased sensitive personal information about someone (e.g., name, address, phone numbers, Social Security number, birth date, et.) from an on-line broker.
3. Email Fraud & Phishing Scams: Thieves who appear to be trusted financial institutions use phony e-mails to hook someone into giving them your financial and personal information.

If you suspect fraud:

What to do if you suspect a criminal is using your account:

- Contact the company with which you hold the account with unauthorized charges.
- If you suspect that your personal information has been compromised, such as your social security number, contact the Credit Bureaus immediately and have a Fraud Alert placed on your profile.

What to do if you suspect a new account has been opened:

- Contact the Credit Bureaus immediately and have a Fraud Alert places on your account profile.
- Contact the companies holding accounts fraudulently opened using your name.
- File a complaint with the Federal Trade Commission. (<https://www.ftccomplaintassistant.gov/>)
- File a report with your local law enforcement and retrieve an Identity Theft report.