Consumer Protection in Mississippi - Identity

Identity theft is a crime. Identity theft occurs when someone uses your personal information without your permission to commit fraud or other crimes, most commonly to obtain access to credit in your name. For example, an identity thief may steal your Social Security number and open, or attempt to open, a credit account under your name. Personal information includes:

- Social Security number
- Driver's License number
- Bank account number
- Credit card number
- Personal Identification Numbers
- Mother's maiden name, or other information used as a security screen
- Passwords
- Any other piece of key information that can be used to gain access to a person's financial resources, or to assume a person's identity

An identity thief can steal your information in a variety of ways. Below are a few examples of how identity thieves may obtain your personal information.

- Mail: Identity thieves steal mail directly from your mailbox. When sending mail, such as bill payments, you could be inadvertently advertising your personal information to potential identity thieves simply by placing the red flag up on your mailbox.
- Trash: Identity thieves can steal personal information from documents or other items that you discard. They have been known to sort through trash for discarded receipts, credit card statements, bank account statements, credit card applications and anything else that could contain personal information.
- Wallet or purse: One of the most common ways identity thieves obtain personal information is by stealing your wallet or purse.
- Home: Identity thieves can burglarize your home and steal important documents they may find, such as credit card and bank account statements, check books, Social Security cards, drivers' licenses and birth certificates.
- Relatives and friends: A survey commissioned by the Better Business Bureau found that you are just as likely to have your identity stolen by a relative, friend or acquaintance as you are to have it stolen online. Relatives and friends conveniently have access to your personal information and all too often they are the culprits behind identity theft.
- Computers: Consumers routinely use personal computers for financial transactions. Identity thieves can illegally gain access to computers for the purpose of stealing your personal information.
- Businesses: Identity thieves can bribe an employee at a business who has access to personal information. In some instances, the employee can steal information and commit identity theft. Also, security breaches can occur by illegally accessing information found on computers. Breaches also may come from theft from the business, or from someone posing

as a legitimate business client. Other breaches occur accidentally when no one intends to steal information.

- Email or phone, “phishing,” “pretexting:” Identity thieves can send emails, posing as legitimate companies, requesting verification of your personal information. This is known as phishing. Legitimate businesses will never request personal information from you by email. Also, identity thieves may call you, posing as a legitimate company, requesting you verify your personal information or they may contact an information source, posing as you, seeking personal information. This is known as pretexting.

Protect yourself by keeping an eye on your personal documents and credit cards. Be careful what when storing personal information, and shred documents that might contain personal or financial information. Do not share personal information over the internet or phone.

If you believe you are a victim of identity theft, file a fraud alert with a national credit bureau, file an identity theft report with local law enforcement, file an identity theft complaint with the Federal Trade Commission, close any suspicious accounts, place a security freeze on your credit report, and consider requesting an identity theft passport for the Attorney General’s office.