TELL AUDIENCE:
Identity theft happens in two ways. The first category is called Nontechnological Schemes and includes some of the following methods.

**Dumpster diving**
Dumpster diving occurs when someone goes through someone else’s garbage to obtain personal identifiable information off items found in the trash, such as credit card bills, utility bills, medical insurance, and bank statements.

**Mail theft**
Mail theft occurs when someone targets your mailbox and removes mail that has pertinent information on it. As in dumpster diving, a thief can take your credit card bills, bank statements; anything that can be used to steal your identity. At times, identity theft criminals have been known to reroute your mail without your knowledge or permission by submitting a change of address to the post office.

**Social engineering**
Social engineering is the practice of someone either in person, over the telephone, or computer, uses means to deceive someone else into divulging sensitive information. Usually, social engineers know some information that leads the victim to believe they are legitimate and give the information asked. Social engineering is commonly known as a “con game” and is perpetrated by “con-men.”

**Shoulder surfing**
This attack may occur anytime you use a password or a device that stores PINs, such as at an ATM. The identity thief attempts to get close enough to you so that when you enter password information, such as a PIN, the thief records the password. Although this typically occurs in a public setting, where the victim is and their credentials are in plain sight, it may also occur through a video camera setup by the criminal.

**Stealing personal items**
Identity thieves can also obtain your personal information by stealing your wallet or purse. When this occurs, you should immediately contact credit card companies, financial institutions, and credit bureaus to let them know of your situation.