What Are Identity Theft and Identity Fraud?

Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

What Are the Most Common Ways That Identity Theft or Fraud Can Happen?

- ATM Skimmers
  - ATM skimmers are used by thieves to steal card information and the corresponding pin number. Thieves will install devices in or outside the card slot of automated teller machine (ATM). The skimmer will store the card number and user's pin number as it is entered during a transaction. Thieves then use the stolen information to produce fake cards and spend victims' money or take cash straight from their bank accounts.

- Shoulder Surfing
  - In public places, for example, thieves may engage in "shoulder surfing", watching you from a nearby location as you punch in your telephone calling card number or credit card number or listen in on your conversation if you give your credit card number over the telephone.

- Pre-Approved Offers
  - If you receive applications for "pre-approved" credit cards in the mail, but discard them without tearing up the enclosed materials, thieves may retrieve them and try to activate the cards for their use without your knowledge. Also, if your mail is delivered to a place where others have ready access to it, criminals may simply intercept and redirect your mail to another location.

- Spam/Unsolicited Emails
  - Many people respond to "spam" or unsolicited e-mails, that promises them some benefit but requests identifying data, without realizing that in many cases, the requester has no intention of keeping their promise. In some cases, criminals reportedly have used computer technology to steal large amounts of personal data.
  - With enough identifying information about an individual, thieves can take over that individual's identity to conduct a wide range of crimes. For example:
    - False applications for loans and credit cards,
    - Fraudulent withdrawals from bank accounts,
    - Fraudulent use of telephone calling cards or online accounts, or
    - Obtaining other goods or privileges which the thief might be denied if they were to use their own name

- Online Scams
  - Many scams are conducted online, with the victim often being promised something that is often too good to be true. Victims are offered homes, cash, sweepstakes/lottery prizes, and goods in exchange for processing fees and taxes.
  - Victim's email accounts are sometimes duplicated, tricking a victim to forward funds under the false pretense of being from a known business partner/associate.
  - Victims, who are usually elderly, are also scammed by being threatened with being arrested by law enforcement, or the IRS. These victims are pressured into sending money or purchasing gift cards to be read to the scammer over the phone.

- Mail Theft
  - Mail theft often leads to Identity thieves applying for credit cards/credit, changing the victim's address, and rerouting their mail to a new address. Mail theft is investigated by law enforcement and the USPS Postal Inspector.

How To Protect Yourself Against Identity Theft

- Protect documents that have personal information
    - Keep your financial records, Social Security number, Medicare cards, and any other documents that have personal information in a safe place. When you decide to get rid of those documents, shred them before you throw them away. If you don't have a shredder, look for a local shred day, or use a marker to block out account numbers.
    - If you get statements with personal information in the mail, take your mail out of the mailbox as soon as you can.

- Ask questions before giving out your Social Security Number
    - Some organizations need your Social Security number to identify you. Those organizations include the IRS, your bank, and your employer. Organizations like these that do need your Social Security number won't call, email, or text you to ask for it.
    - Other organizations that might ask you for your Social Security number might not really need it. Those organizations include a medical provider, a company, or your child's school. Ask these questions before you give them your Social Security number:
        - Why do you need it?
        - How will you protect it?
        - Can you use a different identifier?
        - Can you use just the last four digits of my Social Security number?

- Protect your information from scammers online and on your phone
    - If you're logging in to an online account, use a strong password. Add multi-factor authentication for accounts that offer it. Multi-factor authentication offers extra security by requiring two or more credentials to log in to your account. The additional credentials you need to log in to your account fall into two categories: something you have – such as a passcode you get via text message or an authentication application, or something you are - a scan of your fingerprint, your retina, or your face. Multi-factor authentication makes it harder for scammers to log in to your accounts if they do get your username and password.
    - Do not give your personal information to someone who calls, emails, or texts you. It could be a scammer trying to steal your information.

- Monitoring your credit
    - Credit monitoring can help you detect possible identity fraud and prevent surprises when you apply for credit. If changes occur to your credit file, credit monitoring companies will let you know with an alert notification. There are many credit monitoring companies, but below are the contact details for Experian, Equifax and TransUnion:
    - To contact the national credit bureaus: Equifax: 1-800-685-1111; Equifax.com/personal/credit-report-services. Experian: 1-888-397-3742; Experian.com/help. TransUnion: 1-888-909-8872; TransUnion.com/credit-help.

Due to current laws and recent criminal justice reforms, property crimes are met with reduced penalties. California residents and businesses are increasingly victims of thieves operating near impunity. Meaning Identity Theft and Fraud Crimes will keep occurring but by taking preventative measures like the ones mentioned, our community can reduce the chances of being a target of identity thieves.

If you would like more information regarding Identity Theft and Identity Fraud, please contact Detective Tony Reis at tony.reis@morganhill.ca.gov. If you live in the City of Morgan Hill and believe you have been a victim of Identity Theft or Fraud, please file an online police report here.