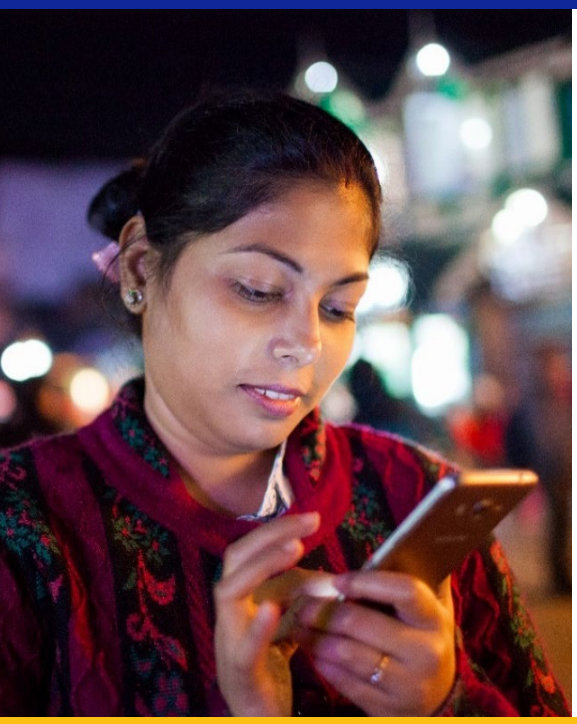
Financial Fraud: *Identity Theft*

Identity Theft is the illicit use of an individual's stolen personal identifiable information (PII) or financial information. Thieves can use an individual's name, credit card, bank account, medical insurance, or Social Security Number (SSN) to commit a variety of crimes.



How identity theft works: Criminals use a variety of methods to steal PII, including breaching organizations that store PII data, physically stealing documents or cards containing PII and financial data, and phishing victims through emails, calls, and texts. Criminals often use social engineering to trick victims into providing PII and other sensitive information.

How to spot possible identity theft: If you experience any of the following, you may have fallen victim to identity theft: Changes in personal finances such as unknown charges or withdrawals from your bank account, contact by debt collectors regarding debt you did not obtain or, changes in personal information or contact details on established accounts, changes in bills from service providers or healthcare providers, notifications of newly opened lines of credit, or notifications of data breach from an organization where you have an account.

Fraud Prevention Recommendations

- **Use cybersecurity best practices**, such as enabling anti-phishing protection on your web browser, avoiding clicking on unsolicited or unknown links, adding multi-factor authentication to account log ins, and using strong, unique passwords for different accounts.
- **Contact your bank directly** by using the phone number or website listed on the back of your card, rather than following guidance from an email, phone call, or text message you received.
- **Use caution when posting on social media**. Be aware that sharing sensitive personal information can provide criminals with clues to answer your security questions.
- **Sign up for purchase alerts with your card issuer.** Purchase alerts are customizable, can be received via email or text, and can be used to confirm legitimate purchases or notify you of suspicious activity.
- **Take advantage of identity and credit monitoring services.** These services may be provided by your bank/credit union, credit card provider, employer, or insurance company. Examine and vet any credit monitoring service to ensure legitimacy and to prevent falling victim to scams.
- **Review bills, bank statements, and credit reports** to identify anomalies that could indicate identity theft.

To learn more about protecting yourself from financial fraud, visit:
https://usa.visa.com/visa-everywhere/blog.html

VISA
everywhere you want to be