Financial Fraud: *Account Takeover*

Account takeover (ATO) fraud is a type of identity theft where fraudsters gain access to their victims' accounts, then make account changes that may include modifying personally identifiable information (PII), requesting a new card, or adding an authorized user. This can allow criminals with stolen credentials total access to victims' accounts and may result in fraudulent funds transfers or other fraudulent activity.

Example of how account take over works: A fraudster gains access to an individual's email account and looks for banking information. The fraudster accesses the victim's online banking site and initiates a password change. The bank sends a one-time passcode (OTP) to the email account as part of the two-factor authentication protocol. The fraudster uses the OTP to complete a password change, enabling access to the individual's bank account.

How to spot possible account take over: If you experience any of the following, you may have fallen victim to account take over: changes in personal finances such as unknown charges or withdrawals from your bank account, changes in contact details - such as shipping address or phone number - on accounts, or sudden use of old or dormant accounts.

Fraud Prevention Recommendations

- **Use cybersecurity best practices**, including enabling anti-phishing protection on your web browser, adding multi-factor authentication to account log ins, using unique, strong passwords for different accounts, and not clicking on unsolicited links.
- **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.
- **Never provide a one-time-passcode to a caller**, or via email or SMS text message, and do not install Remote Access software unless instructed by a trusted system support provider.
- **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.
- **Check shipping details** on accounts. Be aware of details in the 2nd or 3rd lines of the shipping addresses that might be used to reroute packages.
- **Review bills, bank statements, and credit reports** to identify anomalies that could indicate someone else has access to your account.

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

VISA
everywhere you want to be