WHAT IS ACCOUNT TAKEOVER FRAUD?

Account takeover fraud occurs when a criminal gains unauthorized access to a legitimate user account and exploits that access for fraudulent purposes. Account takeover fraud has three defining characteristics:

- **Unauthorized access:** This can be obtained through any available channel, such as direct interaction with financial institution staff (e.g., at the branch or via a call center) or through remote interaction (e.g., email, text, mobile and online portals).
- **Exploitation of trust:** Account takeover occurs under the cover of an already authenticated, seemingly "trusted" user, which enables criminals to take advantage of the account's established history and previously verified identity. Once inside an account, the criminal may change the account owner's contact information, request a debit or credit card replacement, or order new checks, all of which can seem like normal customer behavior.
- **Fraudulent intent:** Account takeover fraud is carried out with the intention of extracting value from the account before the institution or legitimate customer can detect suspicious activity. The criminal may attempt to carry out transactions or fraudulent purchases or access the account's overdraft or credit lines. Additionally, they may steal personal data or account information with the intent of using it to commit other types of fraud.

ACCOUNT TAKEOVER FRAUD VERSUS IDENTITY THEFT: WHAT'S THE DIFFERENCE?

Some industry experts define account takeover fraud as a form of identity theft. While account takeover fraud and identity theft often can be related, they differ in how criminals exploit victims and what they target. It is important to distinguish because they involve different tactics and require different detection methods and responses.

While both types of fraud have a harvesting phase to obtain information about the victim or their account credentials, the ways in which they manipulate and monetize the victim's information differ.

Identity Theft

- Occurs when a criminal uses stolen identity information, such as a Social Security number, driver's license details or date of birth, to impersonate the victim and do something new, such as taking out a loan, opening a deposit account or filing fraudulent tax returns in their name.

Account Takeover Fraud

- Carried out with the primary intent of monetizing the victim's existing financial institution account.
- Can enable identity theft by providing criminals' access to customers' personal or account information, which can be further exploited.

WHAT IS ACCOUNT TAKEOVER FRAUD?

WHAT MAKES ACCOUNT TAKEOVER FRAUD SO CHALLENGING?

Criminals often act quickly and then disappear. By the time financial institutions or customers become aware of unusual transactions on the account, the criminal often has already disappeared. Moreover, the financial institution's fraud team may be able to investigate the incident only after funds have already been stolen. Delayed detection can make recovery of stolen funds challenging.

Social engineering can be used to bypass some types of authentication methods. Multi-factor authentication is an important tool to prevent unauthorized user account access. However, account takeover fraud can still occur even if multi-factor authentication has been implemented. For example, individuals may be tricked into providing authentication factors or personal information to a criminal, such as one-time passcodes or answers to security questions, mistakenly believing them to be their trusted financial institution.

Account takeover incidents can be difficult to distinguish from legitimate customer behavior. If the criminal has the account owner's valid credentials, the login may appear to be normal to the financial institution. User actions such as updating an email or phone number could be legitimate, despite also being key signals of account takeover fraud. Multiple fraud signals may need to be correlated to accurately identify account takeover risks.

The full impact of account takeover fraud can be difficult to assess. Losses can occur because of direct monetization of the account or because of other types of fraud that are enabled by account takeover, such as identity theft. As such, losses may appear downstream, across multiple products and channels. This can potentially make it harder for the institution to assess the full impact of an incident and to prevent the account or account holder from being targeted again.

CONCLUSION

Across the evolving fraud landscape, account takeover fraud stands out as a uniquely damaging and persistent threat. Financial institutions can better protect their customers, preserve trust and reduce the financial and operational costs stemming from these attacks by understanding account takeover, how it can happen and why it is so difficult to address.

The account takeover fraud mitigation toolkit was developed by the Federal Reserve to help educate the industry about scams and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.