WHY ACCOUNT TAKEOVER FRAUD IS SO DAMAGING

Like other forms of fraud, account takeover incidents can result in financial losses, increased operational costs and diminished customer trust in financial institutions. This article explores why account takeover fraud can be so harmful.

ACCOUNT TAKEOVER INCIDENTS CAUSE BILLIONS OF DOLLARS IN DIRECT MONETARY LOSSES EACH YEAR

When criminals gain control of a legitimate customer account, they exploit it in every possible way – initiating unauthorized payments, tapping into overdraft or credit lines and making fraudulent purchases with linked debit or credit cards. Criminals act quickly to rapidly disperse stolen funds through multiple money mule (PDF) accounts, which makes recovery extremely difficult, especially when detection of the stolen funds is delayed. Financial institutions often absorb these losses when they reimburse customers for stolen funds.

REMEDIATION EFFORTS CAN BE MORE COMPLEX AND COSTLY COMPARED TO OTHER FRAUD TYPES

Acting to remediate an account takeover incident can be challenging, and the actions themselves often are manual, which may add up to significant time and resources for financial institutions. Depending on the incident, the financial institution potentially may decide to close the compromised account and open a new one. Financial institution staff will seek to investigate the source of the compromise and take steps to close any vulnerabilities. If the criminal obtains access to the account via online banking, for example, staff will work with the customer to identify which devices used to access the account are legitimate. Since the criminal successfully impersonated the victim to obtain access to the account, staff also must determine what additional security controls are needed to prevent future account access attempts.

ACCOUNT TAKEOVER INCIDENTS HARM CUSTOMERS, POTENTIALLY RESULTING IN LOST TRUST

Even when lost funds are reimbursed, individuals are inconvenienced when their account(s) are frozen or closed, or when their funds access is delayed. They may miss bill or mortgage payments and incur late fees as a result. Individuals also may be revictimized (e.g., through identity theft) due to personal data exposure that occurred because of the account takeover. Such experiences may cause emotional or psychological distress. Similarly, business operations may be disrupted due to lost account access, cash flow issues or an inability to pay vendors or employees.

WHY ACCOUNT TAKEOVER FRAUD IS SO DAMAGING

Affected customers may lose confidence in their financial institution's ability to safeguard their funds and account information, leading to reduced engagement or attrition. According to one industry study (Off-site), 42% of victims of an account takeover incident closed their accounts at financial institutions where the fraud occurred.

ACCOUNT TAKEOVER FRAUD MAY HAVE A NEGATIVE LONG-TERM BUSINESS IMPACT

Over time, repeated incidents can create significant long-term financial and competitive challenges for the financial institution. In addition to customer attrition, repeated incidents can lead to negative publicity or media reports that may harm the financial institution's brand, making it harder or more costly to attract new clients. In the long run, these factors can undermine market positioning and profitability, creating a cycle that is difficult to reverse.

CONCLUSION

The implications of account takeover fraud extend well beyond an initial incident, impacting financial institutions through direct losses, complex remediation efforts, increased operational costs and diminished customer confidence that potentially may persist long after the original event. Moreover, stolen credentials and account access often serve as gateways to other forms of fraud, amplifying losses and complicating recovery efforts. By understanding the full initial impact and implementing robust preventive measures, financial institutions can better safeguard their customers and help mitigate the harm caused by this pervasive threat.

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.