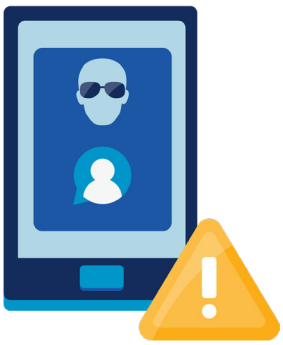
THE ROLE OF NON-FINANCIAL DIGITAL ACCOUNTS IN ACCOUNT TAKEOVER FRAUD

HIGHLIGHTS:

- **Financial accounts** are only as secure as the account holder's weakest non-financial account. Email, E-commerce, streaming and other non-financial accounts contain personal information that can be exploited for account takeover.
- **Unauthorized financial account access** often is enabled when trusted communication channels with the financial institution are breached. Compromised email inboxes and subscriber identity module (SIM) swaps allow criminals to hijack password reset processes and intercept one-time passcodes.
- **Monetization** uses creative methods beyond direct bank theft. Criminals can exploit employee portals to divert paychecks, take over retail wallets for high-value purchases, and open investment accounts to move stolen funds quickly.
- **Financial institutions** benefit from educating their customers on the importance of securing all digital accounts and can encourage them to enable multi-factor authentication (MFA), use strong and unique passwords, and monitor for unusual activity across their non-financial accounts.

NON-FINANCIAL DIGITAL ACCOUNT OVERVIEW



In today's world, it takes much more than a strong password to secure your financial account from unauthorized access. Account takeover risks often begin when criminals take over social media, e-commerce or loyalty accounts, also called non-financial digital accounts, which store personal information that can be used by criminals to impersonate the account holder. Email and mobile phone accounts also serve as gateways to financial accounts. If compromised, they can enable criminals to bypass MFA by intercepting verification codes intended to verify user access.

Understanding the role that digital accounts can play in account takeover fraud is essential to prevention. Encouraging customers to holistically think about their digital security, beyond just their financial institution login, may aid financial institutions to prevent and mitigate account takeover and other types of fraud. Protecting every digital account matters, as sometimes attackers only need one weak link to succeed.

THE ROLE OF NON-FINANCIAL DIGITAL ACCOUNTS IN ACCOUNT TAKEOVER FRAUD

ALL DATA CAN BE VALUABLE

It is easy to assume that criminals are only interested in taking over financial accounts, since these can be directly monetized. However, attackers often start by compromising other digital accounts to obtain information about the user that can unlock more lucrative opportunities later. E-commerce, streaming services, loyalty accounts (e.g., hotel rewards) and other types of digital accounts can be attractive targets for criminals. When breached, attackers gain access to personal information, as well as usernames and passwords that many individuals reuse for their financial institution logins. Even home utility accounts can be valuable, as criminals can use these accounts as "proof of address" to bypass identity checks when opening new accounts or resetting existing ones. Information about the account holder also can be harvested from digital accounts without these ever being compromised. For example, social media and professional networking sites can be a useful source of information for nefarious actors. By scanning profiles, criminals can learn names, job titles and organizational structures that can be used for social engineering or impersonation. The stolen information also can help them more accurately guess login credentials or answer security questions, such as "What is your mother's maiden name?" or "What is the city where you were born?"

Individually, these types of digital accounts may appear to be low risk. But when used together, they can supply a plethora of information that attackers can use to take over financial accounts.

HIJACKING TRUSTED COMMUNICATION CHANNELS

Once criminals have harvested enough information from digital accounts, they shift their focus to gain access to more sensitive accounts. One of the most effective ways to do this is by hijacking the recovery process or intercepting one-time passcodes. Many financial institutions rely on email, mobile phone numbers and identity documents for password resets and MFA, which makes these types of accounts prime targets for criminals to take over.

Email accounts are often the centerpiece of this strategy. If attackers gain control of a user's inbox, they can intercept password reset links and security alerts and even send messages that appear to come from the user. This gives criminals the ability to reset credentials for financial accounts without raising suspicion. Mobile phone accounts are another critical vulnerability. Through a tactic called subscriber identity module or SIM swapping, criminals convince the carrier to transfer the victim's phone number to a new SIM card that they control. This allows them to intercept SMS-based (text) authentication codes or make calls that appear to come from the account holder, bypassing MFA. Finally, cloud storage accounts can hold sensitive documents, such as scans of ID cards (e.g., passports, driver's licenses) or tax forms. If breached, these files can be used to answer identity verification questions or create fake physical IDs for in-person fraud attempts.

THE ROLE OF NON-FINANCIAL DIGITAL ACCOUNTS IN ACCOUNT TAKEOVER FRAUD

MONETIZATION: ONE FRAUD LEADS TO ANOTHER

When criminals gain control of digital accounts, they may not be able to monetize them directly, but they can use them as stepping stones to steal money in ways that are difficult to detect. For example, if they gain access to an employee's work account, they may quietly change direct deposit details to redirect paychecks without detection until payday. Similarly, subscription fraud exploits auto-pay features by linking victims' bank accounts to compromised retail profiles to purchase high-value goods or services that are shipped to criminals or unknown intermediaries. Retail wallets add another layer of risk, as many e-commerce platforms store payment details for convenience. Once attackers infiltrate these accounts, they can make expensive purchases without additional verification. Together, these schemes illustrate how criminals can monetize non-financial digital accounts to steal funds from financial institution accounts, often leaving victims and businesses scrambling to recover.

CONCLUSION

Non-financial digital accounts can play an important role in enabling account takeover fraud. Email, mobile or subscription accounts can serve as entry points for criminals to access valuable data and assets.

To help manage this risk, financial institutions can educate their customers on adopting a holistic approach to securing their digital accounts. They can encourage them to use strong passwords, enable MFA and monitor all their accounts for unusual activity. They can educate customers about the benefits of using a dedicated email account to communicate with their financial institution. Other email account(s) could be used for newsletters and social media notifications. Securing associated accounts may significantly reduce takeover attempts.

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, use 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.