UNDERSTANDING ACCOUNT TAKEOVER FRAUD

Within hours of stealing login credentials, a criminal can drain a bank account, lock out the legitimate owner and vanish without a trace. This is account takeover fraud, and it continues to be a growing threat. Account takeover fraud occurs when criminals gain unauthorized access to legitimate user accounts and exploit them for financial gain. It affects both large and small organizations and targets consumer, corporate, retail and business accounts.

Account Takeover Fraud: A Three-Phase Threat

Understanding the account takeover fraud lifecycle allows financial institutions to better prevent and detect it. The lifecycle has three distinct phases: harvest, access and monetize.

PHASE 1: THE HARVEST PHASE

Storing and retrieving credentials as well as sensitive Personally Identifiable Information (PII), a step also known as "harvesting," helps criminals gather information to infiltrate accounts. With the rise of easy-to-use malicious software tools, criminals have become increasingly sophisticated in stealing personal and financial data. Their primary methods include:

Betrayal of Trust: Impostor Scams – One scam approach is to trick authorized account holders into sharing sensitive information by calling account holders and impersonating trusted organizations, such as financial institutions. The caller might claim there's a problem with the victim's account or that they need to verify personal details immediately, which helps create a sense of urgency. Under pressure, the target reveals login credentials, account numbers or other valuable data, giving the criminal access to the user's personal information, login credentials, account numbers, etc.

Direct Deception: Phishing, Smishing and Vishing – These attacks use fake emails (phishing), text messages (smishing) or phone calls (vishing). They appear to originate from reputable organizations and urge users to click a link, download a file or share or other sensitive and valuable data to be stolen and put to use.

UNDERSTANDING ACCOUNT TAKEOVER FRAUD

Indirect Deception: Fake Websites and Apps – Criminals create fake websites or malicious apps that look legitimate. These sites may mimic a legitimate financial institution's login page or a popular shopping platform. Once the user enters their information, it is captured and used for fraudulent purposes. Additionally, downloading a fake app can give attackers access to the user's device and data.

Malicious Software: Malware and Keyloggers – Software that is specifically designed to disrupt, damage or gain unauthorized access (malware) can infiltrate devices through software downloaded from unverified sources, such as free apps, cracked (unauthorized) programs or fake updates. These tools often come bundled with suspicious downloads or are hidden in infected email attachments. Once inside the user's device, malware and keyloggers (surveillance software or hardware that silently records keystrokes) capture usernames, passwords and other private data. These tools often come bundled with suspicious downloads or are hidden in infected email attachments.

Outside Threats: Third-Party Breaches and Public Data – Account takeover fraud often is enabled by third-party data breaches from entities that may include outside vendors, suppliers or partners. Hackers target companies who have valuable data such as PII, account credentials or weak security. They steal this information, often to sell it on the dark web. Additionally, public data leaks which may occur due to oversharing information on social media or exposed public records can give criminals the puzzle pieces they need to successfully impersonate victims.

PHASE 2: THE ACCESS PHASE

Once cybercriminals have identified their targets, they enter the access phase – a sophisticated multi-step process designed to gain entry, gather intelligence and establish control over victim accounts using automated tools, social engineering tactics, and strategic manipulation. Understanding how criminals navigate this phase reveals both the vulnerabilities being exploited and the brief windows of opportunity available for intervention before significant financial damage occurs.

Initial Access: Attackers typically begin with credential stuffing – automated login attempts using stolen usernames and passwords. If that fails, they try resetting passwords or bypassing multi-factor authentication through tactics such as SIM swapping (hijacking a victim's phone number to intercept security codes).

Reconnaissance: Next, attackers perform reconnaissance to prepare for a cash-out. They check balances, review spending or deposit patterns and identify transaction limits. This careful planning helps them move money in ways that appear normal, reducing the chance of detection and maximizing the payout.

UNDERSTANDING ACCOUNT TAKEOVER FRAUD

Lockout: Finally, after gaining access and reconnaissance, criminals secure the profile by initiating account details changes, thereby officially locking out the authorized account holder. Criminals may change contact information, update passwords, register their own devices or alter authentication preferences. These steps block the legitimate user and ensure the criminals maintain control without triggering alerts. However, this does "start the clock," as authorized account holders attempting to log back in will most likely then contact their financial institution.

PHASE 3: THE MONETIZE PHASE

After criminals seize control of an authorized user's profile, attackers quickly pivot to monetizing that access. Three common approaches to account takeover fraud:

Unauthorized Transactions: The most common approach involves unauthorized transactions such as wire transfers, online purchases or moving funds between accounts. Cybercriminals increasingly rely on cryptocurrency wallets and mule accounts to rapidly transfer stolen money and conceal their tracks.

Account Linking: Another method is account linking, where criminals connect the compromised account to other accounts or wallets. These links allow them to move money through multiple channels, making detection harder and recovery nearly impossible.

Mimicking Normal Behavior: Finally, attackers exploit the account holder's account and transaction history to bypass fraud detection. They avoid triggering alerts by staying within normal transaction patterns, such as typical payment amounts or timing. This combination of speed, stealth and familiarity makes monetization one of the most challenging phases for financial institutions to detect and stop.

UNDERSTANDING ACCOUNT TAKEOVER FRAUD

CONCLUSION

Account takeover attacks are not random. They follow a clear lifecycle that begins with credential harvesting and ends with monetization. By understanding each stage, financial institutions can better recognize red flags, such as unusual password reset requests, changes to contact details or transactions that don't follow regular patterns. Awareness of these account takeover steps is one of the most effective tools for early detection.

Protecting customers and the financial institution is not just the responsibility of the fraud team or IT department, but rather, a shared mission. Every employee, from customer service to operations, can play a critical role in spotting suspicious activity and quickly escalating concerns. Knowing how attackers operate empowers organizations to act more decisively. When everyone understands the account takeover lifecycle, everyone can become part of the defense.

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.