THE NEXT FRONTIER IN ACCOUNT TAKEOVER FRAUD DEFENSE

Account takeover fraud attacks are likely to continue to grow in sophistication, driven by new forms of automation, continued use of social engineering and users' expanded digital footprints. In response, financial institutions should consider how they can evolve their account takeover fraud defenses. Effective account takeover fraud prevention and detection strategies are shifting toward mitigating threats earlier in the user journey, using advanced analytics and tracking behavioral signals that give a broader context of user behavior, devices and intent.

The changing payments landscape adds urgency to this evolution. Innovations such as embedded commerce and the advent of agentic payments may introduce new vulnerabilities. Financial institutions can consider how to integrate smarter, real-time security measures that keep pace with these innovations.

PROACTIVE PROTECTION IN A DIGITAL WORLD

Harvesting personal account holder information and credentials will likely evolve in more sophisticated ways. Reducing reliance on knowledge-based information required for users to interact with digital platforms, a form of digital distancing, can help mitigate account takeover fraud risks. One strategy could be encouraging customers to use authenticator apps or encrypted passkeys instead of traditional passwords or one-time passwords (OTPs). Passkeys eliminate the need for shared secrets and make stolen credentials less useful to attackers in accessing user accounts.

Criminals often exploit information that victims share through their social media or other digital presence to more effectively impersonate account holders to their financial institutions. Therefore, automated capabilities that monitor social media and other public digital sites may play an increasing role in making both users and financial institutions aware of potential account takeover fraud risks in real-time. These tools could monitor a customer's social media and public footprint, proactively alerting them

if posts reveal sensitive details, such as pet names or school mascots, that could be used for security questions or password guessing. This kind of near real-time feedback can empower customers to protect themselves without sacrificing engagement online.

REDEFINING SECURE ENTRY WITH INTELLIGENT LAYERS

As criminals continue to advance social engineering to bypass traditional account security, financial institutions may benefit from a shift from "point-in-time" authentication toward continuous, intelligent user verification throughout the entire customer interaction, not just at login. For example, continuous behavioral biometric monitoring could analyze how a user types, swipes, or moves through an application during the entire online session. These subtle patterns create a unique behavioral fingerprint, making it harder for criminals to mimic legitimate users.

Analyzing multiple biometric characteristics with multi-modal liveness detection could also become an important set of risk signals. Facial recognition combined with voice verification or a pin ensures that the person accessing the account is not using stolen images or recordings. This layered approach adds resilience against deepfakes and synthetic identity attacks.

Consider this:

- **A user has a new device with the correct username and password.**
- **The way the user holds, tilts and presses on the device is very different from prior interactions.**
- **A message is then sent via email with the concern the device and SIM card has been compromised.**

Also, contextual intelligence can elevate fraud detection. Advanced systems may analyze the digital surroundings of an account holder, such as IP address, Bluetooth connections and GPS location to confirm consistency with expected behavior. If anomalies appear, additional verification or notifications can be triggered instantly.

PREVENTING FRAUD AT THE POINT OF MOVEMENT

Once the criminals have breached the account, financial institutions can evolve current defenses to better prevent fraud at the point of movement. Financial institutions can reduce risk by transforming how they share information, verify recipients and analyze signals, impairing criminals' ability to monetize account holder access.

1) Information sharing for payment risk

Financial institutions can consider participating in trusted frameworks to exchange signals about risky accounts, mule activity and unusual payment patterns, for both inbound and outbound payments. Even simple indicators (e.g., "high-risk recipient" flags, velocity alerts or recent account changes) can help institutions spot when a payment is headed to, or coming from, a suspicious destination. The goal is faster, broader visibility without exposing sensitive data.

THE NEXT FRONTIER IN ACCOUNT TAKEOVER FRAUD DEFENSE

2) Verifying payees, not just account numbers

Defenses could be bolstered if payment flows bind identity to the account. Instead of sending to an account, customers and businesses should send to a verified person or business tied to that account through identity checks, name-matching, registered business identifiers or verifiable credentials. Confirmation-of-payee, payee name verification, trusted beneficiary lists and periodic re-validation make business impostor scams and account takeovers harder to monetize.

3) Agentic + AI-powered risk decisions

Programmable, semi-autonomous assistants, or agentic bots, are emerging rapidly and are designed to operate within defined parameters. They may be programmed to complete tasks such as searching for information or making limited, pre-authorized purchases. As these agents assume more activities on behalf of account holders, the patterns they create can provide valuable context for account takeover fraud detection. Combining agentic bots with analytics can foster nuanced decisions that balance security and customer convenience.

CONCLUSION: BUILDING THE FUTURE OF ACCOUNT TAKEOVER FRAUD DEFENSE

As account takeover fraud continues to evolve in sophistication and scale, financial institutions can consider a proactive, predictive approach that combines advanced technology, smarter processes and active customer participation. Innovations such as digital distancing could help reduce exposure before attackers even attempt entry, while continuous authentication and intelligence enable more robust detection in the even that criminals do breach the account. Behavioral biometrics, multi-modal liveness detection and contextual signals may make access dynamic and adaptive, creating friction only for criminals while keeping the experience smooth for legitimate users. Lastly, collaboration and identity assurance will be key to building industry defenses. Sharing information within trusted industry frameworks, using tools such as payee name verification may allow financial institutions to flag high-risk transactions without slowing down commerce.

The future of account takeover fraud attacks may feel daunting. However, through holistic, predictive and creative prevention and detection, financial institutions can stay ahead of criminals and protect their customers.

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.