Allied Solutions

Allied INSIGHTS

Fraud & Security RISK ALERTS

Timely insights to protect against fraud and mitigate risks

AI-Driven Account Takeover Fraud

SUMMARY

Account takeover (ATO) fraud remains a pervasive and financially damaging threat to financial institutions. Over the past year, the threat landscape has shifted dramatically. Fraud actors have evolved past basic credential stuffing and phishing campaigns to deploy sophisticated artificial intelligence (AI), synthetic identities, and deepfake technologies designed to bypass traditional security controls.

AI & DEEPFAKE TACTICS

The adoption of generative AI tools has fundamentally transformed the scale and sophistication of ATO attacks. Four primary techniques drive the current threat environment:

- **AI-Powered Social Engineering:** Large language models (LLMs) enable fraudsters to mass-produce hyper-personalized phishing emails, SMS lures, and voice scripts completely free of historical grammar or formatting clues. Automated AI voice agents can also conduct real-time vishing conversations to extract credentials at unprecedented scale.
- **Deepfake Audio & Video Impersonation:** As little as three to five seconds of captured audio allows bad actors to clone an accountholder's

voice, defeating passive voice authentication in live call centers. On the video side, synthetic media and AI-generated documents bypass video know your customer (KYC) streams, OCR-based verification, and non-liveness-aware facial recognition during onboarding.

- **Adversarial Attacks on Fraud Detection Models:** Sophisticated actors actively probe institution detection limits using "threshold testing" (low-value probe transactions) before executing major fraud. Model inversion techniques allow them to engineer transactions that evade scoring systems, while data poisoning degrades shared model accuracy in federated environments.
- **AI-Enhanced Credential Harvesting:** AI automates and scales traditional theft. By streamlining Open-Source Intelligence (OSINT) collection, mimicking human behavior to solve CAPTCHAs, and automating dark web credential validation against live accounts, a single bad actor can effortlessly execute mass campaigns.

KEY ATO INDICATORS

Watch for the following high-risk anomalies:

- **Inconsistent Geography:** Login attempts originating from locations outside established behavior patterns.
- **Immediate Info Updates:** Contact changes (email, phone) occurring immediately after a successful login.
- **Rapid Security Changes:** Password resets and MFA device modifications executed within the same session.
- **Exfiltration Prep:** A new external account is added, followed immediately by a same-session fund transfer.
- **Call Center Anomalies:** Unusual verbal requests for limit increases or credential resets.
- **Masked Infrastructure:** Account access routed via VPN, TOR, or known proxy networks.
- **Cross-Channel Velocity:** Multiple failed login attempts across various channels, followed by immediate success on a different device.

RISK MITIGATION: BEST PRACTICES

- **Authentication Hardening**
  - Replace standard SMS OTP with secure FIDO2/passkey authentication.
  - Deploy phishing-resistant MFA (such as hardware keys or device-bound passkeys) for all high-risk transactions.
  - Utilize risk-based adaptive authentication that automatically adjusts step-up requirements based on session context.
- **AI-Powered Fraud Detection**
  - Implement behavioral biometrics to detect and flag anomalous access patterns in real time.

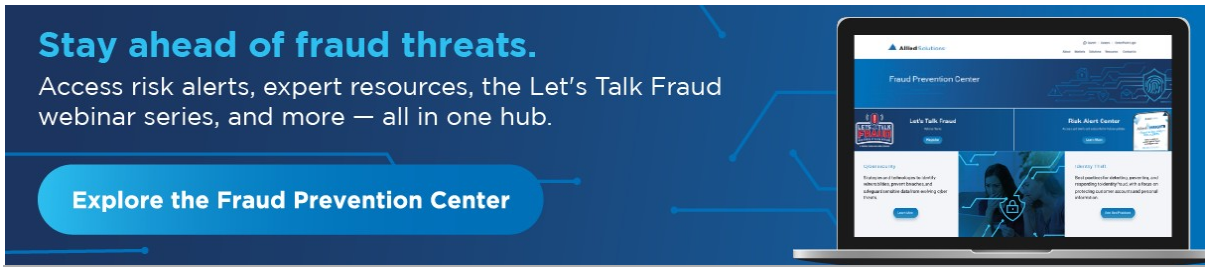
    - Deploy device intelligence and browser fingerprinting to identify automated or emulated environments.
    - Apply real-time transaction risk scoring across the authentication method, device profile, and session signals simultaneously.
- **Call Center Controls**
    - Deploy voice authentication with passive deepfake detection rather than relying on knowledge-based authentication alone.
    - Require strict callback verification for all high-risk requests, including wire transfers and credential resets.
    - Enforce dual approval workflows for any account changes that exceed defined thresholds.
    - Actively train staff to recognize social engineering tactics and synthetic voice indicators.
- **Accountholder Awareness**
    - Clearly communicate that the institution will never request credentials, OTPs, or card numbers via inbound contact.
    - Provide real-time transaction alerts that feature immediate dispute reporting capabilities.
    - Offer self-service step-up authentication controls for accountholders seeking extra protection.
    - Alert accountholders promptly following relevant public data breach disclosures.

RISK MITIGATION RESOURCES

- Access the Federal Reserve's ATO Fraud Mitigation Toolkit.
- Learn about ATO fraud via impersonation of financial institutions from the FBI.
- Read how fraud schemes involving deepfake media are targeting FIs.

Need assistance or want to request a consultation?
Contact our risk specialists at risk_specialist@alliedsolutions.net

The information presented in this email is intended for informational purposes only and should not be construed as legal advice or a legal opinion and it may not reflect the most current legal developments. You should seek the advice of legal counsel of your choice before acting on any information provided in this email.



LinkedIn