CALL CENTER FRAUD

SUMMARY

Financial institution call centers are increasingly targeted by fraudsters, leading to a rise in account takeover fraud. These attacks often involve sophisticated techniques, such as phishing and social engineering, to gain access to account holders' information and carry out unauthorized transactions.

CALL CENTERS AS FRAUD TARGETS

Call centers are prime targets for fraudsters because they handle sensitive member information and interactions. Using tactics such as caller ID spoofing, social engineering, and personal data obtained from identity theft scams and data breaches, fraudsters increasingly focus on compromising call centers to access and take over accounts —schemes known in the industry as account takeovers (ATO).

It's critical for call centers to find effective, efficient ways to distinguish legitimate callers from potentially fraudulent, high-risk ones. Striking the right balance between efficient service and strong customer account security is a complex but essential task.

MITIGATING CALL CENTER ACCOUNT TAKEOVER ATTACKS

To create a more robust authentication process and make it harder for fraudsters to gain unauthorized access to account holder information, employ multiple, layered authentication:

- **Call inspection technologies:** End-to-end call inspection solutions orchestrate identity, device and call-pattern insights, often augmented by AI and biometric features, to help call centers distinguish legitimate callers from fraudsters in real time.
- **Call back verification:** After the initial call, the agent initiates a return call to a phone number on file that hasn't been changed in at least 30 days. This ensures that even if a criminal has possession of personal details, they can't complete authentication from an unrecognized device or line.

- **Automatic Number Identification (ANI) matching and validation:** ANI works like enhanced caller ID — it captures the incoming phone number before the call is answered. By matching that number to records in the call center database, agents can block calls from spoofed or unrecognized lines as a first line of defense.
- **Knowledge-based authentication (KBA):**
  - **Static KBA** uses pre-set questions and answers (e.g., "What was your high-school mascot?").
  - **Dynamic KBA** generates questions on the fly from transaction history or behavioral data (e.g., "Which merchant did you most recently transact with?").
  - **Multi-factor authentication (MFA):** Requires two or more verification factors. For example, after providing a password, the caller must enter a one-time passcode sent via SMS or an authentication app.
  - **Behavioral authentication:** Monitors unique behavioral traits, such as keystroke dynamics or mouse-movement patterns, with behavioral authentication tools to continuously validate identity. Though still a new technology, behavioral biometrics are gaining traction in many contact centers.

RISK MITIGATION RESOURCES

- Automate every call with Interface.ai
  - **Case Study:** Fraud Prevention & Member Service with AI
  - **Watch:** *AI-Driven Fraud Prevention with Voice Biometrics*
- Helpful links:
  - Sign up for our Let's Talk Fraud quarterly webinars
  - View additional risk resources

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

LinkedIn