Allied Solutions

Allied INSIGHTS

Fraud & Security RISK ALERTS

Timely insights to protect against fraud and mitigate risks

Call Center Fraud

SUMMARY

Call centers are considered a softer target for fraudsters, as they can easily convince a call center representative that they are the real accountholder.

Financial Institutions that accept wire transfer requests by telephone or email should treat every request involving a HELOC advance, large CD withdrawal, or high-balance account as a high-risk transaction requiring layered authentication and out-of-band verification. Fraudsters are specifically targeting these channels because knowledge-based authentication (DOB, SSN, mother's maiden name, etc.) is widely compromised.

A strong control framework combines identity verification, transaction risk scoring, employee procedures, and member protections.

Common Fraud Scenarios

Fraudster impersonates an accountholder and requests:

- HELOC advance
- Wire transfer to another financial institution
- ACH transfer or external transfer

Typical Attack Flow

Information Gathering

- Fraudster researches target via social media, public records (property records showing HELOC eligibility) and obtains accountholder information from social engineering, data breaches, phishing, malware, SIM swap, etc.

Contacting the Call Center

- The fraudster may make one or more "test" calls to verify account details or confirm phone numbers on file, answers security questions, sounds confident/urgent and/or claims emergency or real estate closing. The fraudster selects optimal timing (end of day, Friday afternoon before a long weekend, etc.) when staffing is lean and urgency is harder to question.

Carrying out Fraudulent Activities

- The fraudster then requests phone/email changes, password reset, wire transfer, HELOC advance or ACH transfers.

High Risk Requests

- HELOC advances
- Large CD liquidations
- First-time wire destinations
- Changes to member contact information
- Large-dollar transfers
- International wires

Best Practice Controls

- **Wire Transfer Agreement** – A document completed, signed and dated by the accountholder for future contemplated transfer requests and contains reference to specific security procedures that the financial institution is obligated to follow to verify the authenticity of a future payment request (may be required by some insurance contracts, refer to your insurance contract).
- **Callback procedures** – Callback to a number or numbers listed in the Wire Transfer Agreement or on file unchanged for a minimum 30 days (may be required by some insurance contracts, refer to your insurance contract).
- **Strong knowledge-based authentication (KBA)** – Examples: Who is your beneficiary on your account, when was the last time you visited a branch, what branch office, when did you pay off your last loan and what was the loan for, etc.
- **Transaction "cooling off" periods** – Mandatory delay (e.g. 24-48 hours) between first contact and execution for first-time wire destinations or HELOC advances from phone/email requests.
- **Video verification**
- **Voice biometrics**
- **Device recognition**
- **One-time passcodes**
- **Behavioral analytics**
- **Dollar and velocity limits**

RISK MITIGATION RESOURCES

- **https://www.nacha.org/**
- Digital Defenders: Biometrics, Device Recognition & MFA
- Visit our NEW Fraud Prevention Center for additional risk resources.

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

Stay ahead of fraud threats.

Access risk alerts, expert resources, the Let's Talk Fraud webinar series, and more — all in one hub.

Explore the Fraud Prevention Center