Allied Solutions

Allied INSIGHTS

Fraud & Security RISK ALERTS

Timely insights to protect against fraud and mitigate risks

Liability Exposure from Account Takeover

SUMMARY

Equifax reports Account Takeover (ATO) fraud is a rapidly growing, multi-billion-dollar problem with consumer costs reaching $15.6 billion in 2024. Incidents increased 26% from 2022 to 2023.

To meet your duty to protect accountholders and the institution, you should consider stronger controls focused on detecting and stopping transactions driven by deception. This includes improved authentication, transaction monitoring, staff training, and accountholder warnings.

These measures are intended to reduce fraud losses, protect accountholders, and demonstrate that the financial institution is taking reasonable steps to prevent foreseeable fraud.

COMMON FACT PATTERNS AND LEGAL CLAIMS

Common fact patterns seen in litigation and regulatory enforcement pertaining to the accountholder being tricked often become “the financial institution failed to protect.”

- **Pattern:** Accountholder receives a fake text/email from fraudster posing as the financial institution, enters or provides online banking credentials. Fraudster logs in and transfers funds out.
    - **Lawsuit Claim:** The financial institution failed to detect abnormal login behavior and allowed large or unusual transfers without adequate verification.

- **Pattern:** Fraudster convinces mobile carrier to port accountholder's phone number. Financial institution's one-time passcodes are intercepted, and funds are transferred. (See: *SIM Swapping Risk Alert*)
    - **Lawsuit Claim:** The financial institution relied on insecure SMS authentication and failed to recognize high-risk changes followed by transfers.

- **Pattern:** Accountholder is tricked into sending money themselves (Zelle, ACH, wire) believing it's the financial institution or law enforcement.
    - **Lawsuit Claim:** The financial institution allowed a clearly manipulated accountholder to transfer funds without meaningful intervention.

- **Pattern:** Fraudster calls financial institution pretending to be the accountholder, convinces staff to reset credentials or add a new device.
    - **Lawsuit Claim:** The institution failed to authenticate the caller and allowed access based on easily obtainable information.

- **Pattern:** Accountholder reports fraud promptly. Financial Institution delays investigation or denies claim because "accountholder gave their information."
    - **Lawsuit Claim:** The financial institution violated consumer protection laws by refusing to reimburse unauthorized transfers. (CFPB Guidance on Unauthorized EFTs)

PROTECTIVE MEASURES TO REDUCE EXPOSURE

- Financial institutions should go beyond basic login security and implement layered authentication, device and behavior monitoring, and transaction-risk scoring that can detect unusual activity even when correct credentials are used. In short, strong controls plus a defensible response process reduce both fraud losses and legal exposure.
- High-risk actions (new payees, password resets, large or first-time transfers) should trigger step-up verification and clear scam warnings.
- Staff should be trained to recognize manipulation tactics and follow strict identity-verification procedures for call center and branch requests. Courts and regulators increasingly look at whether the financial institution used **commercially reasonable security** for known fraud patterns, not whether the accountholder made a mistake.
- Equally important is how the financial institution responds once fraud occurs. Prompt investigation, fair application of consumer protection rules, and clear documentation of controls help prevent disputes from becoming litigated.
- Denying claims solely because an accountholder was tricked into providing information creates legal and reputational risk if the institution failed to detect red flags or failed to warn.
- To avoid lawsuits, management should be able to show the board, examiners, and courts that the financial institution identified account takeover as a material risk, implemented reasonable preventive controls,

educated accountholders, and continuously adjusted defenses as scams evolved.

RISK MITIGATION RESOURCES

- Learn tips to prevent ATO with the **Account Takeover Fraud Checklist.**
- Read legal analysis of Reg E and scam reimbursement disputes from the **National Consumer Law Center (NCLC).**
- Learn more about account takeover and identity theft reporting and education in the **Identity Theft Resource Center.**
- Learn about scams, authorized push payment fraud, and Reg E expectations from the **Consumer Financial Protection Bureau (CFPB).**

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.