COMBATING DEPOSIT FRAUD: CONSIDERATIONS FOR A FINANCIAL INSTITUTION

Deposit fraud is a significant threat for financial institutions, often fueled by new account fraud, scams and technological advances. Deposit fraud occurs at the point where customers – either unwittingly or complicitly – initiate fraudulent check deposits.

Financial institutions can effectively detect and prevent deposit fraud by understanding criminal methods, identifying vulnerabilities and continuously evolving fraud strategies.

DETECTION STRATEGIES: COMBINING REAL-TIME ANALYTICS AND MANUAL REVIEW

Detecting fraudulent deposits is more effective with a combination of real-time analytics and manual intervention. Common practices include:

Check Image Analysis: manual or technology-based solutions can identify potential red flags on paper checks or digital images of paper checks, such as:

- Atypical characteristics, alignment or security features on the check compared to known valid items
- Traditional attributes, such as the endorsement lines and security features, are missing from the back of the check
- Endorsement does not match the valid signature of the account holder
- Verbiage or signature on the endorsement is consistent with other known fraud
- Cracks or lines through the front of the item, possibly indicating it's a picture of a check being deposited and not the actual paper check

Transaction Monitoring:

Approaches to identifying anomalous transactions may include:

- Duplicate detection: compares deposited items to others previously presented
- Holistic monitoring across accounts: an all-inclusive view of the customer, the account and transaction profiles that help identify elevated risk
- Risk scoring
- Deposit assessment across the account base: if a bad deposit is identified, check if other accounts are receiving deposits that follow the same pattern
- Cross-institutional data sharing and alerts, such as consortium data

These approaches could help to identify atypical activity, such as:

- High volume of checks being deposited or cashed within a short time frame
- Deposits followed by rapid withdrawal of funds
- Increased returns: such as altered fictitious items, insufficient funds or stop payments
- Depositing money orders that are signed by the same individual who purchased them

COMBATING DEPOSIT FRAUD: CONSIDERATIONS FOR A FINANCIAL INSTITUTION

Digital Identity Verification: compares a digital identity to the existing customer profile and usage patterns to help identify mobile and remote deposits that may be coming from a device not associated with the account, such as:

- Behavior analytics
- Device assessment (e.g., is the same device being used to access a higher-than-normal number of accounts?)
- Negative lists for known devices used by criminals

Routine case reviews often surface new fraud attributes and patterns that can be incorporated into prevention and detection strategies. These key insights also provide relevant and valuable information for ongoing training of employees.

A MULTI-LAYERED APPROACH STRENGTHENS PREVENTION

Preventing deposit fraud is just as important as having processes to detect it. Effective prevention strategies have multiple layers, such as:

- Robust onboarding and account opening processes
- Deposit limits and hold policies based on risk tiers
- Workflows for handling suspected fraud, including escalation procedures
- Staff training to recognize red flags and escalate concerns
- Customer education on scams and fraudulent deposits
- Monitoring for suspicious "on-us" items – checks that are drawn from the same institution that cashed or accepted these checks for deposit

Multi-layered prevention practices work best when applied consistently and reviewed on a regular basis to adapt to evolving fraud trends.

THE FUTURE OF DEPOSIT FRAUD MITIGATION

Criminals will continue to evolve their tactics and target areas of vulnerability. Organizations can set up a strong, long-lasting line of defense by:

- Continuously training staff and improving detection models with robust data and feedback loops
- Integrating check deposit data and alerts with other fraud channels, such as ACH, instant payment transfer, cards and wire
- Leveraging consortium data and participating in fraud intelligence networks
- Exploring emerging technologies, such as artificial intelligence (AI) signature analysis and image anomaly detection

COMBATING DEPOSIT FRAUD: CONSIDERATIONS FOR A FINANCIAL INSTITUTION

CONCLUSION

Check deposit fraud will continue to evolve as criminals continue to adapt their tactics, expand their use of technology and exploit vulnerabilities. However, financial institutions can equip themselves with a diligent, multi-layered defense that incorporates technology, effective policies, fraud intelligence and a strong team armed with tools and education to prevent and detect check deposit fraud.

The check fraud mitigation toolkit was developed by the Federal Reserve to help educate the industry about check fraud 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.