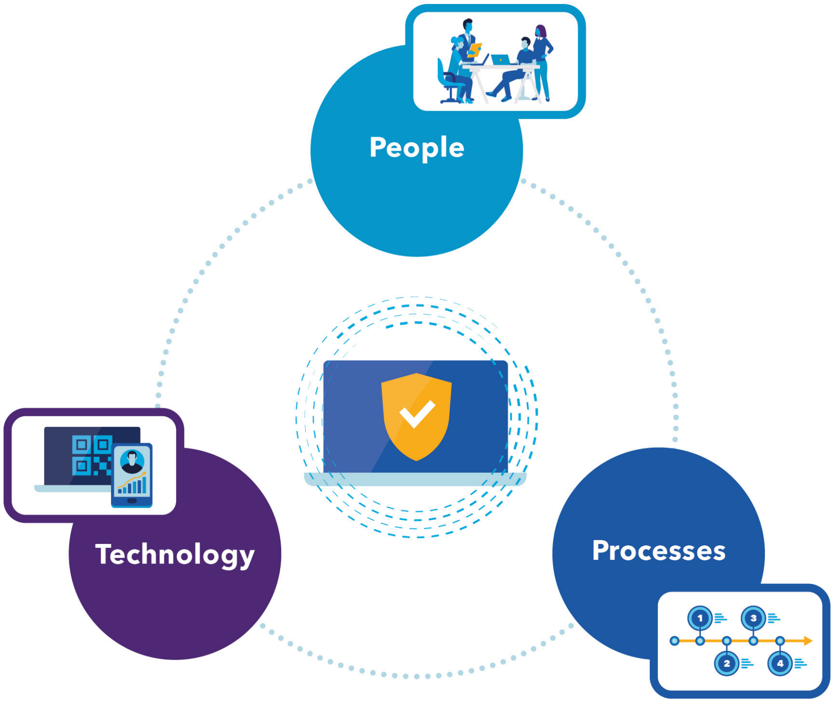
MITIGATE FRAUD WITH PEOPLE, PROCESSES AND TECHNOLOGY

Check fraud schemes range in complexity. Some criminals rely on simple low-skill level tactics, while others are organized and increasingly sophisticated. Regardless of the fraud tactics applied, financial institutions can enhance their anti-fraud strategies to mitigate check fraud through a layered approach that focuses on ***people***, ***processes*** and ***technology***.



Employees and customers of financial institutions are both critical components of an effective fraud mitigation strategy. Arming people with the knowledge they need to help mitigate fraud can be extremely valuable.

Training and empowering employees. Employees are often the first line of defense against check fraud. Offering training on a recurring basis helps staff stay aware of ways to identify suspicious behavior and new check fraud trends. Furthermore, providing tools and resources – such as check fraud playbooks, procedures and guides – aids employees in identifying check fraud, prepares them to respond, and empowers them to protect customers and the institution.

Promoting internal collaboration. Check fraud can be far-reaching. Aligning fraud strategies and sharing emerging fraud trends across teams helps ensure prioritization of check fraud prevention and addressing related risks. Organizational awareness about fraud mitigation can help break down internal siloes and keep teams aligned on fraud risks.

MITIGATE FRAUD WITH PEOPLE, PROCESSES AND TECHNOLOGY

Engaging and educating customers. Criminals frequently target customers with various fraud and scam tactics. Consider offering proactive education to customers, such as a customer education campaign, to help them better identify fraudulent checks and raise awareness of common scam tactics.

Information sharing. Fraud mitigation efforts can be more effective when sharing known fraud attributes and trends. Sharing fraud intelligence within the industry can help institutions work more efficiently to break down organized crime rings and stop check fraud schemes that are repeated across institutions. Industry-wide resources – such as consortiums and threat intelligence – can also be leveraged to stay ahead of fraud trends.

Processes

Within financial institutions, robust fraud detection processes can provide structured controls to decrease risk and promote early detection.

New account opening and customer onboarding. Criminals may open new accounts – either in person or online – with the intention to commit check fraud. Supplementing Know-Your-Customer (KYC) processes with robust forms of identity verification and document validation, as well as risk scoring, can help identify higher-risk account applications.

Fraud detection for check deposits. Automating check image analysis can be more accurate and efficient in identifying possible counterfeits or alterations. Deposits that exceed dollar, velocity or other risk thresholds may be escalated for manual review or delayed availability. Duplicate detection also can help mitigation efforts, as checks may be fraudulently deposited multiple times across different channels.

Tiered funds availability. High-risk deposits and new accounts may warrant delaying funds availability from deposited checks, compared to seasoned accounts with more reputable histories. Processes, including holds and available funds from deposits, could be tiered based on risk.

Account and transaction monitoring. Processes built within real-time fraud detection platforms and strategies to identify suspicious transactions, as well as to review and respond to fraud alerts, can help identify and stop fraud faster. Ongoing reviews of transactions and account activity can detect potential fraud even after an account has been established.

Defect review. Routinely reviewing fraud cases allows institutions to conduct root cause analyses and identify common attributes, vulnerabilities and other details. The valuable information learned can be fed back to fraud models, strategies and staff training. Such feedback loops also can be incorporated into fraud metrics and trend reporting to measure the effectiveness of process changes.

MITIGATE FRAUD WITH PEOPLE, PROCESSES AND TECHNOLOGY

Technology

When used effectively, technology can be one of the most powerful tools to fight check fraud. It offers automation, advanced analytics – produced using machine learning and artificial intelligence – and real-time response capabilities. However, technology depends upon timely, accurate data, complementary application integration and ongoing support to remain effective and prevent biases that could lead to unfair or discriminatory outcomes.

Real-time fraud detection. Real-time fraud detection can be used to analyze in-clearing and deposit transactions, flag them as suspicious and/or hold them in accordance with Regulation CC, Availability of Funds and Collection of Checks – all before the funds are available or disbursed. Software also can integrate into deposit platforms and be used to automate image analysis that looks for alterations, forgeries, counterfeit checks, and other indicators of potential fraud in real-time.

Enhancing detection and analytics. Examples of enhancing detection and analytics include machine learning (ML), artificial intelligence (AI) and robust data feeds. ML- and AI-based algorithms learn from historical known fraud patterns and attributes. They can use new trends and data, such as fraud signals and attributes identified in a defect review, to continuously learn and improve detection capabilities – improving false positive rates and reducing manual review. This technology also has the capabilities to identify anomalies in check usage that humans or rule-based approaches may miss.

Connecting to external data sources. Technology enables valuable connections to external data sources and consortiums that can be integrated into the real-time monitoring system. These additional data sources enhance check fraud detection by providing earlier notification of checks that may have a higher likelihood of return and quicker identification of known criminals, or suspicious receiver accounts.

CONCLUSION

A layered strategy that combines people, processes, and technology can equip financial institutions to be more proactive against check fraud.

- **People:** employees, customers and external partners all are valuable resources to help prevent and detect fraudulent checks
- **Processes:** act as foundational guardrails that enable people and technology to follow proven steps to escalate concerns, mitigate fraud and limit risk.
- **Technology:** enhances the efforts of people and automates processes, pulling each component together to mitigate fraud in real time.

The key is integrating all these together into a cohesive, proactive fraud framework, because each component relies on the others to reach their full potential.

MITIGATE FRAUD WITH PEOPLE, PROCESSES AND TECHNOLOGY

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.

FedPaymentsImprovement.org

THE FEDERAL RESERVE
FedPayments Improvement
COLLABORATE·ENGAGE·TRANSFORM