IMPROVING YOUR ORGANIZATION'S SCAM DETECTION CAPABILITIES

Any organization is susceptible to the negative impacts of scams, such as financial losses, data breaches and loss of customer trust. When it comes to detecting scams more effectively, businesses and other organizations should consider the following multilayered approach:

Strengthening the staff's scam defenses: Train staff members to identify common scam tactics and empower them to report and escalate suspicious activity for investigation.

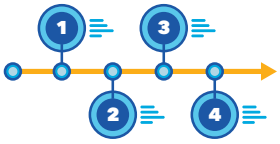
Incorporating scam detection into business process controls: Evaluate your business' processes for their susceptibility to scam threats and put controls in place as needed to help mitigate risks.

Leverage technology: Explore how different technology solutions can be used more effectively to secure access to data and systems and streamline detection.

People

- Talk to employees about common scam tactics aimed at businesses (e.g., CEO impersonation, fake invoices)
- Train staff on reporting and escalation processes
- Regularly test employees' ability to detect phishing (e.g., through email spoofing)

Processes



- Segregate staff duties related to payment initiation, approval, and execution
- Verify invoices and payment instructions through independent channels
- Clarify reporting procedures and escalation policies

Technology

- Implement multi-factor authentication
- Explore email security solutions and spam filtering tools
- Install anti-malware software
- Take advantage of vendor account validation solutions

Keep playing offense: Scam tactics and schemes are constantly evolving as criminals find new ways to bypass technology and controls. Organizations cannot afford to take a passive approach to scam detection. It is important to regularly evaluate your scam detection strategies and adjust them based on emerging fraud trends.

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