THE LAST LINE OF DEFENSE AGAINST SCAMS

Financial institutions have an essential role in protecting their customers and their institutions from scams. Customers expect safety and security for their money and financial transactions. Due to the increasing sophistication of scams, this protection requires a multifaceted approach:

- Customer education for scams and prevention tips
- Scam prevention controls
- Secure communications to reduce bank impostor scams

CUSTOMER EDUCATION

Providing common scam types and tactics may help customers to identify a scam ***before they fall victim to one.*** Education and awareness may occur in many forms, such as:

- Educational campaigns through mail, emails or text messages
- Posting scam tactics and trends on their website or social media platforms
- Conducting webinars that customers can attend to learn more about scams and preventing them
- Recorded messages that play during hold times in contact centers
- Delivering educational alerts at the time of decision — e.g., when a payment is being requested

Financial institutions can help customers recognize scams by communicating what to expect in typical interactions involving fraudulent account activity. For example, financial institutions are often clear they will not ask customers to provide their online banking username and password to verify account transactions. This can help to prevent phishing of login credentials that could result in unauthorized access. In a bank impostor scam, the criminal may pose as the financial institution and instruct the customer to move their money to a new "secure" account which is controlled by the criminal. By alerting customers to this type of scam and ensuring they know financial institutions would NOT ask customers to make a payment to secure their money, customers are better equipped to avoid this scam.

USING TECHNOLOGY TO PREVENT SCAMS

Scams can result in *authorized payments* — where customers are manipulated to send a payment — or *unauthorized payments* which are initiated by criminals after customers provide credentials to enable access to their accounts. Customers can help prevent unauthorized access or payments by using security controls and account notification services that their financial institutions may offer. However, when customers are manipulated to send an authorized payment due to a scam, the security controls in place to prevent unauthorized payments are less effective.

THE LAST LINE OF DEFENSE AGAINST SCAMS

Financial institutions may need to adjust their approach to identify authorized payments prompted by a scam. Prevention of scam payments may include fraud signals for user authentication, device monitoring, analyzing customer behavior and payment details. The table below provides examples of detection solutions that can apply to authorized or unauthorized payments as denoted by the X.

Preventing Scam Payments	Authorized Payments	Unauthorized Payments
Transaction monitoring using rules and models	X	X
Negative lists for payee names / account numbers	X	X
Behavioral biometrics (e.g., unusual mouse movement or typing)		X
Active call detection for mobile devices	X	
Tailored alerts for suspected scam payments	X	
Device fingerprinting		X
IP address and geolocation		X
Encourage customers to use available prevention, such as:		
Multi-factor authentication (at login, new payees, payment requests, etc.)		X
Biometric verification (e.g., fingerprint, facial recognition and voice)		X
Payment transaction limits		X
Notifications for user logins and payment activity		X
Payee verification for receiving account	X	

BRAND PROTECTION FOR FINANCIAL INSTITUTIONS

Financial institutions can take advantage of third-party tools — which may include those offered by telecom and email providers — to help protect their brand and prevent customers from interacting with spoofed websites, apps, emails or phone numbers.

- Websites and applications:
  - Identifying spoofed websites and apps to request takedowns of these sites/apps as they may be used for phishing information, selling non-existent merchandise or facilitating scams
  - Monitoring domain registrations to detect internet websites with close variations to legitimate company websites
  - Registering similar variations of website addresses or domain extensions if available to avoid use by criminals
- Email:
  - Using email authentication protocols, which can identify and block unauthorized use of registered business email domains

  - Providing an option for customers to report phishing emails so organizations can identify and respond to scam attempts
- Phone numbers and text messages:
  - Using a trusted telecom provider with services to authenticate phone calls and text messages, as well as identify spoofing of registered numbers
  - Enabling phone number authentication protocols — digital signatures to verify the origin of the call — to help counter caller ID spoofing used for impersonation scams

SCAM PREVENTION THROUGH RELATED PROCESSES

An end-to-end view of how scams are impacting their customers can help financial institutions proactively fight future scams.

- Detecting money mule accounts
  - By monitoring inbound and outbound payment activity and the source or receiving account, money mule accounts can be investigated and then shut down to prevent further activity. The account closures disrupt the movement of fraud funds, making it harder for criminals to profit from their scam activity.
- Applying information sharing of scams intelligence and data
  - Access to industry information for scam intelligence can be used for customer and employee education and awareness. It may also be a resource to refine detection strategies for scam payments if there are common elements available, such as dollar amount ranges, ring-specific tactics or victims located in a specific geographic area.

PROTECTING CUSTOMERS FROM SCAMS

Financial institutions are in a unique position to help to protect their customers from scams.
Prevention requires a dynamic approach utilizing people, processes and technology, which may include:

- Proactively educating customers about scams and red flags
- Encouraging the use of available security features to prevent unauthorized payments
- Having effective processes in place supported by well-trained employees
- Monitoring payments for authorized or unauthorized scam activity
- Shutting down impostors using fake digital platforms and communications

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.