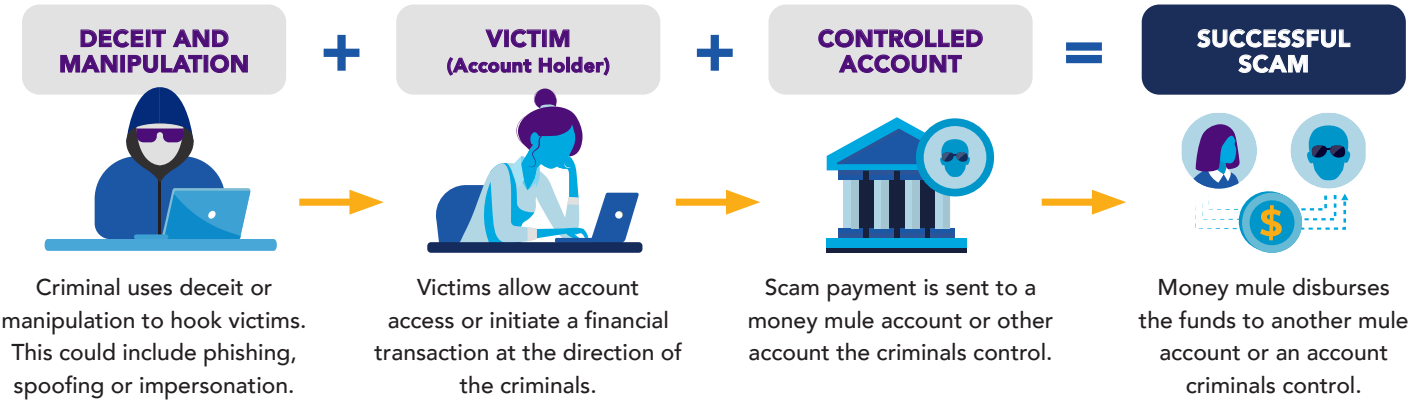
CONSIDERATIONS FOR FINANCIAL INSTITUTIONS TO DETECT SCAMS

Scam prevention requires a foundational understanding of the way scams work, the roles involved, and which key elements make a scam successful.

A common scam scenario starts with a criminal using deceit and manipulation to draw in the victim. The criminal is then able to convince the victim (an account holder) to initiate a payment (or allow access to make a payment) to a money mule or other account that the criminal controls.



The situations often are more complex than what is depicted above and involve multiple stakeholders — such as financial institutions, telecom and social media companies. However, each of the steps shown represent opportunities to identify and prevent the scam from being successful.

1 SCAM AWARENESS AND EDUCATION

Although educating customers to identify scams is critical to prevention, the inherent deceit and manipulation used in scams requires a multifaceted approach to scam payment detection. The complexity for detection is increased based on authorized users sending scam payments or enabling access to their online accounts, resulting in unauthorized payments.

For this reason, it is important to have a response plan ready to help potential victims. Scams typically involve a criminal creating a level of trust with their victim or coaching the victim in a way that creates distrust of others — including their family, friends and financial institutions. This presents a difficult challenge that requires a thoughtful approach to connect with victims. The conversational approach may vary based on the stage of the scam and the corresponding monetary transaction request. As a scam progresses, the objective of the interaction with a potential victim shifts from prevention to detection, then finally to response.

CONSIDERATIONS FOR FINANCIAL INSTITUTIONS TO DETECT SCAMS

2 IDENTIFY SUSPICIOUS OUTGOING PAYMENTS

There are times when education and preventive awareness may not stop criminals from deceiving their victims. For this reason, financial institutions may consider creating a risk-based approach for transaction alerts to help protect customers and their accounts if a scam is suspected. The following list outlines potential indicators of scam activity where an authorized account holder requests the payment. Financial institutions may consider monitoring anomalies like these to identify and alert potential scam activity.

Data and Trend Analysis

Incorporate data from external sources, industry intelligence and other open-source information to identify higher-risk activity. This could include using:

- Negative lists, such as known mule accounts and other accounts that have been associated with fraudulent activity
- Consortium data to detect new fraud patterns, tactics and bad actors
- Geographic data showing high concentrations of fraudulent activity
- Root cause analysis to identify scam trends — focusing on higher risk customer segments, transaction types, and methods used to move funds
- Central repository for customer and transaction data and data available from external sources

Customer Trends and Transaction Requests

Investigate deviations from normal customer activity using a holistic view of the relationship to maximize potential scam indicators, including:

Potential fraud signals for scam payments
Changes / increases in online banking logins (e.g., failed logins)
Atypical requests across multiple payment methods
Individual or cumulative higher-than-normal payment amounts
Payment velocity for incoming and outgoing payments within short time periods
First-time customer activity (i.e. sending money to crypto-platform or investments)
Unusual funding source for payments (e.g., retirement account, line of credit, etc.)

CONSIDERATIONS FOR FINANCIAL INSTITUTIONS TO DETECT SCAMS

Response Plan

Have a proactive response plan to handle potential scams, which may include:

- Customer outreach and effective scripting to verify purpose of payment and discern potential scams — keeping in mind this may not be a "did you authorize this transaction" type of conversation for authorized scam payments
- Stepped-up verification for transactions based on risk level
- Designated and trained employees to handle alerts/customer contact for scams
- Practices around delaying payment requests based on risk appetite
- Customer messaging and warnings specific to scams

Keep in mind that while these indicators — alone or in combination with others — may be a trend that your institution escalates for additional investigation. These are not always associated with a scam and could be legitimate activity. This is also considered a foundational list of considerations and not an inclusive one, as scam tactics and available data elements change or differ between institutions.

3 IDENTIFY SUSPICIOUS INCOMING PAYMENTS + PREVENT MONEY MULES / BAD RECIPIENT ACCOUNTS

Funds from scams are often sent to accounts belonging to money mules that have been recruited by criminals or to accounts that the criminal may control directly. Criminals ensure these recipient accounts are set up and ready to receive illicit funds prior to convincing the victim to send funds. Monitoring for, identifying, and restricting these recipient accounts is also key in preventing future scams from being successful. Indicators of these types of accounts may include uncharacteristic account activity, such as:

- Increased transaction volume
- Newly opened accounts or sudden use of a dormant account
- Mismatched transactions atypical for account holder profile
- Large/frequent international transfers or cryptocurrency purchases
- Sudden increase in account balance
- Rapid movement of funds — funds quickly moved after receiving them
- Inconsistencies in customer explanations of account activity
- Frequent or intentional layering of transactions to hide the origin of the illicit funds

CONSIDERATIONS FOR FINANCIAL INSTITUTIONS TO DETECT SCAMS

USE DATA AND REPORTING TO FOSTER A CULTURE OF APPLIED LEARNING

- Improve scam reporting to exclude other payments fraud to identify the full impact of scams
- Stay up to date on trends and sound industry practices
- Provide reporting channels for consumers that are easy to find and use
- Create actionable reviews of reports and complaints to identify fraud
- Perform regular customer vulnerability assessments
- Establish a feedback loop to incorporate learned trends and attributes into prevention strategies

KEY TAKEAWAYS

- ✓ Education, transaction interdiction, and customer alerts may be used to help prevent a scam from being successful
- ✓ Monitor both inbound and outbound transactions — ideally in real time
- ✓ Consider a multi-layered strategy across customer, account, and transaction profiles
- ✓ Establish scam reporting, trend analysis and a feedback loop to improve scam prevention strategies
- ✓ Explore how existing tools for unauthorized fraud detection may also be beneficial in preventing scams

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.