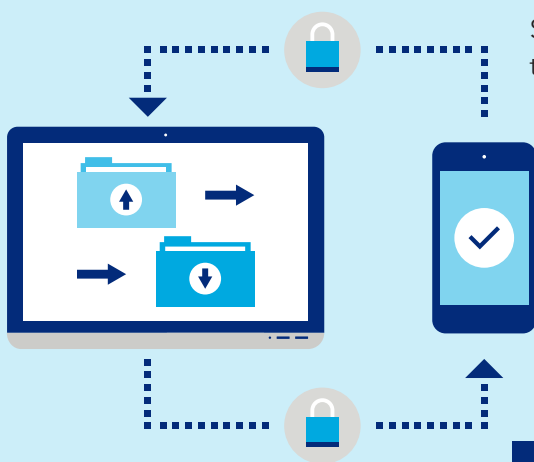


MITIGATING SCAMS THROUGH INFORMATION SHARING

Sharing timely insights on emerging scam tactics has become a critical weapon for financial institutions to help prevent and mitigate scams. This collaborative approach enables earlier detection, makes loss prevention more effective and enhances customer protection.

As scams become increasingly sophisticated and identifying authorized payments fraud continues to be challenging, financial institutions are seeking new ways to leverage available intelligence sources.



Sharing of information related to scams occurs in multiple forms across the financial industry.

- Threat intelligence organizations that specialize in aggregating and sharing information about emerging scams and tactics
- Industry consortiums sharing scam intelligence and data
- Formal information-sharing initiatives established by financial institutions, often focused on regional trends
- Informal peer-to-peer exchanges between financial institutions and fraud prevention teams

Ensuring that threat intelligence can be incorporated into fraud and scam detection models and rules should be a priority for financial institutions. Information sharing can deliver tangible benefits across the payments ecosystem.

The following scenarios illustrate different approaches to scam intelligence sharing and demonstrate how this information can be used to more effectively help prevent and detect scams.



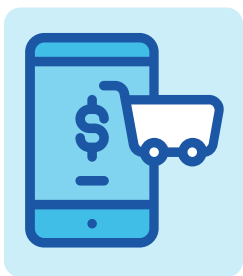
SCENARIO 1: GOVERNMENT IMPOSTOR (JURY DUTY) SCAM

An individual receives an email claiming he missed jury duty. The email threatens that an arrest warrant will be issued if the individual doesn't pay a fine and court costs within 24 hours.

The person clicks the payment link in the email to pay the fine and begins entering his payment details. He becomes suspicious about the \$950 payment amount. The individual contacts his county courthouse to verify that this email is indeed fraudulent. Next, he contacts his financial institution to confirm that a payment had not been made. The customer describes the scam to his financial institution and provides key details, including the fraudulent account name "Court Costs Co." and the associated instant payment phone number.

MITIGATING SCAMS THROUGH INFORMATION SHARING

During a meeting, the financial institution shares this scam intelligence and phone number with several financial institutions in its region. This proactive information sharing proves valuable when another financial institution identifies a similar scheme where a customer attempted to make a \$1,500 payment. The phone number is added to a bank negative list and generates a fraud alert. The financial institution then contacts its customer and confirms the payment was intended for a purported jury duty penalty, allowing the institution to stop the scam payment.



SCENARIO 2: ONLINE MERCHANDISE SCAM: PREVENTING SCAMS WITH CUSTOMER AWARENESS

A financial institution contacts a customer to validate a pending payment for \$2,500 that was higher than the account's normal activity. The customer explains she initiated the payment to purchase designer merchandise from an online advertisement.

During their conversation, the financial institution representative asks questions to better understand the purpose of the payment. The representative discovers the customer had no prior relationship with the seller and was primarily motivated by below-market pricing. Recognizing potential red flags, the representative encourages the customer to research online sellers through ratings and reviews before completing such transactions.

While still on the call, the customer locates a review indicating the offer was fraudulent, as another buyer reports she never received the ordered merchandise. The customer promptly requests cancellation of the payment.

The institution shares the details of the online merchandise scam with its payments service provider for inclusion in a fraud data consortium. This information sharing directly prevents additional victims when two other financial institutions subsequently identify and block payments to the same seller. Those institutions confirm their customers are targeted by the identical merchandise scam, where the products are never shipped or don't exist at all. The scam details also are shared with the intended receiving financial institutions.



SCENARIO 3: BANK IMPOSTOR SCAM: PREVENTION THROUGH INTELLIGENCE SHARING

A financial institution uncovers a sophisticated scam targeting its customers through telephone spoofing (where a criminal manipulates caller ID to display the financial institution's name). During these deceptive calls, criminals claim the customers' accounts were compromised and instruct them to transfer funds to alternative "secure accounts," a well-known tactic for bank impostor scams.

A glowing blue warning sign icon with an exclamation mark inside a triangle, set against a background of binary code and network lines.

MITIGATING SCAMS THROUGH INFORMATION SHARING

After identifying this pattern, the financial institution shares intelligence about the scheme with peer banks in its region. One financial institution leverages the intelligence to post a warning message on its online banking platform, alerting customers to the specific tactics being used. This timely warning results in five customers who report they received similar scam calls and did not make a payment based upon the proactive notice.

CONCLUSION: PREVENTING SCAMS USING AVAILABLE TOOLS

Information sharing can be used by the financial industry to enhance customer awareness and strengthen defenses against fraudulent transactions. Financial institutions should consider available intelligence and data sources for use within their operational frameworks. Collaborative information exchanges have become increasingly vital to both educate customers and establish robust preventative measures against 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, use 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.