THE FEDERAL RESERVE
FedPayments Improvement

COLLABORATE · ENGAGE · TRANSFORM

Scams Information Sharing Industry Work Group Recommendations

Executive Summary

Scams are being executed all around us, and the damage they do to businesses and individuals continues to grow. According to the Federal Trade Commission, consumers reported losing more than $10 billion to fraud in 2023, a 14% increase over 2022.[1]

Many organizations see the value of sharing information about scams with their peers, but are held back by the complexity of the challenge and lack of an industry-level solution. As a result, most information about fraud and scams remains siloed, causing fragmented, less effective attempts to combat them. Furthermore, disconnected efforts to detect and prevent scams allows fraudsters to repeat tactics – with minor variations – on multiple victims. And the list of victims grows.

The scams information sharing industry work group was created to evaluate opportunities for information sharing to combat and disrupt scam payment activity. Its goal was to craft recommendations for further consideration by the payments industry that could promote information sharing, encourage participation in information-sharing opportunities, and foster collaboration within the industry to bring about voluntary and collective change in the fight against scams. The group referenced examples of existing industry information-sharing efforts as a guide to overcoming challenges and focused its recommendations on achievability and value.[2] Although many industry organizations facilitate information sharing at some level today, these efforts are not sufficiently far-reaching. The industry work group's recommendations are intended to provide ideas to facilitate a more holistic information-sharing exchange by connecting information sources and expanding access to intelligence and data.

As a result, the group recommends the industry consider establishing an information exchange to provide scam intelligence across payment rails, which includes ideas on how the exchange should be established and evolve. By sharing data within the industry on scam trends and known bad information, organizations can be better prepared to mitigate scam payment activity.

1 As Nationwide Fraud Losses Top $10 Billion in 2023, FTC Steps Up Efforts to Protect the Public | Federal Trade Commission, Feb. 9, 2024

2 Achievability and value were perceived broadly and do not encompass any applicable legal, regulatory or privacy rules, any of which could impact the viability of the recommendations.

The problem

Stakeholders in the U.S. payments industry lack real-time access to current, industrywide information necessary to develop effective strategies to detect and prevent a growing number of scams, and other fraud types, that cause significant financial losses and negatively impact both consumers and organizations.

The scams information sharing industry work group developed the problem statement above to guide its work and discussions.

The group was launched in June 2023 with administrative support from Federal Reserve Financial Services. The group is made up of 30 fraud prevention and payments experts from across the U.S. Members represent financial institutions, payment providers, payment networks, financial technology firms and consumer advocacy groups. Their work is built upon a belief in the value of collaboration through information sharing. They began by recognizing the many challenges of information sharing, including reputational risks; diminishing an organization's competitive advantages; implementation time and cost; access to timely, industrywide data; and the fragmented, complex state of the U.S. payment system.

Industry work group members agreed that the need for information sharing is clear. Scammers take advantage of individuals to trick them into making authorized payments, making it more challenging to detect this activity. Organizations need to work together to stay ahead of fraudsters targeting consumers or businesses and improve their own scam prevention tactics. Scammers often use the same approaches across multiple organizations and payment rails to convince victims to send authorized payments. Information sharing could expose and counter successful scam tactics before they are replicated elsewhere.

Several benefits of scam information sharing include:

- Provide scam intelligence to improve countermeasures and controls.
- Share details on scam receiver accounts – that is, accounts used by fraudsters – so organizations can better prevent scams at payment initiation, improve detection and prevent losses.
- Help identify mule accounts, making it harder for scammers to move and access money.
- Disrupt the use of largely identical scam tactics across organizations and payment rails.
- Produce trend reports to help organizations measure and improve anti-fraud performance.
- Provide consolidated information to law enforcement.

The industry work group identified scam information-sharing opportunities and produced recommendations that could prevent scams or mitigate their impact. A primary focus was on ways to bring information about scams to a wider audience, so stakeholders can better evaluate the risks to their organizations.

Recommendations

The work group's primary recommendation is for the industry to consider a solution or establish an independent information exchange framework that would facilitate the secure exchange and connection to existing scam intelligence and data sources. This information exchange must be trusted and agile. It also must have sufficient capacity to grow and adapt, so it can continue to track and distribute data about scam impacts and fraudsters' evolving tactics.

The industry work group members believe key components of this information exchange should include the ability to:

- Connect to scam information produced by, and maintained within, organizations.
- Route participant requests to compare an organization's data to multiple information sources, allowing them to identify matching or relevant scam intelligence and data.
- Aggregate results, including trends from multiple information sources, to provide to participants.
- Determine if a receiver account number has been reported in association with suspected or confirmed scam activity.
- Enable participating organizations to submit scam intelligence and payment details and make that information available to other participants across various payment rails and types.

While understanding that legal and regulatory barriers can change, the industry work group developed its recommendations without a detailed review of any existing legal, regulatory or privacy rules that might prohibit or limit the proposal.

Establishing an Information Exchange

The scams information sharing industry work group believes that an information exchange must have innovative leadership and robust requirements that ensure efficiency, privacy and transparency. The proposed steps:

Create a governing structure for the information exchange.

The work group recommends establishing an industry-led group or coalition to govern the information exchange and advance scam information sharing. The purpose of the governing body should include:

- Identifying scam information to be shared by payment stakeholders.
- Developing an engagement plan to involve key stakeholders.
- Recognizing gaps in the current information-sharing landscape.
- Determining priorities for effective information sharing.

This governing body would be charged with prioritizing requirements, implementing the necessary processes and ensuring participation by trusted entities. It also would offer guidance on how to overcome obstacles to information sharing.

Establish requirements for the information exchange.

Permissible use of the exchange must be clearly defined. Participants must agree to guidelines and refrain from using the exchange for other purposes. So, the success of the exchange begins by vetting participants. It's critical to ensure that only authorized entities can access and contribute to the exchange.

Meanwhile, participants should have broad visibility into how the exchange operates. This requires a transparent governance framework that outlines decision-making processes, roles and responsibilities.

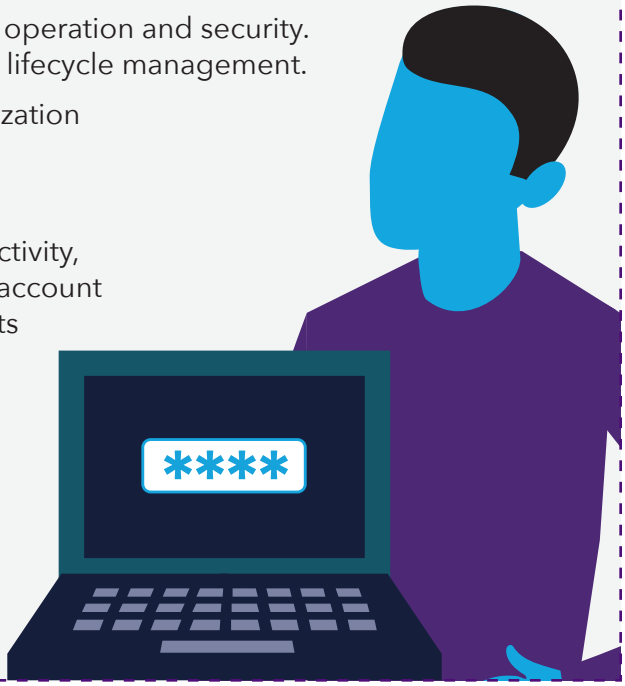
Industry participation must be as broad as possible, which expands the scope of information sharing. To encourage widespread industry involvement, the exchange should evaluate options for a funding mechanism that offers access at minimal cost.

At the outset, the exchange should be scalable enough to accommodate rapid expansion. Ease of use also can encourage growth.

Privacy

Participants must be assured the exchange safeguards sensitive information and follows all relevant laws and regulations while promoting data sharing. The industry work group believes this can be accomplished if the exchange:

- Follows **industry standards** for data management, operation and security. Best practices should be considered, such as data lifecycle management.
- Ensures **data privacy** using tools, such as anonymization and tokenization.
- Uses **encrypted channels** for data transfer.
- **Securely stores** scam information and exchange activity, and enables participants to submit scam receiver account data that then will be available to other participants within the exchange.
- Defines and uses a **consistent taxonomy** for classifying scam-related data, which helps to ensure uniformity in data representation
- Is **agnostic** about payment type and network, so it can support various payment networks and allow access to data on any payment type.

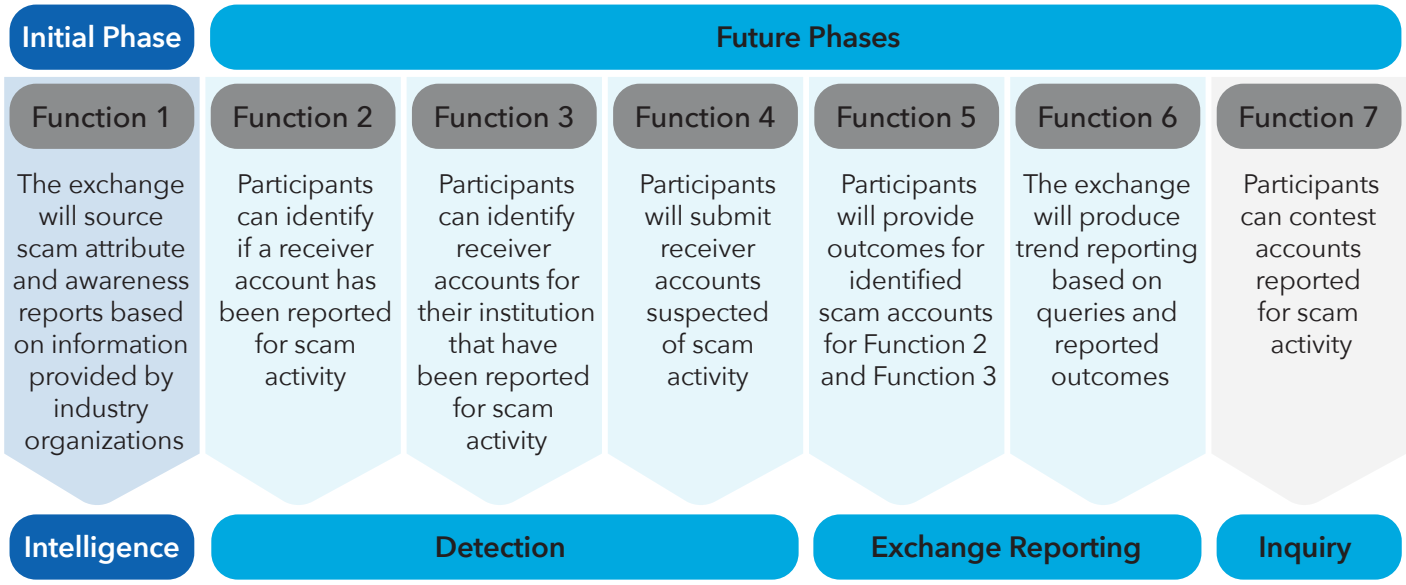


Primary Recommended Functions

The need for information sharing about scams is urgent. However, identifying or building a solution with the full functionality envisioned by the scams information sharing industry work group will take time.

To get an exchange operating as soon as possible, the industry work group recommends a phased approach that starts with minimal viable functionality. This will allow the exchange to begin operating more quickly while providing value to participants.

During this initial phase, the work group recommends that the exchange establish processes allowing industry organizations to share scam intelligence as part of their existing operations. The exchange's functionality could be expanded in phases, as follows:



Initial Phase:

Function 1: Issue scam attribute and awareness reports.

Industry organizations should be able to submit scam-related insights and trend data, which in turn can be used by other participants to aid in detection and prevention of emerging risks. This information also can be used to raise awareness about scams. For example, observers have seen a significant increase in scams involving cryptocurrency investments using impostor or illegitimate websites.

Exchange content could be aggregated and accessible through a portal or distributed to information exchange participants. Standardized templates and predefined fields should be used to ensure consistency.

These intelligence reports should flag scam activity and methods, including:

- Changes in scam volume by type.
- New or evolving tactics, approaches and language.
- How the scam was detected and total dollar value and recovery amounts.
- Scam signatures, such as dollar amount, geography and device detail.
- How the scam was initiated, i.e., by phone, email, website, etc.
- Targeted payment platforms, payment type, products and account type.
- Details, including the scam's time frame, warning signs, and how the scam was executed (e.g., account takeover or business email compromise).

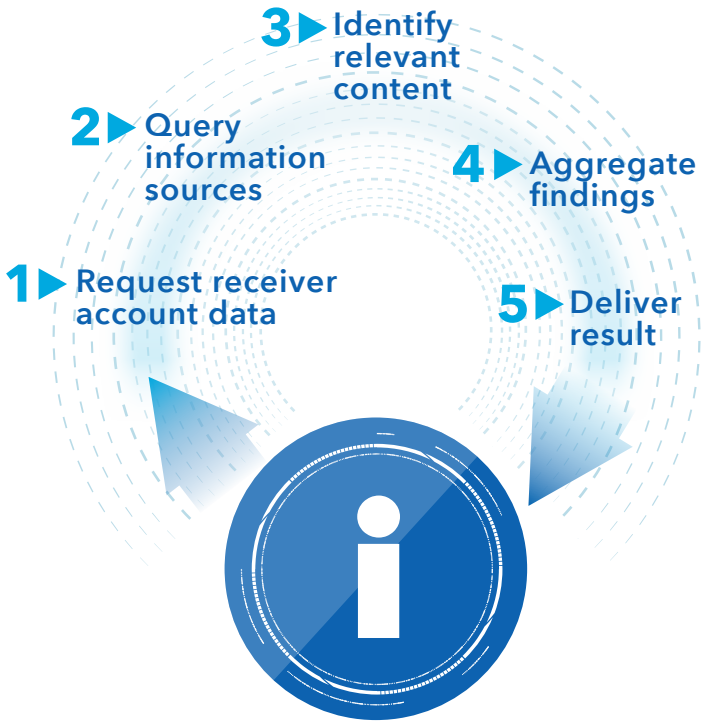
As a future component for this function, the exchange also should produce its own intelligence on scam trends, tactics and potential indicators. The use of "link analysis" – visuvally presenting networks of connected entities – is recommended to identify potential criminal rings and generate reports for participants. This intelligence also may be provided to law enforcement for awareness.

Future Phases:

Function 2: Identify scam receiver accounts using existing information sources.

Exchange participants who send payments should have the ability to verify whether receiver accounts have been flagged for suspected or confirmed scam payment activity. Essential characteristics:

- Exchange participants should be able to query using the receiver account and receiving institution based on information about payments initiated by their customers. They can decide when to search for a receiver account to supplement their payment risk thresholds. The results should be immediately available either through real-time calls to information sources or by searching against a locally downloaded data file.
- Queries should result in a binary "Yes" or "No" response from industry organizations. "Yes" would indicate that the receiver account has been reported for engaging in suspected scam activity. A "Yes" response may include additional details, such as the number of scam reports and reason codes for account status.
- Each receiver account query submitted by exchange participants should include the payment type; the payment rail or application name; and its date, time and amount.
- The queries should include the sender organization name and identifier; the receiving organization name and identifier (such as an ABA routing number); the sender's name and account number or identifier; and the receiver's name and account number, identifier or token – such as an email address or phone number. As a result, the transmitted data likely would be considered personally identifiable information.



Function 3: Identify scam receiver accounts for a participant's institution.

Exchange participants should be able to search for receiver accounts reported for scam activity. They should be notified if these accounts appear at their own institutions, either through a push notification or by the ability to download the data. A participant's search will use the organization's name and identifier (e.g., an ABA routing number) to identify reported scam accounts from existing information sources.

Function 4: Enable participants to submit scam receiver accounts.

The exchange should have the ability to accept scam receiver account information and account numbers identified and submitted by participants and make the information available to other participants. The submitting organization would provide its name and contact information, and the submitted data must be defined by the payment rail and formatted to align with the lookup capabilities of that payment rail.

Exchange participants submitting a receiver account identified for scam activity should provide the following details, if known or available:

- Type of scam, based on classification structure.
- Scam origination or contact method.
- Detection method identified and reported amount(s).
- Transaction date(s) and time(s).
- Sender ID.
- Suspected or confirmed status.

Function 5: Participants provide an outcome for account queries.

The exchange should require participants to provide an outcome for each receiver account notification or query result that leads to suspected or confirmed scam activity. This would enable other participants to benefit from knowing about payments or accounts that were identified as scam activity.

The outcome should be entered in a timely way, but no later than 90 days from the date of the account notification or query result. The following scam information should be required from participants for each notification or query result for receiver accounts:

- Scam identifier (suspected, confirmed or not confirmed).
- Scam type and classification.
- Scam origination or contact method, if known.
- Available payment details, such as payment type, payment application, authorized or unauthorized payment, loss amount(s), prevented loss amount, transaction date(s) or times, etc.

Function 6: Trend reporting for query activity and outcomes.

The exchange should generate trend reports based on queries and outcomes. The trend reporting will include the top scam types reported as part of the query outcome information. It may include the number of receiver account queries submitted, whether the receiver accounts were present in the information sources, and the "Yes" or "No" scam payment outcome provided by participants.

Function 7: Resolution of contested information.

Participants should be able to contest inaccurate scam reports linked to their organizations. This would include requesting a correction or the posting of additional details to support the organization's findings. Any notice will include contact details for the participant who disputes the report, which would allow direct communication with the original party.

Future Enhancements

The scams information sharing industry work group identified numerous possible future enhancements for the exchange, including:

- A data analytic capability that uses artificial intelligence to better analyze emerging risks and evolving tactics for proactive detection of the first occurrence of scam payment activity from a sending account.
- Supplemental data from other scam information-sharing sources, such as telecommunications and social media companies.
- Alerts based on analysis of scam information.
- Demographic details on scam victims, such as age, location and account tenure.
- Access to structured or unstructured data, including freeform case details and notes.
- Scam payment details, if funds were moved from the initial receiving account to another.
- Information related to other fraud types.
- Access to consumer-reported scam information sources.
- Identification of potential new members who can add insights, including new data sources and evolving business risks related to scams.
- Collaboration with government, industry and/or social media groups to educate the public on current and evolving scams and recommended best practices to prevent scams.

Conclusion

An information exchange could be a powerful tool to disrupt and thwart scams and the fraudsters who commit them.

An exchange could enhance collective anti-scam efforts by bringing together representatives from the payments industry to act as a single source for aggregated scam information across payment rails. An exchange also can address the fragmented information that is allowing fraudsters to thrive while businesses and individuals face mounting damage.

An information exchange could allow financial institutions to gain a comprehensive view of emerging scam threats, patterns and tactics – and it would enable better analysis and more effective preventative measures.

The governing body for an industry exchange must facilitate collaboration, standardize reporting and promote best practices. It also can evaluate and prioritize what needs to be done to streamline scam information sharing and increase anti-fraud collaboration.

These recommendations are intended to promote dialogue, identify key considerations (e.g., legal, regulatory or privacy barriers), and assist the further evaluation of sharing options. Industry collaboration is necessary for a solution or exchange to address the issues that inhibit scam information sharing. The primary aim of the industry work group is to encourage action; increase scams information sharing; and counter the growing impacts of, and financial losses from, scams.

Glossary

Exchange – the connection point and request router for users to submit requests and access scam information, and the future capability to accept and store information provided by users.

Information source – an organization that has an established process to produce scam intelligence and collect scam data (e.g., scam receiver accounts) and agrees to make this information available to the exchange.

Participant – an organization that has agreed to use and contribute content to the information-sharing exchange or solution.

Limitations

The recommendations described in this paper were prepared by the scams information sharing industry work group for further consideration by the payments industry. The industry work group did not conduct a detailed review of any legal, regulatory or privacy restrictions that might prohibit or limit the viability of the proposed recommendations.

Join the FedPayments Improvement Community for updates on this work.