SCAMCLASSIFIER℠ MODEL FREQUENTLY ASKED QUESTIONS

Q: WHAT IS THE SCAMCLASSIFIER MODEL?

A: The ScamClassifier model is a voluntary classification structure that can be used to classify authorized and unauthorized activity where the root cause was a scam.

This methodology can help organizations better understand scam activity. A commonly used taxonomy aids in industrywide scam reporting, trend identification and detection improvement.

The ScamClassifier model and definitions are available for download at fedpaymentsimprovement.org.

Q: HOW DOES THE SCAMCLASSIFIER MODEL WORK?

A: The ScamClassifier model begins by confirming the event being classified meets the definition of a scam. If it does, the classification continues by assessing if the payment was authorized or unauthorized. This is done because "who" completed the payment is a critical foundational element in classification.

Once the payment is identified as authorized or unauthorized, the user selects the scam category and then dives a level deeper into the scam type.

Scam categories and types are intended to be specific enough to be mutually exclusive, while still offering a broad approach to allow for future scams and variations.

In order to promote consistent usage across the industry, definitions for each of the terms are included with the model.

Q: WHY SHOULD AN ORGANIZATION CONSIDER ADOPTING THE SCAMCLASSIFIER MODEL?

A: *Targeted Prevention and Detection.* Organizations report improved consistency in classification and scams reporting when using the ScamClassifier model. This helps enable analytics to better determine what types of scams are being perpetrated on customers and what scam payment detection strategies are effective.

Streamlined Response and Resource Allocation. Users indicate the model helps employees respond to scams more efficiently. The ability to quickly identify a scam, stop scam payments and protect customer accounts can improve the overall customer experience.

Improved Education and Communication. The ScamClassifier model and corresponding definitions can be used for employee education, helping them understand different types of scams and more consistently use key terms. Using the same scam classifications and terms allows employees to communicate based on a common understanding within their organization, as well as across the industry. Consistent analysis of scams also can be used to alert customers about potential risks in their geographic area or scam attempts targeting them.

SCAMCLASSIFIER℠ MODEL FREQUENTLY ASKED QUESTIONS

Data Analysis and Trends. Those using the ScamClassifier model report more consistent data and communication when sharing, reporting and analyzing data across scam types, attributes and variations, both internally and externally. Consistent reporting of scam types is important to compare scam activity with other organizations and benchmark performance; discover new trends and tactics; and identify potential improvements or controls.

Q: HOW CAN THE SCAMCLASSIFIER MODEL OFFER AN ORGANIZATION A MORE HOLISTIC VIEW OF SCAMS?

A: The ScamClassifier model allows organizations to classify both authorized and unauthorized activity that originated from scams. This creates broader awareness and highlights the prevalence of issues related to scams.

Q: IS THE USE OF THE SCAMCLASSIFIER MODEL MANDATORY?

A: Adoption of the ScamClassifier model is completely voluntary at the discretion of each individual entity and 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.

Q: WHO DEVELOPED THE SCAMCLASSIFIER MODEL, AND FOR WHAT PURPOSE?

A: Federal Reserve Financial Services led the Scams Definition and Classification Work Group from 2023-2024 to help the industry address challenges around the multiple operational definitions of scams and the lack of detail in existing classification approaches.

This industry work group brought together a broad range of expertise within the payments industry to develop an industry-recommended operational definition of the term "scam" and classification structure to help provide a foundation for improved consistency and detail in both fraud classification and reporting of scams.

Q: CAN THE SCAMCLASSIFIER MODEL BE USED TO CLASSIFY SCAMS FOR ANY PAYMENT TYPE?

A: Yes. The ScamClassifier model was designed to enable classification for all payment types and payment channels.

SCAMCLASSIFIER℠ MODEL FREQUENTLY ASKED QUESTIONS

Q: DOES THE SCAMCLASSIFIER MODEL INVOLVE DATA STORAGE? HOW DO I SEND IN REPORTS OF SCAMS TO BE INCLUDED IN THIS CLASSIFICATION?

A: The ScamClassifier model was designed for classification purposes only. It does not collect, track or store data.

Q: HOW CAN DIFFERENT SCAMS BE CLASSIFIED USING THE SCAMCLASSIFIER MODEL?

A: Visit the ScamClassifier model webpage to access information about how to use the model and examples of how different scenarios are classified.

Q: CAN THE SCAMCLASSIFIER MODEL BE USED WITH THE FRAUDCLASSIFIER℠ MODEL?

A: Yes – the ScamClassifier and FraudClassifier models can be leveraged together to create a deeper classification of the scam or fraud event that has occurred. For additional information on how the two models can be used together, listen to this video tutorial, which provides four scenarios where the models interact and account for both authorized and unauthorized scenarios.