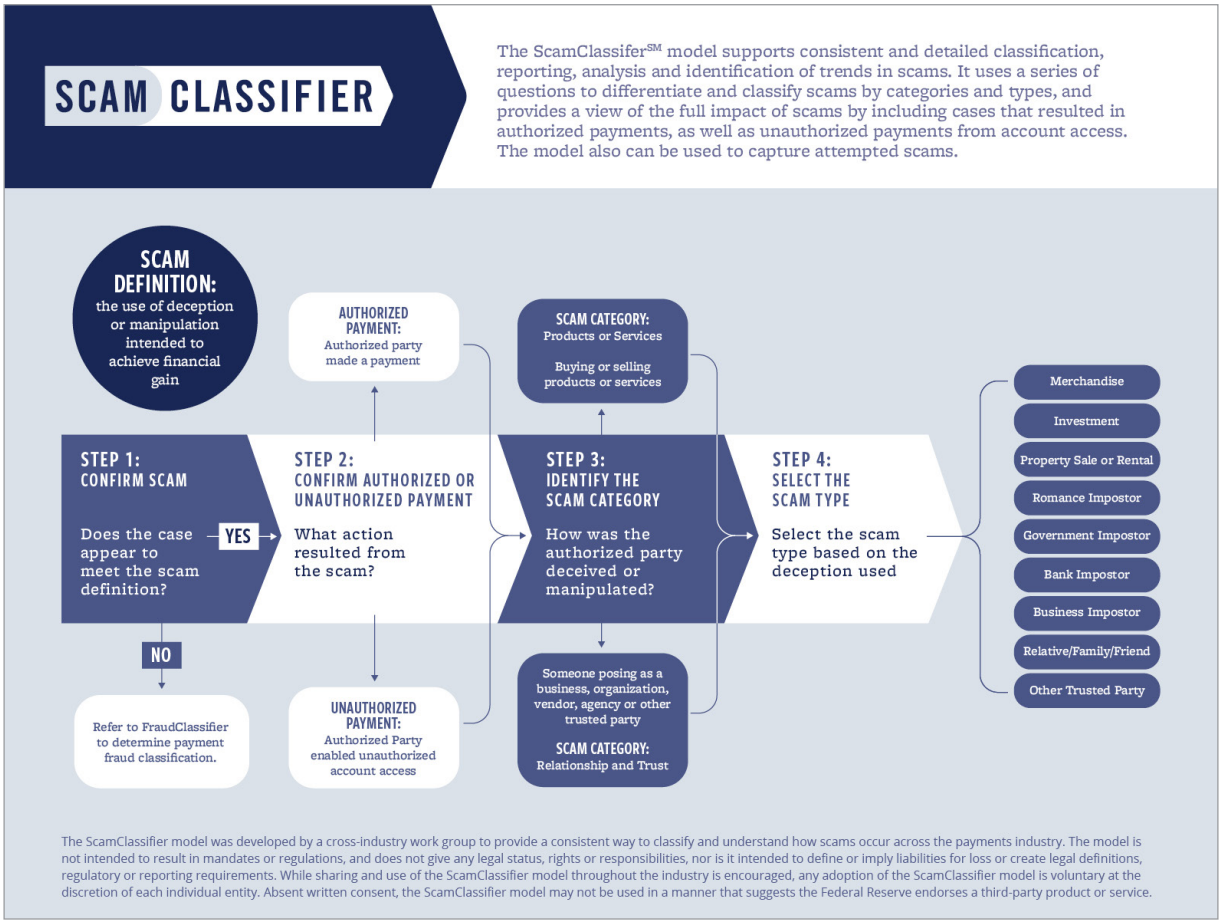
ABOUT THE SCAMCLASSIFIER℠ MODEL

The ScamClassifier model is a voluntary classification structure that supports consistent and detailed classification, reporting, analysis and identification of scams and related trends — a prerequisite to help promote accuracy of scam reporting, detection and mitigation. It can be used as a standalone classification structure or applied either before or after the FraudClassifier℠ model — which is used more broadly to classify an incident as various other fraud types.

Explore how the two models can be leveraged together.

Similar to the FraudClassifier model, the ScamClassifier model does not depend on the communication method, payment application or payment type. The ScamClassifier model uses a series of questions to differentiate and classify scams by methods, categories and types.

Classification begins with the scam definition, **the use of deception or manipulation intended to achieve financial gain**, to distinguish an actual or attempted scam from other types of fraud. Subsequent questions determine the results of the scam, method of deception and scam type. The model further facilitates accurate scam classification by including definitions and examples of the nine scam types shown in the graphic below.

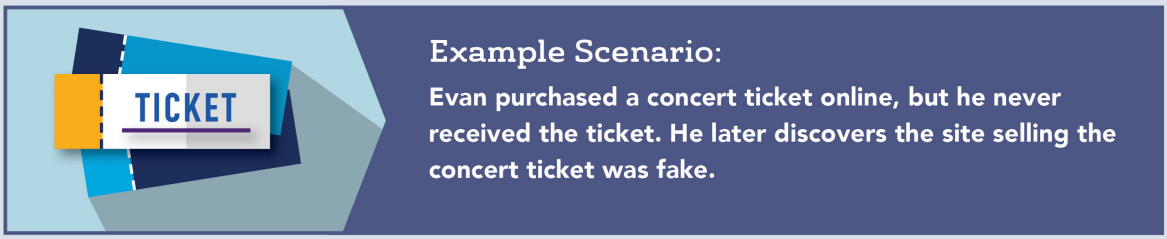


ABOUT THE SCAMCLASSIFIER℠ MODEL

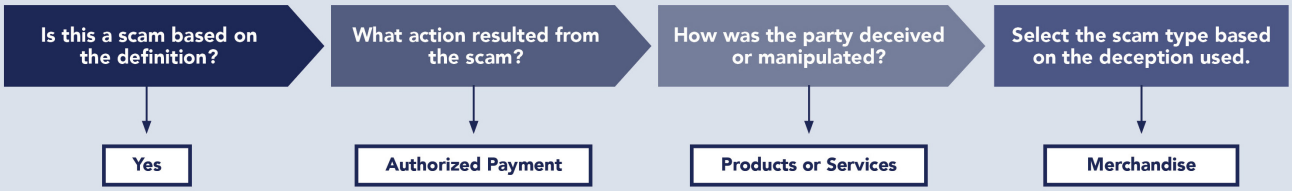
HOW TO USE THE SCAMCLASSIFIER MODEL

The model uses a series of questions to differentiate and classify scams and attempted scams by category and type.

- **Step 1: Does the incident meet the definition of a scam: the use of deception or manipulation intended to achieve financial gain?**
  - Incidents that are suspected of being fraudulent but not classified as scams can be further investigated using the FraudClassifier model.
- **Step 2: What action resulted from the scam?**
  - Either an authorized party was tricked into making the payment, OR the authorized party was tricked into enabling the criminal to access the account.
- **Step 3: How was the authorized party deceived or manipulated?**
  - Answers to this question are used to categorize the incident as either a *products or services scam* (e.g., to buy or sell something), OR as a *relationship and trust scam* (e.g., someone posing as a business, organization, vendor, agency or other trusted party).
- **Step 4: Classify the scam type based on the type of deception.**
  - The nine scam types in the ScamClassifier model focus on characteristics of the impostor and desired outcome: *merchandise scam, investment scam, property sale or rental scam, romance impostor scam, government impostor scam, bank impostor scam, business impostor scam, relative/family/friend scam* or *other trusted party scam.*



Result of the ScamClassifier℠ Model:



ABOUT THE SCAMCLASSIFIER℠ MODEL

For more examples of how scams can be classified, visit Module 5: Scam Scenarios.

Financial institutions and other organizations can evaluate their processes for fraud and scams to determine how the ScamClassifier model could provide consistency and value in combating scams. In addition, organizations can assess potential integration of the ScamClassifier model into their existing scam classification case management tools.

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.