USING THE FRAUDCLASSIFIER℠ AND SCAMCLASSIFIER℠ MODELS TOGETHER

As part of a continued focus on understanding and helping to mitigate fraud and scams, the Federal Reserve convened multiple industry work groups that developed two classification models: the FraudClassifier model and the ScamClassifier model.

The FraudClassifier model: This model guides users through answering questions to determine who initiated the payment, how the fraud was executed, and what type of fraud occurred — helping organizations better understand fraudulent activity and trends.

The ScamClassifier model: This classification tool was designed to take users through a series of questions about a given fraud case to determine if it was a scam, the result, the method of deception used to deceive or manipulate the victim, the scam category and type.

These models can be used ***individually or together*** for an industry-wide common fraud language to help organizations:

- Improve mitigation strategies
- Develop internal training
- Enhance reporting
- Educate customers on specific fraud and scam trends

Leveraging Both Models for Enhanced Classification

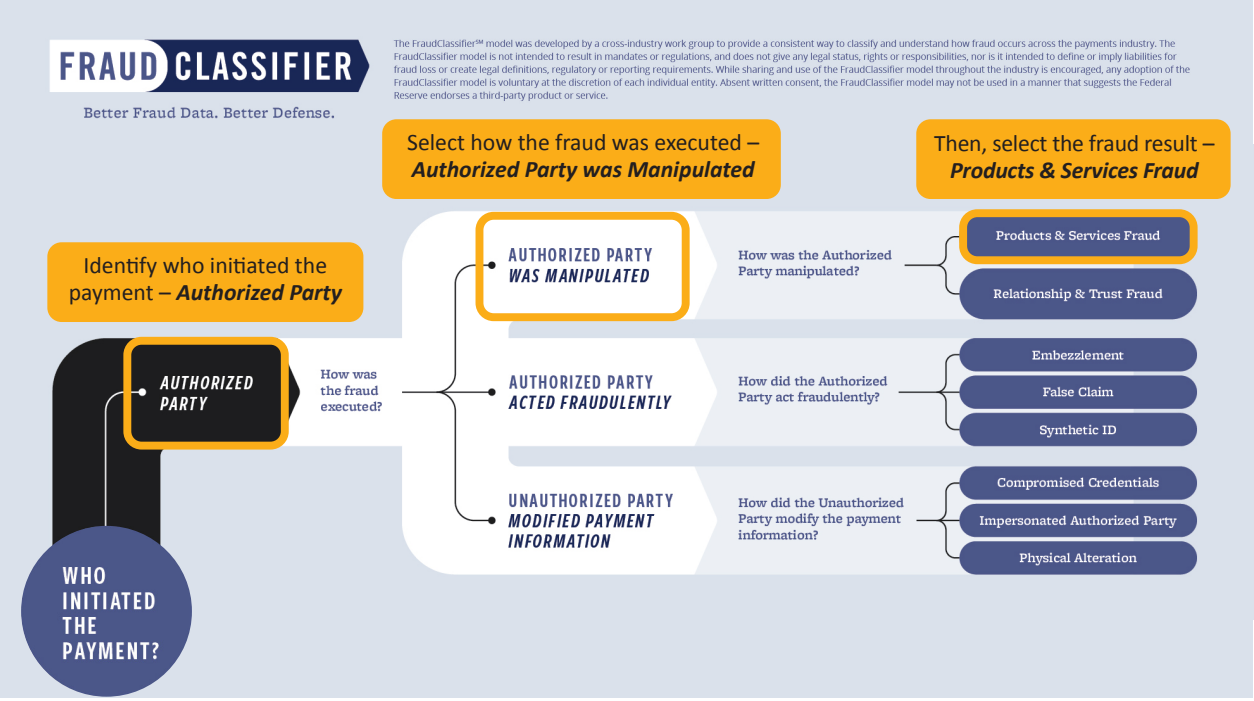
Multiple connection points between the models create opportunities for users to bypass repetitive steps when navigating between them. For example, when using the FraudClassifier model to classify a fraud event, the ScamClassifier model also can be used for an additional level of classification if the root cause of the fraudulent activity was a scam. The following scenarios elaborate on the connections between the models and how the models can interact based on which model is used as the starting point and whether the party or payment was authorized or unauthorized.

SCENARIO 1: Authorized Party was Manipulated into Sending a Payment

Emily made a payment to purchase a puppy she saw online, but she never received the puppy. The seller stopped responding to her and she later finds out the puppy isn't real.

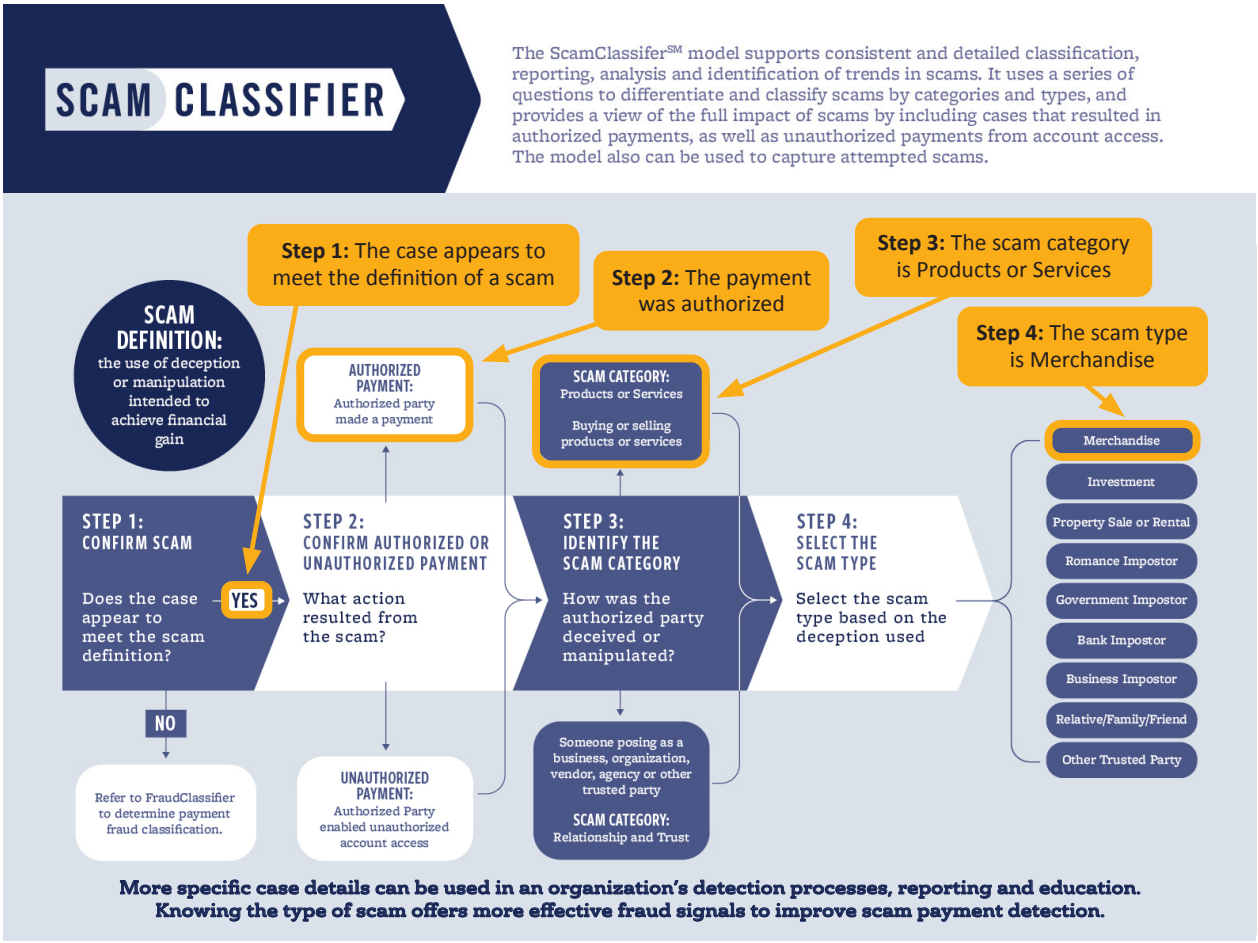
In this first scenario, an authorized party was manipulated into sending a payment. Beginning with the FraudClassifier model, the series of questions guides the user to classify this as a product and services fraud.

USING THE FRAUDCLASSIFIER℠ AND SCAMCLASSIFIER℠ MODELS TOGETHER



USING THE FRAUDCLASSIFIER℠ AND SCAMCLASSIFIER℠ MODELS TOGETHER

Navigating over to the ScamClassifier model, the user can locate the products or services category in step 3 and then dive a level deeper to select the scam type in step 4.

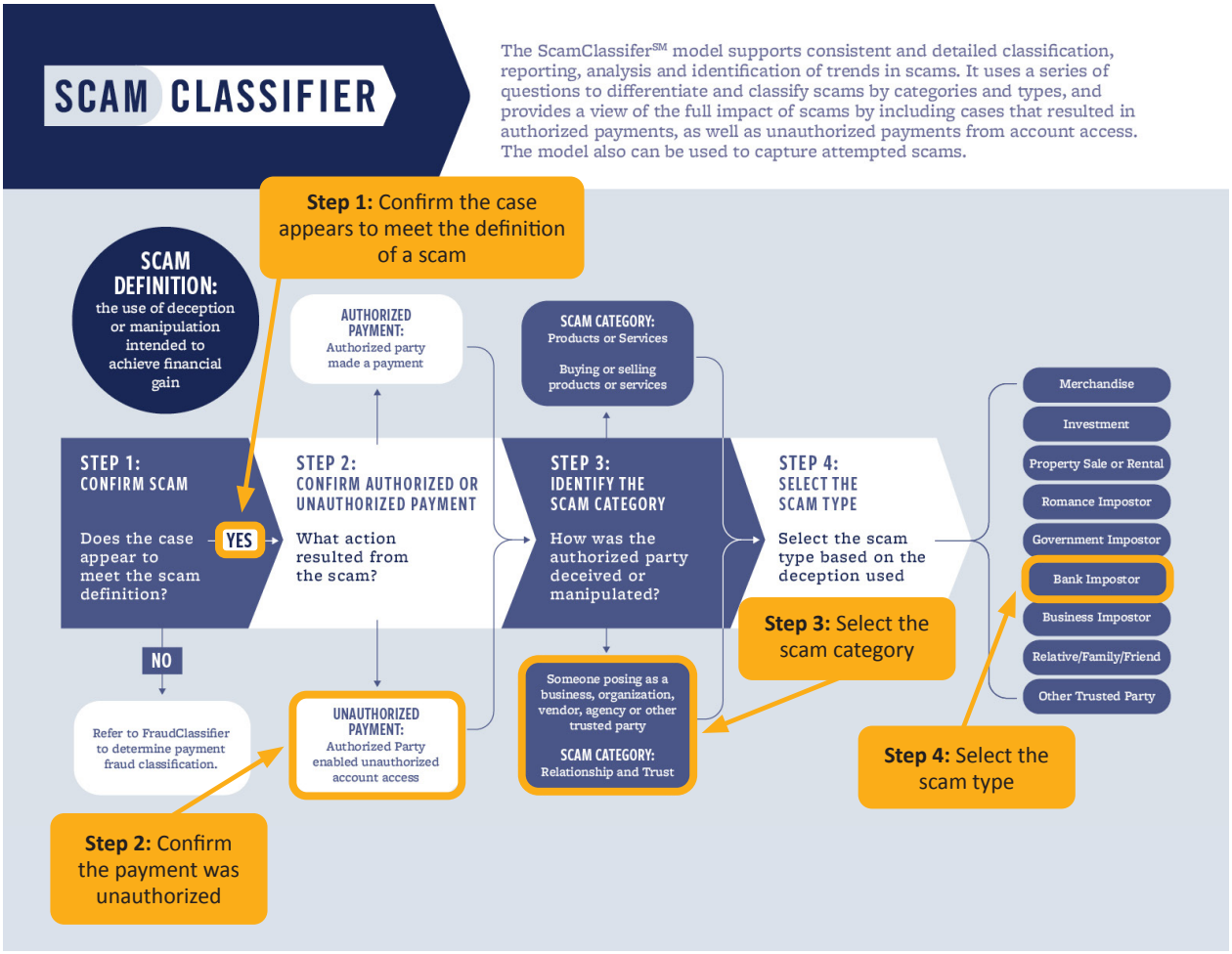


SCENARIO 2: Unauthorized Party Completed an Unauthorized Payment

Zack received a text that he thought was from his financial institution. He clicked on the link in the text message and provided his online banking credentials. Later, he noticed unauthorized payments from his account.

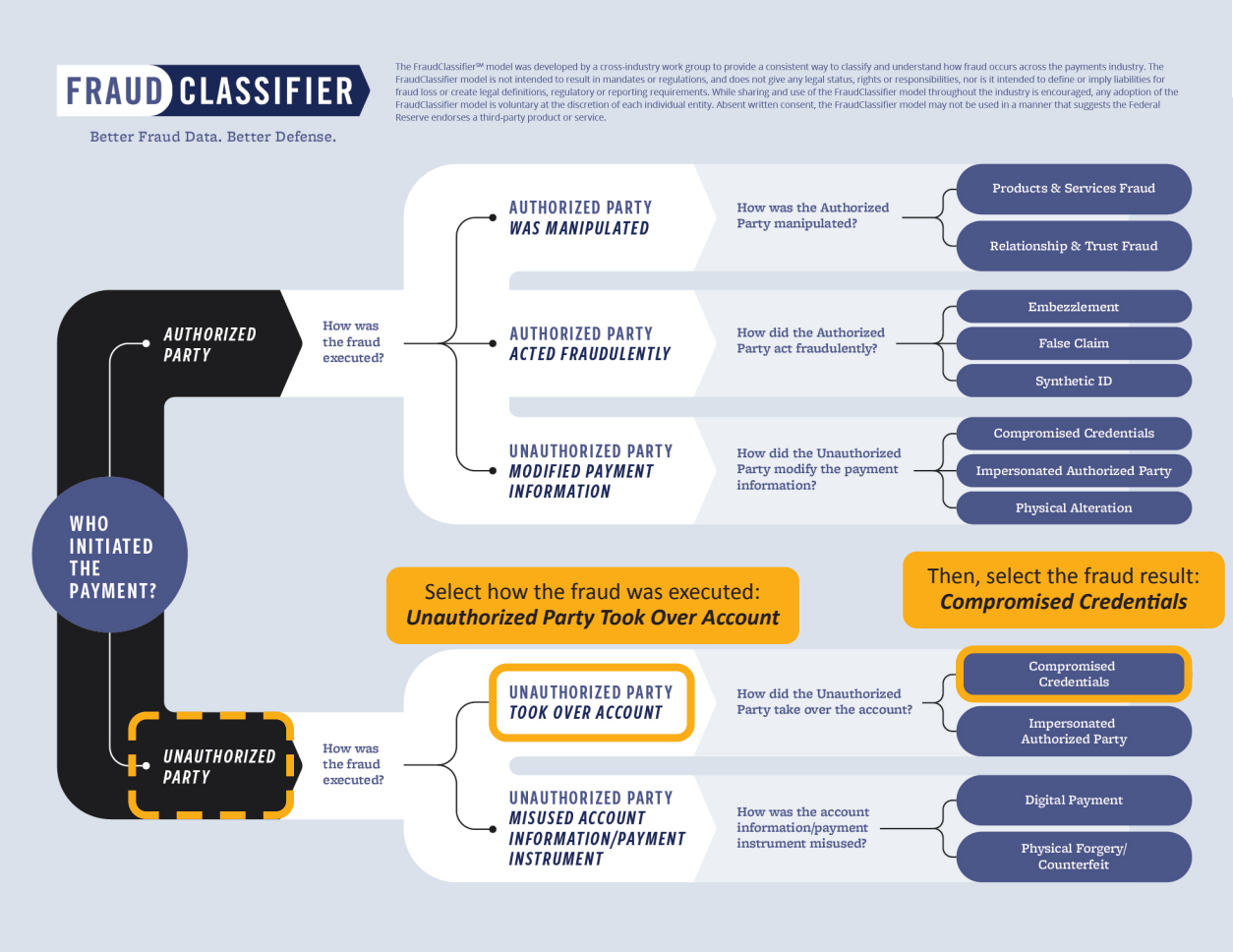
USING THE FRAUDCLASSIFIER℠ AND SCAMCLASSIFIER℠ MODELS TOGETHER

This is an example of an unauthorized party making an unauthorized payment. Although the classification could begin with either the FraudClassifier model or the ScamClassifier model — based on the user's preference — this example will begin with the ScamClassifier model.



USING THE FRAUDCLASSIFIER℠ AND SCAMCLASSIFIER℠ MODELS TOGETHER

Since it is already known that an unauthorized party initiated the payment, the user can jump to the next step on the FraudClassifier model that asks, "How was the fraud executed?"



This additional level of classification provides the fraud type — compromised credentials — that led to the unauthorized activity, as well as the scam type that led to the customer compromising his credentials.

CONCLUSION

Organizations can benefit from understanding the connections between the FraudClassifier model and ScamClassifier model. The fraud scenario and type may dictate using one or the other model as a stand-alone. However, using these models in conjunction can help identify additional critical classification details, avoid the need to answer *repetitive* questions and surface actionable information for fraud mitigation.

USING THE FRAUDCLASSIFIER℠ AND SCAMCLASSIFIER℠ MODELS TOGETHER

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.

The ScamClassifier model is not intended to result in mandates or regulations, and does not give any legal status, rights or responsibilities, nor is it intended to define or imply liabilities for loss or create legal definitions, regulatory or reporting requirements. While sharing and use of the ScamClassifier model throughout the industry is encouraged, any adoption of the ScamClassifier model is voluntary at the discretion of each individual entity. Absent written consent, the ScamClassifier model may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.

Sharing and use of the FraudClassifier model throughout the industry is encouraged; any adoption of the FraudClassifier model is voluntary at the discretion of each individual entity. The FraudClassifier model is not intended to result in mandates or regulations, and does not give any legal status, rights or responsibilities, nor is the FraudClassifier model intended to define or imply liabilities for fraud loss or create legal definitions, regulatory or reporting requirements. Absent written consent, the FraudClassifier model may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.

Both "ScamClassifier" and "FraudClassifier" are service marks of the Federal Reserve Banks. A list of marks related to financial services products that are offered to financial institutions by the Federal Reserve Banks is available at FRBservices.org.