

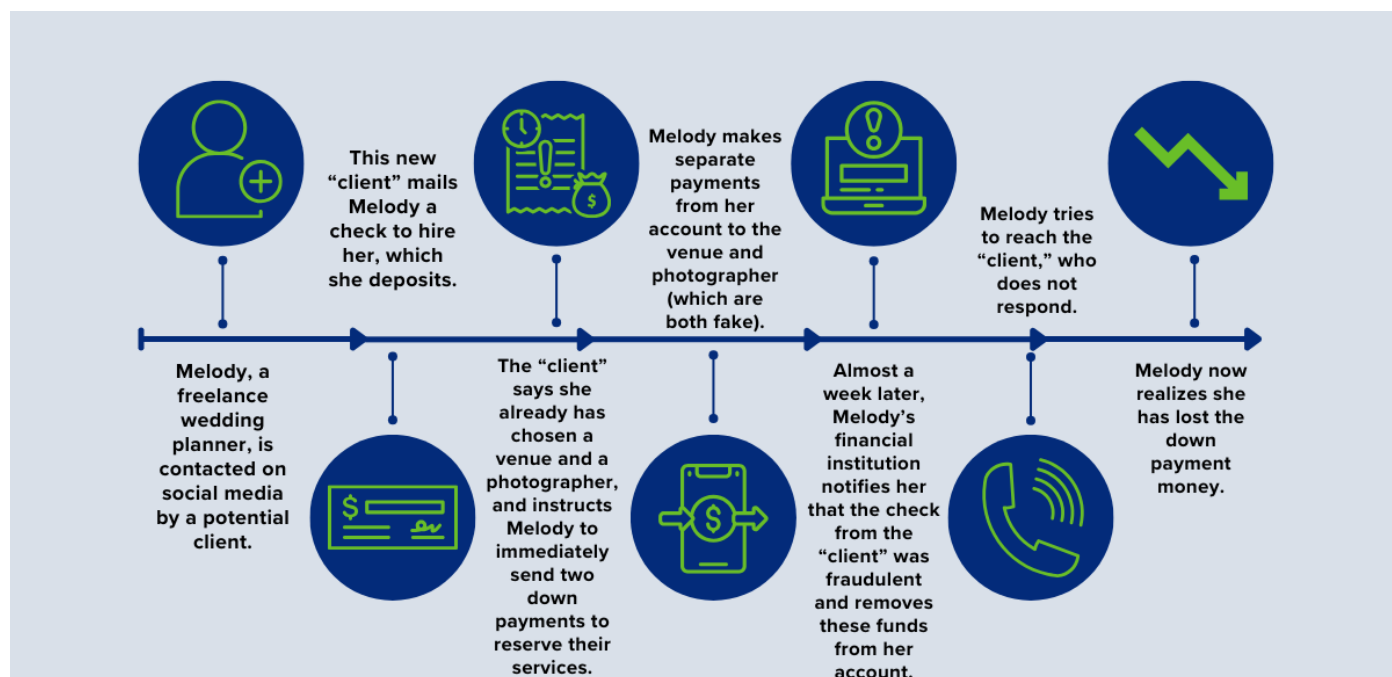
LEVERAGING THE SCAMCLASSIFIERSM MODEL FOR CHECK SCAMS

Over the years, criminals often have leveraged fraudulent paper checks to help perpetrate scams – defined as [the use of deception or manipulation intended to achieve financial gain](#). Longstanding trust in the legitimacy of paper checks, as well as lengthy processing times, can make them a lucrative target for scams and fraud. For example, a financial institution may allow a customer to access funds from a check deposit within two business days, even though it may take a week or more for the institution to be notified the check is fraudulent. The customer then loses any money that he spent using fraudulent deposit funds after they are removed from his account.

Introduced by the Federal Reserve in 2024, the [ScamClassifier model](#) can assist in identifying the root cause of the fraud that occurred due to a scam – either as a products or services scam, or as a relationship and trust scam. Use of the ScamClassifier model to support more consistent and detailed classification of scams can help prevent losses. In addition, having clear insights into the most relevant trends ultimately can lead to more targeted education and prevention strategies.

CHECK FRAUD SCHEME: THE WEDDING PLANNER

In this example, a freelance wedding planner is manipulated by a criminal. The supposed “client” sends her a fraudulent check in the mail as an initial payment for her services. The wedding planner deposits the check into her account without realizing the check is fake. Several days later, her financial institution is notified that the deposited check was created fraudulently using a stolen account number and in turn, notifies the wedding planner and removes the funds from her account.

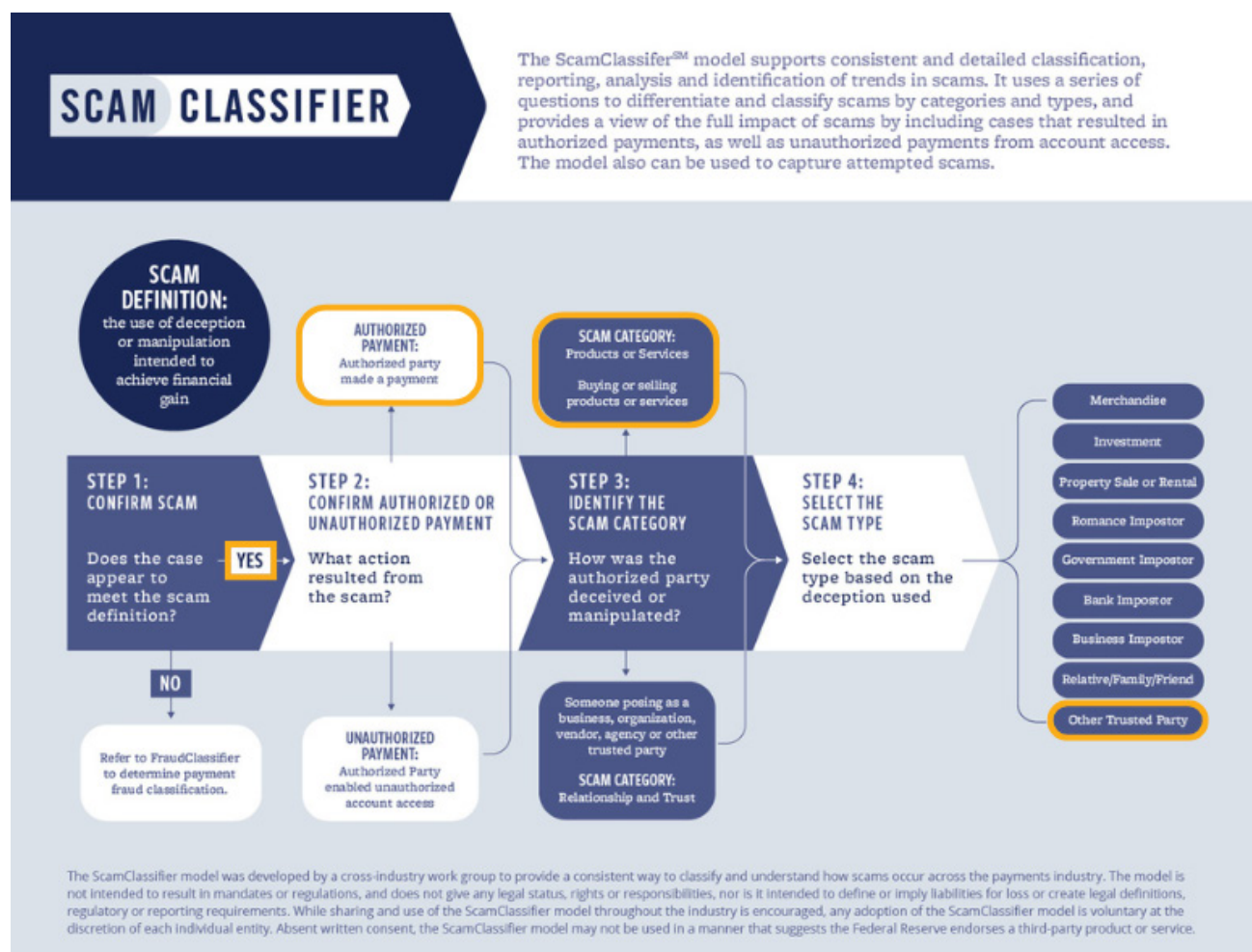


LEVERAGING THE SCAMCLASSIFIERSM MODEL FOR CHECK SCAMS

SCAM > AUTHORIZED PARTY > PRODUCTS OR SERVICES > OTHER TRUSTED PARTY

When this scenario is analyzed using the ScamClassifier model:

- Step 1 is to confirm it is a scam using the scam definition outlined above and in the graphic below. This case is a scam because the criminal uses manipulation to achieve financial gain (the down payment money).
- In step 2, whether the payment was authorized or unauthorized is assessed. These were authorized payments since Melody, the authorized party, deposited the check and sent down payments to the fake venue and photographer.
- Step 3 is where the scam is categorized as products or services, because it involves Melody's wedding planning services.
- Last, in step 4, selection of the scam type is made based on the deception used. In this case, the scam involved an "other trusted party," signifying that many small business owners inherently trust their clients.





LEVERAGING THE SCAMCLASSIFIERSM MODEL FOR CHECK SCAMS

A key to mitigating fraud and spreading awareness about it is having a better understanding of the risk. The layers of classification within the ScamClassifier model, along with other attributes if desired, can help provide a holistic picture of scams involving check fraud and corresponding trends, as illustrated by the check fraud scheme described in this article. Ultimately, greater adoption of the model also may provide more consistent industrywide classifications to facilitate sharing information between entities, assist users to identify cross-industry scam trends, and more accurately define the true magnitude of this growing problem.

As the payments industry continues the fight against scams, explore the value of the ScamClassifier model for:

- Holistic awareness of trends
- Scope, volume and financial impacts of check scams
- Streamlined remediation for victims
- Robust employee training
- Targeted and relevant customer education

The check fraud mitigation toolkit was developed by the Federal Reserve to help educate the industry about check fraud 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.