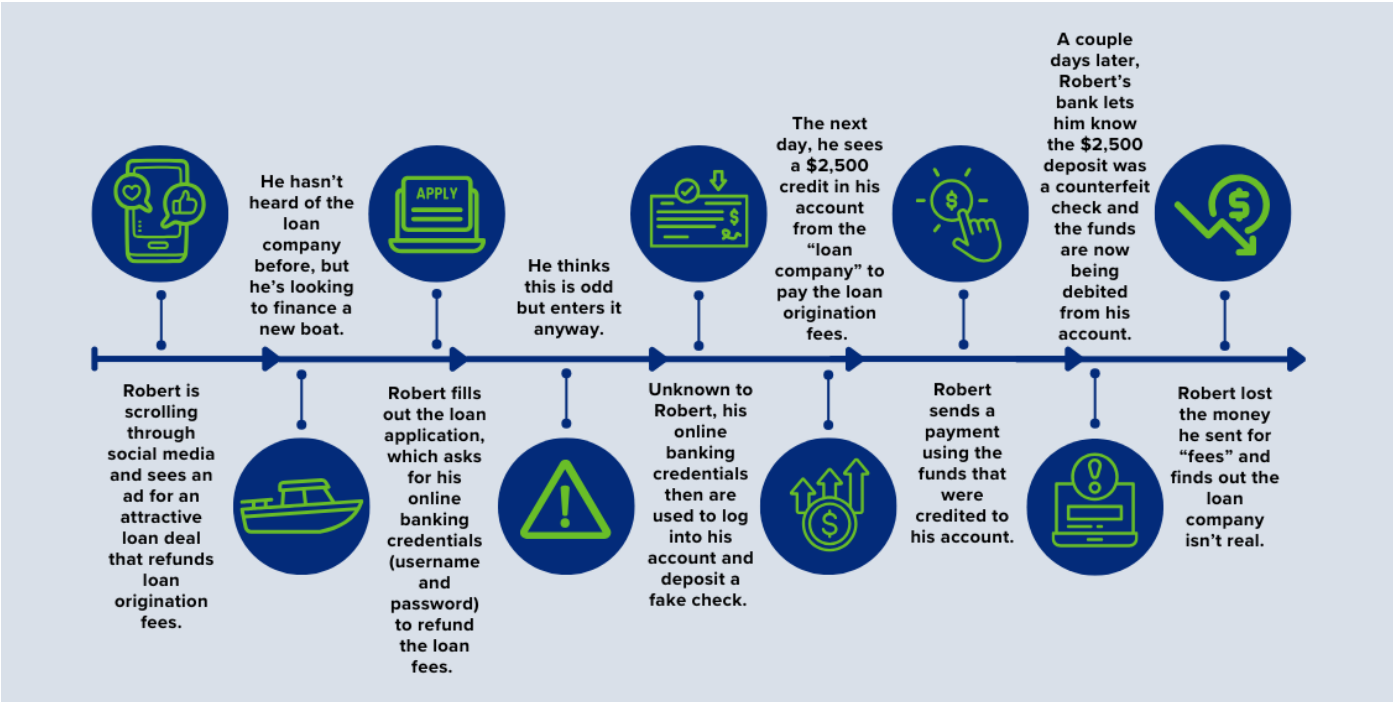
ADDRESSING DEPOSIT FRAUD USING BOTH THE SCAMCLASSIFIER℠ AND FRAUDCLASSIFIER℠ MODELS

Individuals can be tricked into depositing fraudulent checks. Alternatively, they may be deceived or manipulated into providing their online banking credentials to a criminal, which allows the criminal unauthorized access to their accounts. This could facilitate fraudulent check deposits made through online or mobile banking. If customers are deceived into believing the deposit is from a legitimate source, they may spend the funds and find themselves with a financial loss when the deposited check is identified as fraudulent and removed from their account.

Scams can lead to *authorized transactions* made by the authorized account owner, or *unauthorized transactions,* where a payment is initiated by a third party who has no legitimate right to move the money. The following scheme demonstrates how the ScamClassifier model can be used alongside the FraudClassifier model to classify an event when the root cause of unauthorized activity was a scam. Together, the models can be used to enable more robust classification for fraud reporting, prevention and education.

UNAUTHORIZED DEPOSIT FRAUD STEMMING FROM A SCAM

In this scenario, an individual completes a loan application believed to be directed to a legitimate lender but that is actually triggered by a criminal impersonating a lender. The application prompts applicants for their online banking credentials, which they enter and therefore, unknowingly provide a criminal with access to their online banking accounts. As a result, a fraudulent deposit is made, and the "lender" tricks the applicant into sending them funds. This scenario discusses how unauthorized deposits can originate from scams if the authorized party is deceived or manipulated into providing account access that leads to activity the authorized account holder did not initiate or approve.

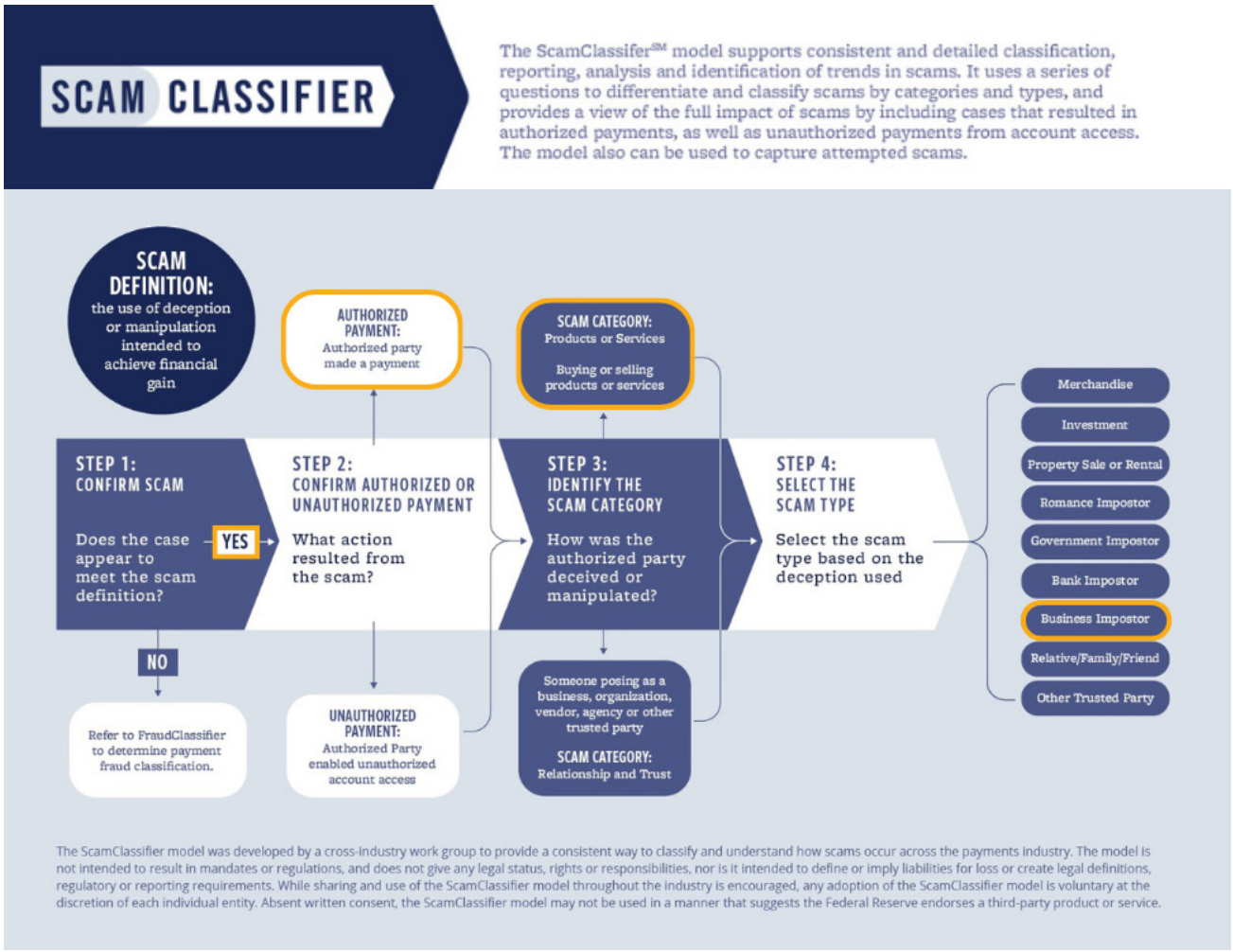


ADDRESSING DEPOSIT FRAUD USING BOTH THE SCAMCLASSIFIER℠ AND FRAUDCLASSIFIER℠ MODELS

SCAM > AUTHORIZED PARTY > PRODUCTS OR SERVICES > BUSINESS IMPOSTOR

The ScamClassifier model can be used to classify the root cause of an event when it is a scam.

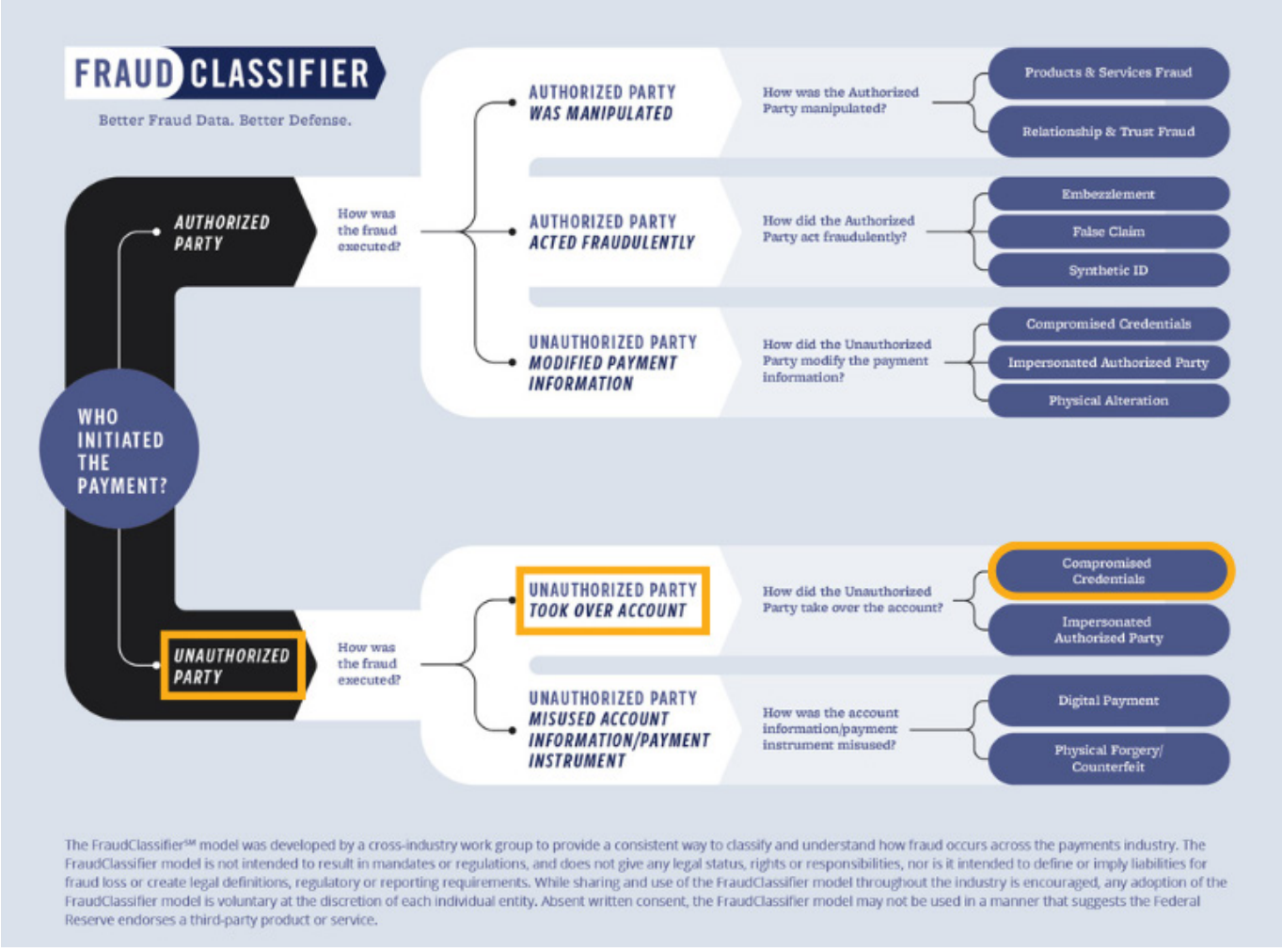
- Step 1 is to confirm it is a scam using the definition in the graphic below. The root cause of this case is a scam because Robert was deceived into submitting a loan application and sending money for loan fees he thought were legitimate.
- In step 2, this is considered an authorized transaction since Robert initiated the fee payment.
- Step 3 is where the scam is categorized as products or services because the loan is considered a service.
- In the final step, since the loan ad and application impersonated a lending company that Robert thought was legitimate, the scam type is "business impostor."



ADDRESSING DEPOSIT FRAUD USING BOTH THE SCAMCLASSIFIER℠ AND FRAUDCLASSIFIER℠ MODELS

Since Robert did not initiate or authorize the $2,500 check deposit into his account, the FraudClassifier model also can be used to classify the fraud event. This additional level of classification generates more robust reporting and awareness about the root cause of the check fraud, which can be incorporated into fraud prevention strategies and education.

- In step 1, when determining who authorized the payment, unauthorized party is selected.
- Step 2 is where it is determined how the fraud was executed. In this case, a third party made the unauthorized deposit by taking over the account.
- In step 3, the account was taken over because the online banking credentials were compromised during the scam. The fraud classification is "compromised credentials."



The ScamClassifier and FraudClassifier models can provide actionable insight into the trends and the corresponding root causes that are most impactful to the payment industry.

ADDRESSING DEPOSIT FRAUD USING BOTH THE SCAMCLASSIFIER℠ AND FRAUDCLASSIFIER℠ MODELS

As the payments industry continues the fight against scams, explore the value of the ScamClassifier and FraudClassifier models to support:

- 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 and scams mitigation toolkits were developed by the Federal Reserve to help educate the industry about check fraud and scams and outline potential ways to help detect and mitigate these fraud types. Insights for the toolkits were provided through interviews with industry experts, publicly available research, and team member expertise.

These toolkits, and the FraudClassifier and ScamClassifier models discussed in these toolkits, are 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 the toolkits and the models is encouraged, utilization is voluntary at the discretion of each individual entity. Absent written consent, neither the toolkits nor the models may be used in a manner that suggests the Federal Reserve endorses a third-party product or service.