ROMANCE SCAMS, CHECK FRAUD AND THE SCAMCLASSIFIER℠ MODEL
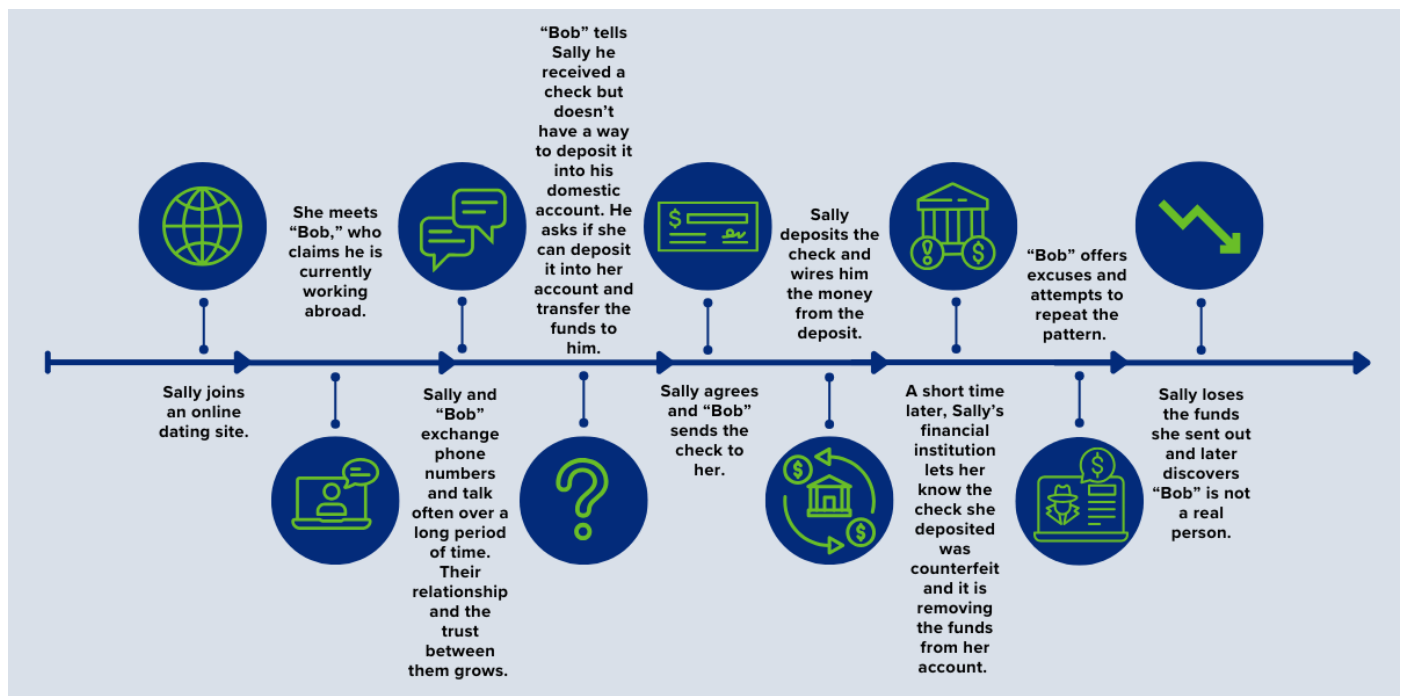
Criminals create scams to carry out check fraud by deceiving individuals into depositing counterfeit checks in their accounts. At the direction of the criminal, financial institution customers who do not realize a deposited check was fraudulent may send funds from this check deposit to someone else – i.e., the criminal. As a result, customers may become unwitting money mules by helping criminals transfer illicit funds. Customers also may find themselves liable for the funds they sent when these deposited checks are identified as fraud and the deposited amounts are subsequently removed from their accounts.

The ScamClassifier model divides scams into either a products or services scam or a relationship and trust scam. Relationship and trust scams typically involve a transfer of funds to an imposter acting as a trusted or authoritative party, where there is no expectation or promise of merchandise in exchange for the funds. The following scheme exemplifies how check fraud can stem from relationship and trust scams, and how the ScamClassifier model can be leveraged for more robust prevention and customer education to help customers recognize and avoid these scams.

CHECK FRAUD SCHEME: ONLINE ROMANCE

In this scheme, an online relationship is cultivated between an unsuspecting victim and a "love interest," who is really a criminal. Over a long period of time, the "love interest" works to develop the victim's deep level of trust. Due to the relationship that has been established, the criminal is able to convince a victim to deposit a check and forward the money. The victim later realizes the check was fraudulent and discovers the supposed "love interest" was fabricated by a criminal.
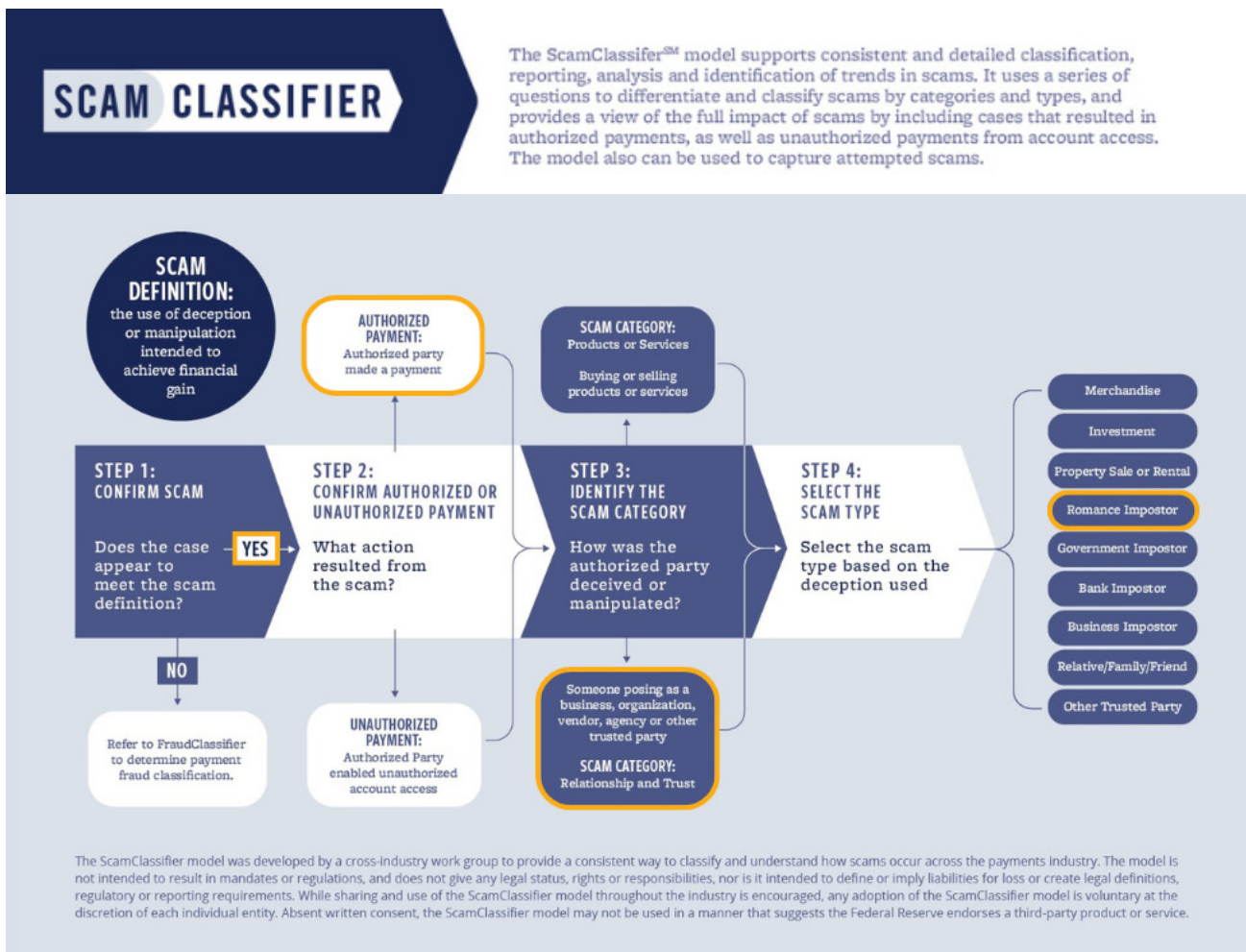

Top row (events above the timeline):

- She meets "Bob," who claims he is currently working abroad.
- "Bob" tells Sally he received a check but doesn't have a way to deposit it into his domestic account. He asks if she can deposit it into her account and transfer the funds to him.
- Sally deposits the check and wires him the money from the deposit.
- "Bob" offers excuses and attempts to repeat the pattern.

Bottom row (events below the timeline):

- Sally joins an online dating site.
- Sally and "Bob" exchange phone numbers and talk often over a long period of time. Their relationship and the trust between them grows.
- Sally agrees and "Bob" sends the check to her.
- A short time later, Sally's financial institution lets her know the check she deposited was counterfeit and it is removing the funds from her account.
- Sally loses the funds she sent out and later discovers "Bob" is not a real person.

SCAM > AUTHORIZED PARTY > RELATIONSHIP AND TRUST > ROMANCE IMPOSTOR

When using the ScamClassifier to assess the type of scam in this scenario:

- Step 1 is to confirm that the scenario meets the definition of a scam, outlined in the graphic below. Since "Bob" deceived Sally, this is a scam.

- Step 2 determines whether the payment was authorized or unauthorized. Sally sent the money to "Bob" – therefore, the payment was authorized.

- In step 3, the scam category is defined as "relationship and trust" because "Bob" leveraged the trust he developed with Sally to carry out this scam.

- Last, in step 4, the scam type is "romance impostor" due to the way the criminal "Bob" pretended to be a love interest to deceive and manipulate Sally.

The ScamClassifier℠ model supports consistent and detailed classification, reporting, analysis and identification of trends in scams. It uses a series of questions to differentiate and classify scams by categories and types, and provides a view of the full impact of scams by including cases that resulted in authorized payments, as well as unauthorized payments from account access. The model also can be used to capture attempted scams.

The ScamClassifier model was developed by a cross-industry work group to provide a consistent way to classify and understand how scams occur across the payments industry. The 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.

The ScamClassifier model is a tool that provides insight into the types of scams that target individuals, which can be used to increase financial institution employee and customer awareness of scams – including those related to check fraud and money mule activity. Information on the different types of money mules and the signs associated with money mule activity is available from the FBI.

Additionally, the ScamClassifier model offers a structure for consistent classification to complement efforts to identify and prevent check fraud and the movement of illicit funds originating from scams, as well as to educate potential scam victims.

> **As the payments industry continues the fight against scams, explore the value of the ScamClassifier model to support consistent classification 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