CLASSIFYING ACCOUNT TAKEOVER FRAUD USING THE FRAUDCLASSIFIER℠ AND SCAMCLASSIFIER℠

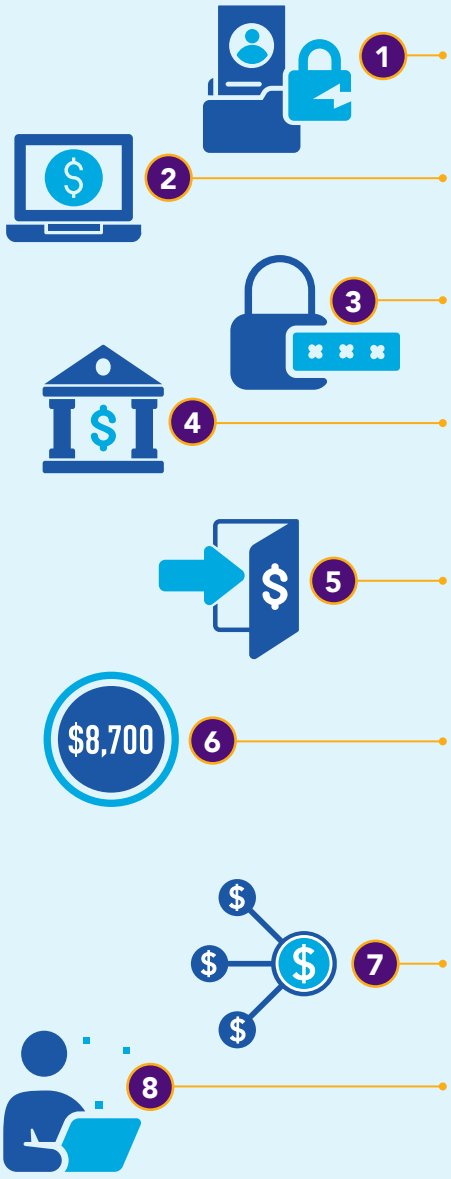
Account takeover fraud can vary in terms of how criminals *harvest* credentials, obtain account *access*, and *monetize* the account. For financial institutions, more consistent classification of these incidents supports account takeover fraud prevention and detection efforts.

The FraudClassifier and ScamClassifier models are voluntary classification structures that were developed to help address the industrywide challenge of inconsistent classifications for fraud and scams. They enable payments stakeholders to classify fraud and scams independently of payment type, payment channel or other payment characteristics. The FraudClassifier model can be used as a standalone classification structure applied for fraudulent payments resulting from account takeover fraud. In instances where the account takeover fraud incident was enabled by a scam, the ScamClassifier model can also be used. Usage of the models can help organizations improve account takeover fraud mitigation through better identification of fraud and scam types, enhanced reporting, and more tailored customer education.

CLASSIFYING ACCOUNT TAKEOVER FRAUD USING THE FRAUDCLASSIFIER℠ AND SCAMCLASSIFIER℠

USING THE FRAUDCLASSIFIER MODEL TO CLASSIFY PAYMENTS FRAUD RESULTING FROM ACCOUNT TAKEOVER

In the following hypothetical scenario, Jason gains access to Mona's financial institution account using compromised personal information obtained via a data breach:

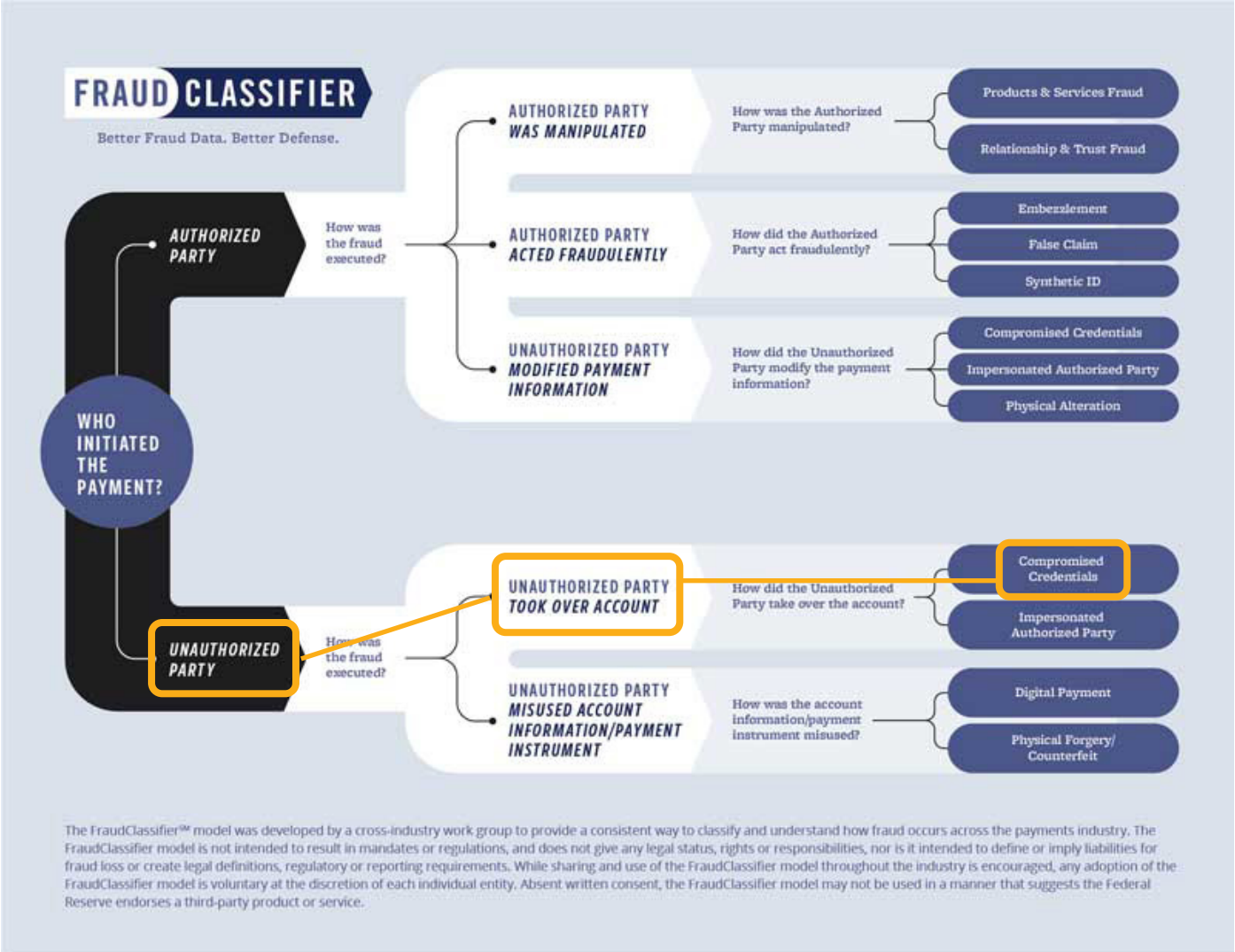


1. **An online retailer experiences a data breach,** exposing Mona's name, birthdate, username (her email address) and password.
2. Two weeks later, Jason purchases the online retailer's breached data on a **dark web marketplace**.
3. With the help of AI tools, Jason creates **thousands of username-password combinations** from the stolen data.
4. **Using automated scripts,** he attempts account logins across hundreds of online banking portals until he identifies the correct financial institution and valid credentials for Mona's account.
5. **Jason gains unauthorized access** to Mona's account. Once inside the account, he changes her password and updates the user email address and phone number with contact information that he controls.
6. **He transfers $8,700 to an account** at another financial institution that he controls. The financial institution flags the unusually large transaction as suspicious and sends an automated text message to the phone number on file. Jason receives the message and confirms the transaction as legitimate.
7. **The funds are sent and quickly dispersed** through a network of mule accounts.
8. The next day, **Mona tries to log in to her account** but is unable to do so. She contacts her financial institution for assistance.

CLASSIFYING ACCOUNT TAKEOVER FRAUD USING THE FRAUDCLASSIFIER℠ AND SCAMCLASSIFIER℠

Let's begin classification of the incident using the FraudClassifier model.

- **Step 1:** Determine whether an authorized or unauthorized party initiated the payment. In this scenario, Jason is not an authorized party on the account. Therefore, an unauthorized party initiated the payment.
- **Step 2:** Confirm how the unauthorized payment was executed. In this case, Jason took over the account.
- **Step 3:** Assess how the unauthorized party took over the account. Jason purchased Mona's account credentials on the dark web following a data breach. The fraud was executed using compromised credentials.



The FraudClassifier℠ model was developed by a cross-industry work group to provide a consistent way to classify and understand how fraud occurs across the payments industry. The FraudClassifier 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 fraud loss or create legal definitions, regulatory or reporting requirements. While 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. 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.

CLASSIFYING ACCOUNT TAKEOVER FRAUD USING THE FRAUDCLASSIFIER℠ AND SCAMCLASSIFIER℠

The ScamClassifier model can be used alongside the FraudClassifier model to classify payments fraud when the root cause of the unauthorized account access was a scam. The user can start with either model depending on their preference.

USING BOTH THE FRAUDCLASSIFIER AND SCAMCLASSIFIER MODELS TO CLASSIFY AN ACCOUNT TAKEOVER FRAUD INCIDENT

In this example, a bank impersonation scam enables a criminal to gain access to John's financial institution account and make an unauthorized payment:

1. **Blake receives a text message** from a sender that he believes to be from his financial institution. The message indicates that the debit card associated with his account has been frozen due to suspicious activity. It states that the account must be verified immediately to restore access.

2. **Blake is concerned about losing access to his account.** The text message prompts him to click on a link to login, where he can verify access and unlock his account.

3. **Blake clicks on the link**, which leads him to a fake login page designed to mimic his financial institution's mobile site. He enters his username and password as requested.

4. The criminal, Jane, **immediately uses the credentials to try to log into the real bank** website, triggering a real one-time password (OTP) request from Blake's financial institution.

5. Blake receives another text message that instructs him to enter the OTP using the link provided to complete verification. **Having received the OTP from Blake, Jane gains access to the account.** She initiates a large ACH credit transfer to another account.

6. **The next day, Blake sees a story about a bank impostor scam** impacting his bank on the local news. He tries to log in to his account to check his balance, panicked he may have been a target of this scam. He is unable to do so and reaches out to his financial institution for help.

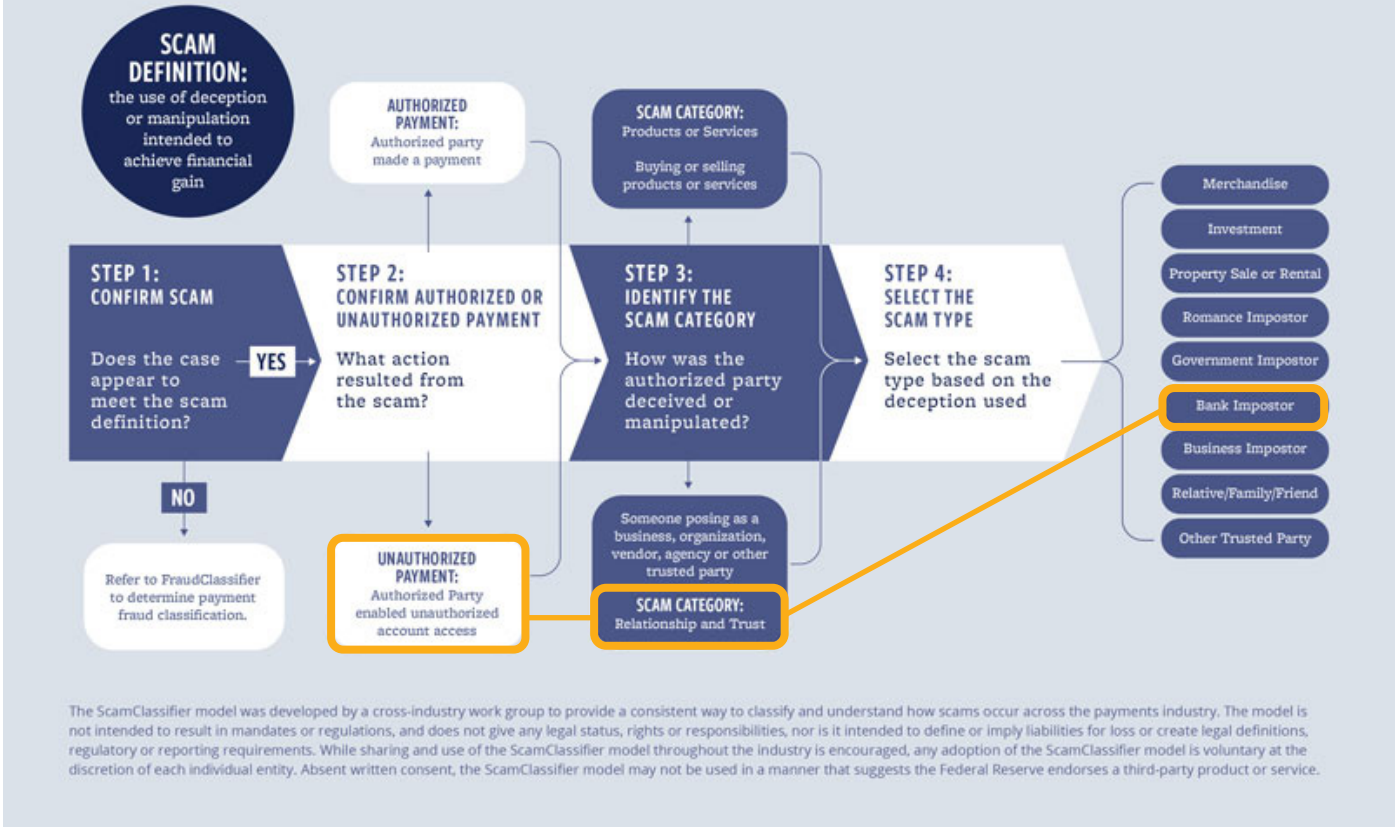
CLASSIFYING ACCOUNT TAKEOVER FRAUD USING THE FRAUDCLASSIFIER℠ AND SCAMCLASSIFIER℠

Let's begin classification of the incident using the ScamClassifier model.

- **Step 1:** Confirm whether the scenario meets the definition of a scam, or "the use of deception or manipulation intended to achieve financial gain". Since Jane deceived Blake into providing his account credentials and OTP, this incident meets the definition of a scam.
- **Step 2:** Determine whether the payment was authorized or unauthorized. In this scenario, an authorized party enabled unauthorized account access, resulting in an unauthorized payment.
- **Step 3:** Assess the appropriate scam category. In this example, the scam category is "relationship and trust" because the criminal leveraged the user's inherent trust in their financial institution to carry out the scam.
- **Step 4:** Label the scam type as "bank impostor" because Jane pretended to be Blake's financial institution.

SCAM CLASSIFIER

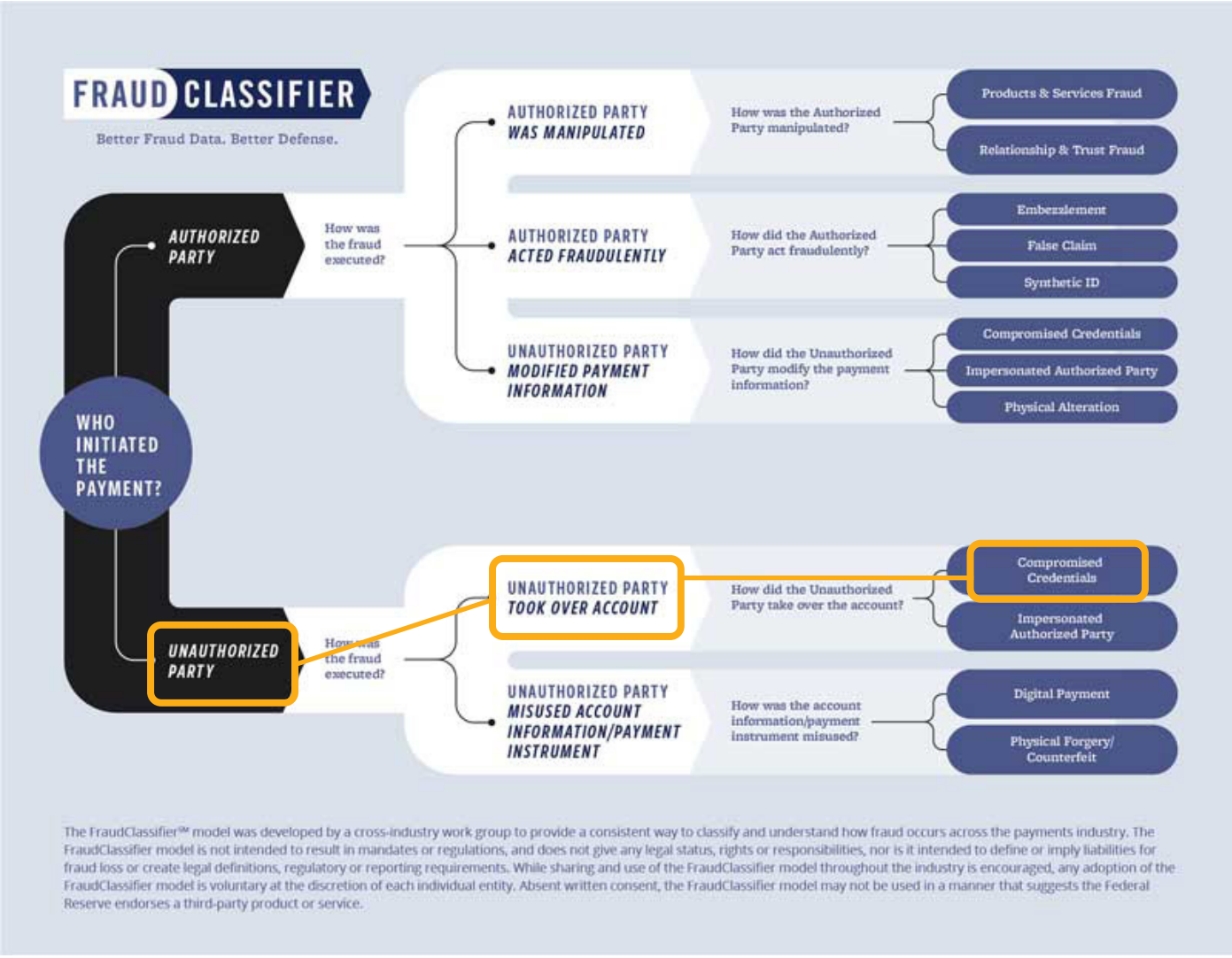
The ScamClassifier℠ model supports consistent and detailed classification, reporting, analysis and identification of trends in scams. It uses a series of questions to differentiate and classify scams by categories and types, and provides a view of the full impact of scams by including cases that resulted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



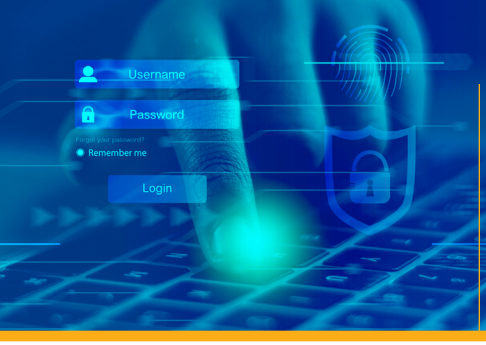
The ScamClassifier model was developed by a cross-industry work group to provide a consistent way to classify and understand how scams occur across the payments industry. The model is not intended to result in mandates or regulations, and does not give any legal status, rights or responsibilities, nor 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.

CLASSIFYING ACCOUNT TAKEOVER FRAUD USING THE FRAUDCLASSIFIER℠ AND SCAMCLASSIFIER℠

Now the user can move on to classification using the FraudClassifier model. Since it is already known that an unauthorized party initiated the payment, the user can jump to the second step on the FraudClassifier model regarding how the fraud was executed. Again, in this case, an unauthorized party took over the account. The last level of classification provides the fraud type – compromised credentials – that led to unauthorized activity, as well as the scam that led Blake to provide his credentials.



The FraudClassifier℠ model was developed by a cross-industry work group to provide a consistent way to classify and understand how fraud occurs across the payments industry. The FraudClassifier 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 fraud loss or create legal definitions, regulatory or reporting requirements. While 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. 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.



CLASSIFYING ACCOUNT TAKEOVER FRAUD USING THE FRAUDCLASSIFIER℠ AND SCAMCLASSIFIER℠

CONCLUSION

By leveraging the FraudClassifier and ScamClassifier models for account takeover fraud, organizations can gain greater clarity into account takeover fraud trends impacting their customers and tailor their prevention and detection strategies accordingly. Ultimately, greater adoption of the models 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.

The account takeover fraud 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.