THE FEDERAL RESERVE
FedPayments Improvement

COLLABORATE. ENGAGE. TRANSFORM.

MACHA Fraud Day

Scams, Swindles - and Solutions: Improving Payment Scam Reporting with ScamClassifier and FraudClassifier Models

Mike Timoney
Vice President of Strategic Industry Engagement
Federal Reserve Financial Services

November 6, 2024

Payments System Improvement

Overview of Role and Purpose

- **Federal Reserve Financial Services (FRFS) Vision:** Deliver a contemporary and trusted payment system that works for everyone
- **Payments System Improvement Mission:** To facilitate material, end-to-end advances in the U.S. payment system that promote integrity, efficiency, and accessibility

Fraud Landscape Summary

Biggest challenges include both “old” and “new” forms of fraud attacks

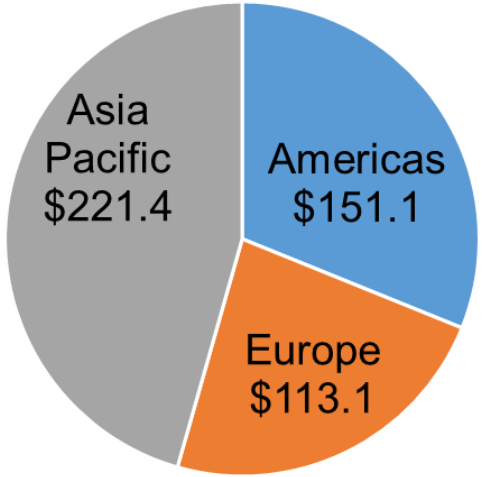
Rise of Historic Threats → **Check Fraud**, **Account Takeover**

Evolving Threats → **Scams**, **Synthetic Identities**, **Money Mules**, **New Account Fraud**

Future Concerning Threats → **GenAI Deep Fakes**, **Scripted Attacks**

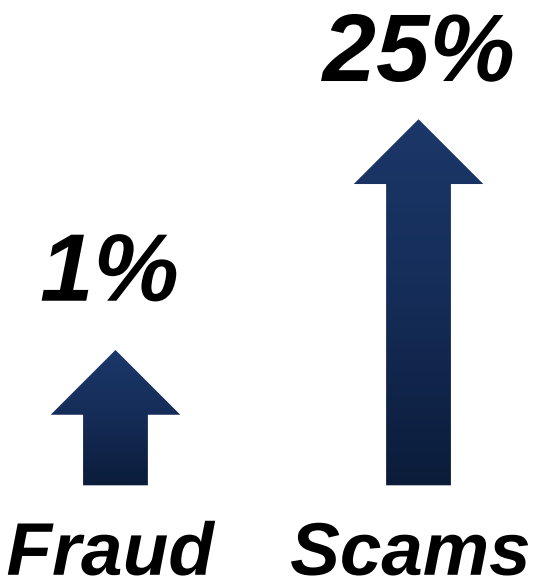
Fraud Landscape Loss Summary (2023)

Global Fraud Loss $485B



Nasdaq Verafin - 2024 Global Financial Crime Report

Loss Increase Over 2022



iC3 – Loss Report

Top Scam Losses

1. ***Investment Related $4.5B***
2. ***Imposter $2.7B***
3. ***Business/Job Opportunities $491M***

Federal Trade Commission – Report Fraud Data

Evolving Threat: Scams

Scams Occur Across Multiple Products & Channels

Federal Trade Commission – Report Fraud Data

Evolving Threat: Scams

Many Factors Contribute to Significant Scam Growth

Data Breaches Increased Availability of Personally Identifiable Information (PII)

Shift to Digital Channels

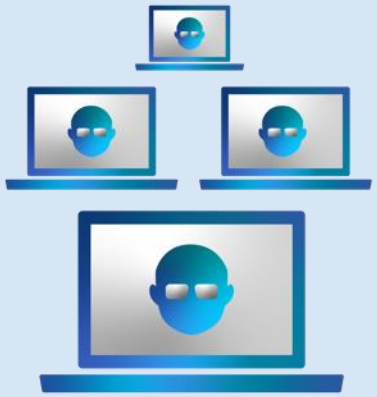
Technology Advances

Convenience of Digital Transactions

Emotional Vulnerabilities

SCAMS – A GROWING PROBLEM

Innovative Fraud Schemes Can Defeat Traditional Fraud Controls



Criminal Groups Increasingly Target Individuals & Businesses

Instant Payments Introduction Encourages Greater Urgency

Fraudulent Authorized Push Payments Often Are Harder to Identify

SCAMS – ADDRESSING THE PROBLEM

Scams Definition & Classification Work Group

Challenge

- Multiple operational definitions of scams
- Lack of necessary detail in existing classification approaches

Response

- Align on an industry-recommended operational scam definition
- Build a classification structure that is detailed enough to document scam nuances and tactics

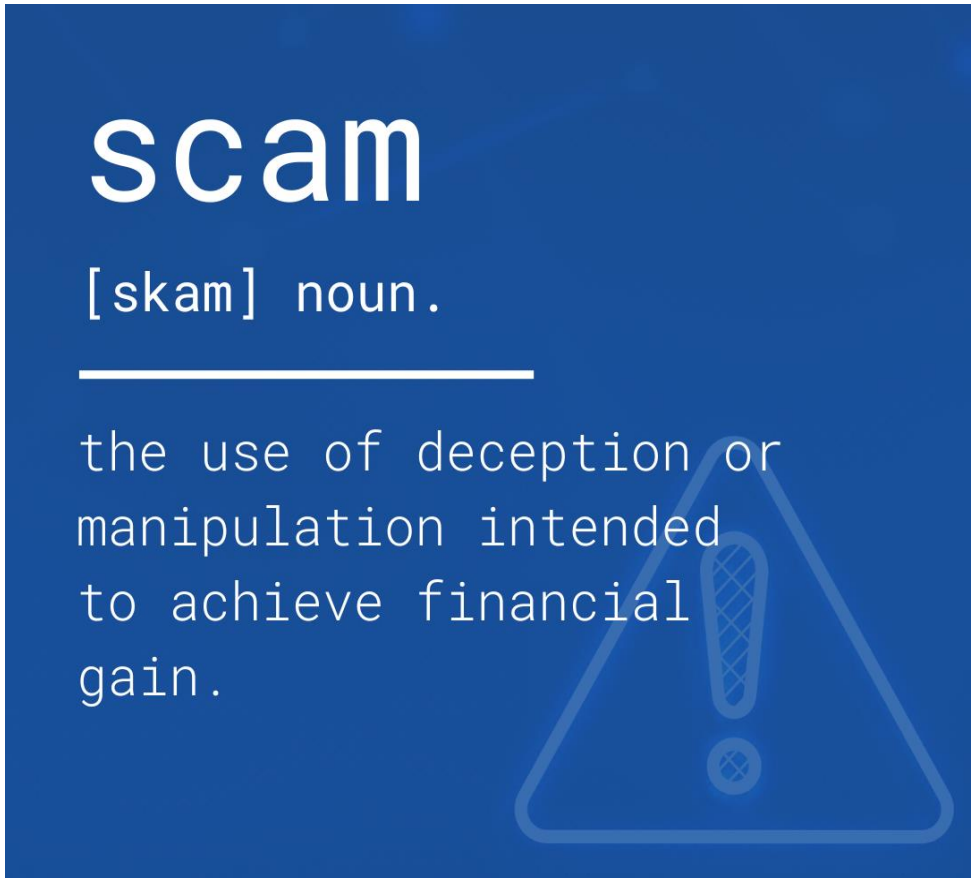
Industry Value

- A shared understanding of the term “scam” and the different scam types
- More consistent scam reporting
- Insights to help improve mitigation

Work group participants are listed on FedPaymentsImprovement.org

SCAMS – A GROWING PROBLEM

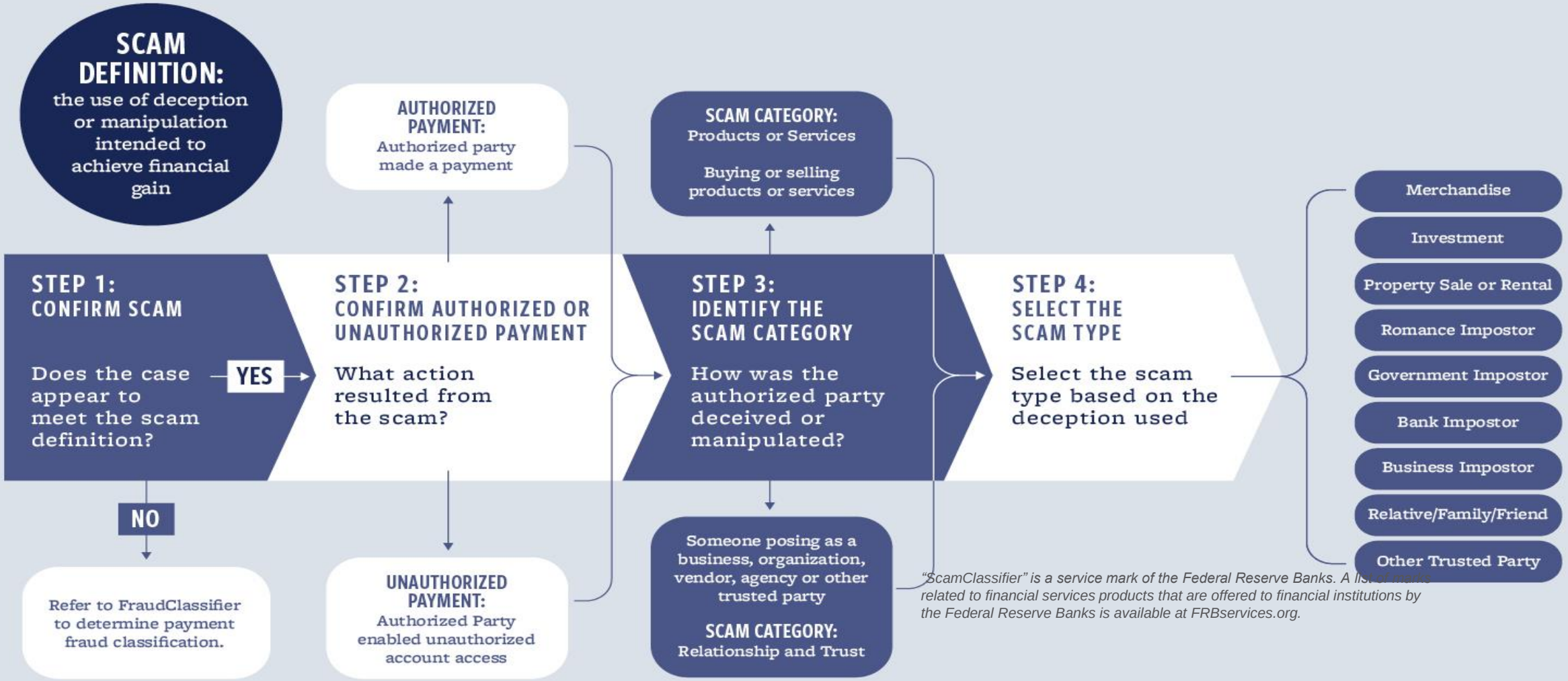
Define Scams to Fight Scams



- **Straightforward definition**
- **Applies to multiple scam types**
- **Promotes a common understanding**
- **Help advance more consistent identification and classification**
- **Can benefit multiple industries**

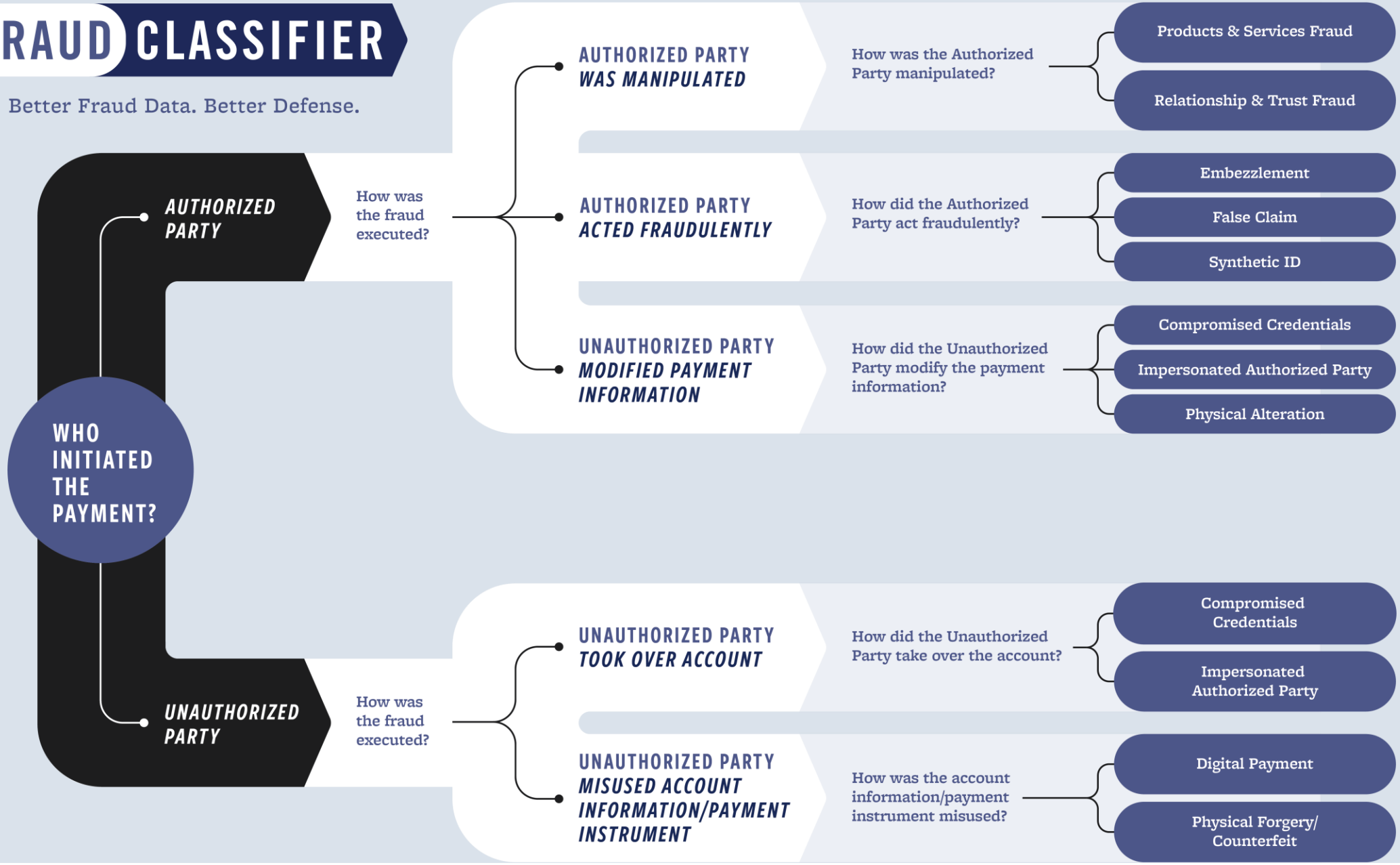
SCAM CLASSIFIER

The ScamClassifer℠ 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.



FRAUD CLASSIFIER

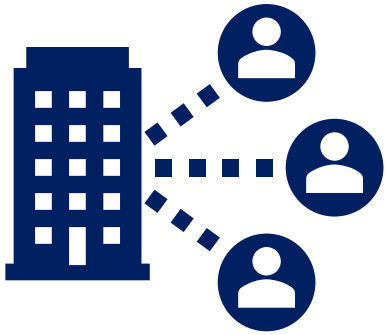
Better Fraud Data. Better Defense.



Evolving Threat: Scams

How Do We Slow Down the Fraudsters?

Education



Fraud Information Sharing

Technology

SCAMS – ADDRESSING THE PROBLEM

Scams Information Sharing Work Group

Challenge

- Fraudsters repeat the same tactics across organizations
- Can be challenging to identify effective, timely mitigation approaches
- Information sharing is incomplete, leading to fragmented approaches and sharing models

Response

- Develop recommendations for fraud information sharing approaches
- Will consider data types, methods and benefits of information sharing

Industry Value

- Stronger management of scams
- Faster reaction to fraud trends
- Enhanced industry awareness

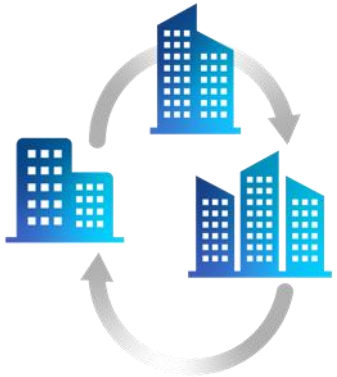
Work group participants are listed on FedPaymentsImprovement.org

SCAMS – ADDRESSING THE PROBLEM

Information Sharing Can Help Mitigate Fraud Losses

Consumer Awareness of Current Fraud Trends Reduces Victimization

Broader Access to Fraud Information Helps Train Fraud Models to Proactively Identify Suspicious Transactions



Sharing of Information Across Industries Can Help Mitigate Fraud Across Organizations

FedDetect® Anomaly overview

FedDetect Anomaly Notification for FedACH® Services helps your institution **identify anomalous activity** and **supplements your fraud detection and alerting** tools, by:

1) **detecting atypical activity** for the current day, using

- **baselines** established for your financial institution's **historical activity,** or
- by **comparing** your ACH transactions **to industry rules;** and

2) allowing your institution to **receive notifications via secure email**.

FedDetect® Anomaly Notification global use cases

Same Day Large Dollar Debit alerts

- Intended for DFIs who receive high dollar debit batches that will settle on the current processing day, potentially requiring funding of Fed/correspondent accounts late in the day
- Starting March 19, 2021, ODFIs were permitted to submit Same Day ACH files until 4:45 p.m. ET; Nacha further increased the per-payment maximum for Same Day ACH transactions from $100,000 to $1 million effective March 18, 2022
- While these changes support innovation and accessibility to Same Day ACH, they also add new challenges for DFIs who may receive late day debits
- Notifications of high dollar debits will help provide awareness and time to ensure appropriate funding action is taken

Notification of Change (NOC) alerts

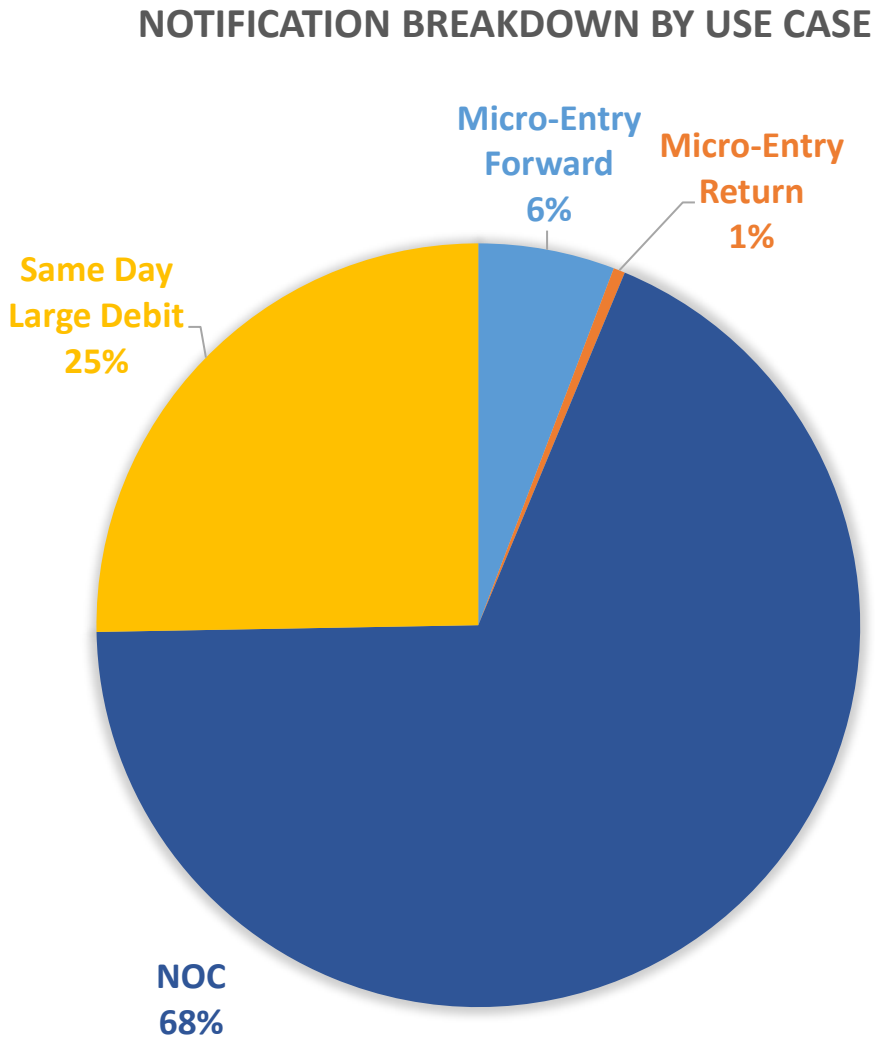
- Intended for ODFIs who receive the same NOC more than once outside of prescribed Nacha change timeframes, indicating that the Originator is not making required updates
- NOCs continue to be an industry pain point, representing between a third to a half of total violations processed by Nacha
- By making ODFIs aware that an Originator has received multiple NOCs for the same Receiver, the ODFI is able to follow up with its Originator to provide education or take appropriate action

Micro-Deposits (Forward and Return) outside of baseline

- Intended for ODFIs whose Originators use these small dollar entries for account verification and experience anomalous volumes of forward or return items, potentially indicating fraudulent activity
- A new Nacha rule for micro-entries became effective March 17, 2023; this new rule requires commercially reasonable fraud detection for micro-entry origination, including at a minimum monitoring forward and return volumes against a baseline of normal activity

FedDetect® Anomaly Notification Stats

- Over 1,350 enabled customers in first nine months since launch
- Majority of activity in the Notification of Change (NOC) use case, followed by Same-day debit large dollar variance
- Micro-Entry Forward and Return activity spikes can identify potential anomalous activity and the value of this use case is primarily Nacha compliance and fraud detection



Easy sign-up..

- There is **no additional cost** for current customers to enable FedDetect Anomaly
- Existing FedACH Subscribers may **self-enable notifications**:

Log into your FedLine Web® or FedLine Advantage® Solution

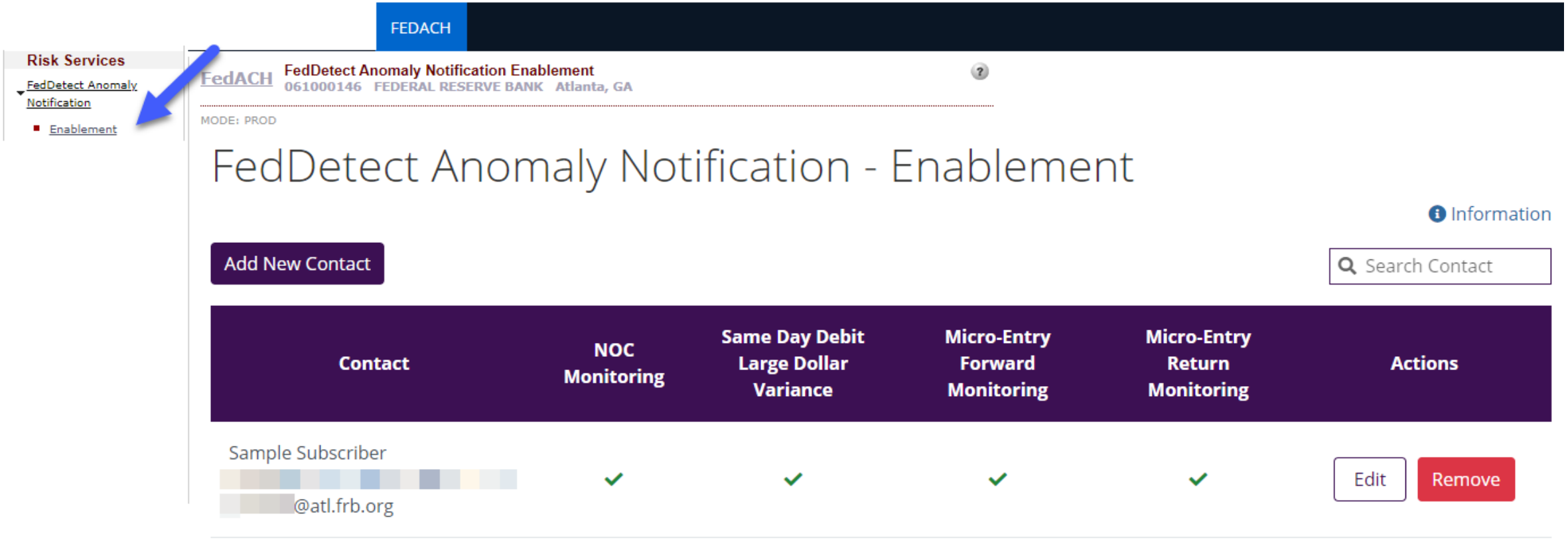
Click on the FedDetect Anomaly Notification link under the “Risk Management” heading

Add contacts and start receiving secure email notifications

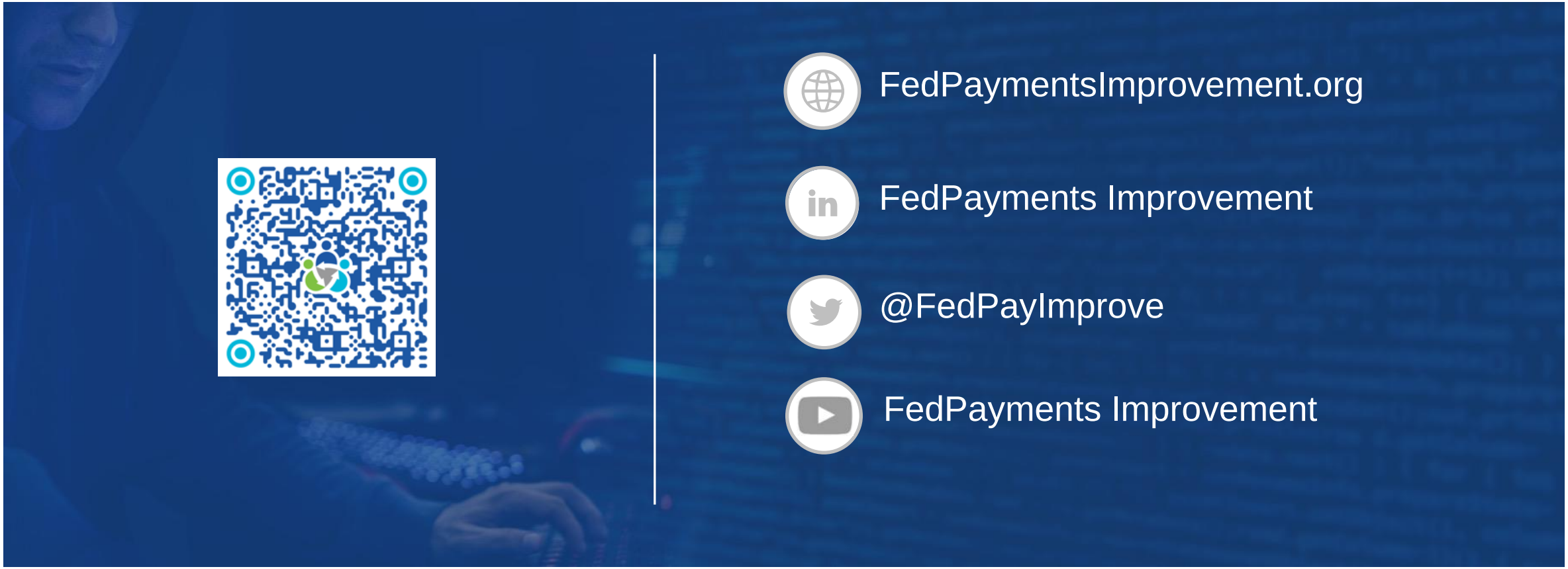
- Customers without FedACH Information Services access or that wish to sign up multiple RTNs may complete and submit Part 6H of the FedACH Participation Agreement to the Support Center to enable these RTNs

Self-service enablement in FedLine

THE FEDERAL RESERVE
FedLine® Solutions



Get Connected. Stay Engaged.



Notification of change (NOC) use case

Notifications of change

Improve your operations by monitoring when your institution receives the **same NOC more than once** outside of prescribed Nacha-designated change timeframes, indicating that an originator has failed to make updates

- NOCs continue to be an **industry pain point**, representing between a third to a half of total **violations** processed by Nacha
- By making ODFIs aware that an Originator has received multiple NOCs for the same Receiver, the ODFI is able to follow up with its Originator to **provide education or take appropriate action**

Same-day debit large dollar use case

Notifications of change

Gain insight on your Fed account when **unusual high-dollar debit batches** will settle on the current processing day in the **final same-day window** and potentially require settlement account funding

- Starting March 19, 2021, ODFIs were permitted to submit Same Day ACH files until **4:45 p.m. ET**; Nacha further increased the per-payment maximum for Same Day ACH transactions from $100,000 to $1 million effective March 18, 2022
- While these changes support innovation and accessibility to Same Day ACH, they also add **new challenges** if your institution receives late day debits
- Notifications of high dollar debits will help **provide awareness** and time to help ensure **appropriate funding action** is taken

Micro-entry forward and return use case

Monitor velocity of forward and return micro-entries for originators that use these small-dollar entries for **account verification purposes**, and potentially mitigate your institution's **fraud risk**

- Nacha rule for micro-entries became effective March 17, 2023; this **new rule requires commercially reasonable fraud detection for micro-entry origination**, including at a minimum monitoring forward and return volumes **against a baseline of normal activity**

Scams Definitions and Examples

KEY TERMS AND DEFINITIONS

Authorized Payment

A payment entered or requested by a legitimate account owner or user from the owner's account.

Unauthorized Payment

A payment entered or requested by a third party who has no legitimate right to move money from another entity's account.

SCAM CATEGORIES AND DEFINITIONS

Products or Services

A situation involving a transfer of funds in exchange for a product or service, irrespective of the nature of the relationship between the two parties, in which the receiver of the funds does not deliver the product or service or delivers a grossly inferior product or service than the one advertised or promised.

Relationship and Trust

A situation involving a transfer of funds to a trusted party, or an impostor acting as a trusted or authoritative party, where there is no expectation or promise of merchandise in exchange for the transferred funds. The seemingly trustworthy party can be an existing or emerging relationship or a party pretending to be an authority or reputable company.

SCAM TYPES DEFINITIONS AND EXAMPLES

Merchandise Scam

Purchase of merchandise that is never delivered or is substantially different from the advertised description or quality.

Scam examples: Online purchase scams, puppy and pet scams, and sales of fake sports or concert tickets, counterfeit prescription drugs or fake anti-aging remedies.

Investment Scam

An investment in a financial asset with expectation of a high return rate based on false promises.

Scam examples: Investments in fake business opportunities, fake cryptocurrency purchases or buying precious metals that do not exist.

Property Sale or Rental Scam

The purchase or rental of a home, apartment, or property that was fictitious, was not made available, or was not rightfully owned by the offering party or agent.

Scam examples: Making a down payment for a new home purchase or rental that is not for sale/rent by the real owners. Paying for a fake rental property offered online.

Scams Definitions and Examples

SCAM TYPES DEFINITIONS AND EXAMPLES

Romance Impostor Scam

The use of a fictitious online identity to establish a trusted relationship (romance or friendship) with another person with the intent to request money by using a false situation to create a sense of urgency.

Scam examples: Travel expenses requested for a visit to further the relationship, money requested for medical bills, car or home repairs, family emergencies or to access restricted funds.

Government Impostor Scam

A person poses as an employee of a government agency, law enforcement, or a trusted authority like a court representative to deceive an authorized party to make a payment or provide sensitive information often based on the potential for negative consequences like arrest, financial penalties or reputational harm.

Scam examples: IRS back taxes, arrest warrant issued, agency penalties or fines, government refund offers, Medicare/benefits coverage offers.

Bank Impostor Scam

A person poses as a legitimate financial institution, bank department or bank representative to deceive individuals or businesses into revealing confidential banking information or as a bank impostor, instructing a customer to make a payment to protect the customer's money.

Scam examples: Posing as a fraud department, bank security department or bank customer service representative to request funds be moved to a secure account, request login credentials or obtain a one-time passcode from an account holder.

Business Impostor Scam

A type of deception where an individual poses as a legitimate business, company or brand to deceive a victim into making payments or providing sensitive information.

Scam examples: Tech support, business email compromise (BEC), lottery/prizes, employment offer, utility bill payment offer, student loan forgiveness, adoption scam, advanced fee scam, fake healthcare offers, prepaid funeral expenses, CEO/treasurer impostor, mortgage/title company down payment or closing costs, fake invoice payment scam, airline/travel offer scam, shipping/delivery company scam.

Relative/Family/ Friend Scam

A person poses as a family member or someone representing a family member who contacts a relative to request money to help the family member based on a false situation or emergency.

Scam examples: Grandparent scam, fake kidnapping, fake travel issues or accidents, fake arrests.

Other Trusted Party Scam

A person poses as a specific role to engage another person to request money based on a false expectation.

Scam examples: Charity/disaster relief impostor scams, babysitter scam (posing as a potential customer).

Additional information about the connections between the ScamClassifier and FraudClassifier models is planned for publication in the third quarter of 2024.

Learn more about the ScamClassifier model at FedPaymentsImprovement.org