Fraud Definitions Work Group
Strategy and Adoption Roadmap
Fraud Definitions Work Group Overview
The Federal Reserve’s Engagement in U.S. Payment Security

Payment security landscape:
- The payments ecosystem continues to evolve from physical payments to a digital environment
- Fraud risk is increasing and continues to pose a threat to the U.S. payment system
- Payment industry collaboration and information sharing remain a challenge

Anticipated outcome:
- Payment fraud and security vulnerabilities are assessed and targeted work efforts have been identified and prioritized for action
- Industry stakeholders are collectively engaged and taking action to reduce fraud and maintain the integrity and resiliency of the U.S. payment system
- Payment fraud is consistently and accurately calculated, tracked, reported and reduced over time
- Federal Reserve payment networks, services and security practices are enhanced to help promote strong payment security
Background of the Fraud Definitions Work Effort

**Form & Engage Industry Work Group**

- Establish an industry work group, led by the Fed, to define a consistent and holistic payments fraud classification model

**Focus on ACH, Wire, and Check**

- Initial focus on ACH, wire, and check payments but extensible model for future inclusion of other payment types

**Collaborate on Adoption**

- Collaborate with industry to align on an adoption strategy that drives consistent and wide-spread use of the model and related definitions
**Role of Work Group Members**
- Promote work group efforts and content
- Socialize work group deliverables within their organizations and help promote industry adoption

**Role of the Federal Reserve**
- Lead work effort, and create and provide external communications and toolkits that can be shared with industry
- Discuss and promote work group efforts/deliverables at industry meetings and conferences

---

**Fraud Definitions Work Group**
21 cross-industry experts and stakeholders.

- **Payment & Security Consultants** (PwC, Javelin)
- **End Users** (AARP, Pepsi, U.S. Treasury)
- **Fraud Analytics, Detection, and Prevention** (SAS, Guardian Analytics, Early Warning Systems)
- **Payments Rules & Education** (NACHA)
- **Payment Processors & Operators** (FRS WPO, FRS RPO, TCH, Jack Henry, Fiserv, FIS)
- **Financial Institutions** (JPM Chase, Citizens Bank, First Century Bank, Navy Federal Credit Union, SECU of North Carolina, American National Bank & Trust)
- **End Users** (AARP, Pepsi, U.S. Treasury)

---

© 2019 Federal Reserve Banks. Materials are not to be used without consent.
Fraud Definitions Work Group Objectives

A greater understanding of payment system fraud trends is essential for mitigating risk. The Federal Reserve sees value in evolving towards a more consistent and holistic U.S. fraud perspective through a collaborative approach with industry professionals.

**WORK GROUP DELIVERABLES TO INDUSTRY**

**Fraud Classification Model for ACH, Wire, and Check Payments (Model)** that includes detailed definitions and categories that fully describe key fraud data points while enabling analysis and mapping to a higher-level categorization that helps promote a consistent understanding in the industry; and

**Industry Adoption Roadmap** to encourage broad industry adoption of its recommended Model, to include identification of additional opportunities to improve the consistency and timeliness of payments fraud data sharing and analysis.
Fraud Classification Model for Payments (Model)  
*Design Guidelines*

1. Consider existing, best-in-class and widely accepted payments fraud taxonomies in use by the industry, as well as ongoing efforts to create similar models.
2. Establish a holistic, high-level structure to classify in scope payments fraud scenarios.
3. Ability to dynamically add emerging fraud without impacting the overall architecture of the Model.
4. Enable measurement and comparison of payments fraud in a consistent manner, both in terms of breadth and depth of data, and over time.
5. Enable the collection, summarization, and analysis of payments fraud; must be inclusive of all dimensions, categories, and attributes necessary to identify unique trends and patterns and how fraud is perpetrated.
6. Allocate fraudulent transactions to only one category in the classification structure to ensure it is counted only once.
7. Available and usable to all payment system stakeholders.
Fraud Classification Model for Payments

Who initiated the payment?

Authorized Party

- How was the fraud executed?
  - Authorized Party acted fraudulently
  - How did Authorized Party act fraudulently?
    - How was Authorized Party manipulated?
      - Products & Services Fraud
      - Relationship & Trust Fraud

- Unauthorized Party modified payment info?
  - Impersonated Authorized Party
  - Compromised Credentials
  - Physical Alteration

Unauthorized Party

- How was the fraud executed?
  - Unauthorized Party took over account
  - How did Unauthorized Party take over account?
    - Impersonated Authorized Party
    - Compromised Credentials

- Unauthorized Party misused account info/instrument
  - How was acct info/instrument misused?
    - Digital Payment
    - Physical Forgery/Counterfeit

DRAFT
Section 1: Payment Initiation

Who initiated the payment?

Definitions:

Authorized Party
An individual or entity with the right to initiate the payment

Unauthorized Party
An individual or entity without the right to initiate the payment
Section 2: Fraud Method

**How was the fraud executed?**

- **Authorized Party was manipulated**
  - Authorized Party is deceived or coerced to initiate a payment

- **Authorized Party acted fraudulently**
  - Authorized Party initiated the payment with intent to defraud

- **Unauthorized Party modified payment information**
  - Unauthorized Party modified the payment information and/or payment instructions (including forged endorsement) without the knowledge of the payment initiator

- **Unauthorized Party took over account**
  - Unauthorized Party gains control of the account, which includes the ability to manage or change account information, and initiate payments without the knowledge of an Authorized Party

- **Unauthorized Party misused account info/payment instrument**
  - Unauthorized Party does not have control of the account, but obtains a payment instrument or enough account information to initiate a payment without the knowledge of an Authorized Party
Fraud Classification Model for Payments

Who initiated the payment?

- Authorized Party
- Unauthorized Party

How was the fraud executed?

- Authorized Party
- Unauthorized Party

How was the fraud executed?

- Authorized Party acted fraudulently
- Unauthorized Party modified payment information

How was Authorized Party manipulated?

- Authorized Party was manipulated

How did Authorized Party act fraudulently?

- How did Authorized Party act fraudulently?

How did Unauthorized Party modify payment info?

- How did Unauthorized Party modify payment info?

How did Unauthorized Party take over account?

- How did Unauthorized Party take over account?

How was acct info/instrument misused?

- How was acct info/instrument misused?

Products & Services Fraud
- Embezzlement
- False Claim
- Synthetic ID

Relationship & Trust Fraud
- Impersonated Authorized Party
- Compromised Credentials
- Physical Alteration

Digital Payment
- Physical Forgery/Counterfeit

DRAFT
**Section 3: Fraud Tactic**

- **Products & Services Fraud**: A situation involving a transfer of funds in exchange for a product or service, whereby the receiver of the funds does not deliver the product or service, or delivers a grossly inferior product or service than advertised or promised.

- **Relationship & Trust Fraud**: A situation involving a transfer of funds to a trusted party, or an imposter acting as a trusted or authoritative party, where there is no expectation or promise of goods or services 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.

- **Embezzlement**: Theft or misuse of funds legally placed in one’s trust or belonging to one’s employer.

- **False Claim**: An intentional lie or deception in order to receive a payment or avoid a payment obligation.

- **Synthetic ID**: A crime in which perpetrators combine real and/or fictitious identifying information, such as Social Security Numbers (SSN) and names, to create new identities with which they defraud financial institutions, government agencies, or individuals.

- **Impersonated Authorized Party**: A person/organization who does not have authorized credentials, but has enough information to authenticate as the Authorized Party.

- **Compromised Credentials**: Account login information (e.g. ID/password), intended only for Authorized Party, is obtained by an Unauthorized Party.

- **Physical Alteration**: The act of tampering with a physical payment instrument (to include forged endorsement).
Section 3: Fraud Tactic (cont.)

How did Unauthorized Party take over account?
- Impersonated Authorized Party: A person/organization who does not have authorized credentials, but has enough information to authenticate as the Authorized Party.
- Compromised Credentials: Account login information (e.g. ID/password), intended only for Authorized Party, is obtained by an Unauthorized Party.

How was acct info/instrument misused?
- Digital Payment: Account information, intended only for Authorized Party, is used by an Unauthorized Party to initiate an electronic payment.
- Physical Forgery/Counterfeit: An imitation of a legitimate, physical payment instrument is used to initiate a payment.
Industry Adoption of the
Fraud Classification Model for Payments

End-State Goal and Potential Benefits

Achieve widespread industry adoption and consistent use of a fully-populated Fraud Classification Model for Payments and related definitions, resulting in **improved data quality, timeliness, and fraud mitigation effectiveness.**

- **Improved Fraud Data Quality**
- **Timely Fraud Information Sharing**
- **Effective Predictability and Prevention**
- **Faster Access to Fraud Information**
- **Proactive Communication**
- **Reduced Losses via Cross-Industry Collaboration**
- **Analytics Capability via Consistent & Timely Data**
Full adoption of the Model for ACH, wire, and check

- Model and supporting definitions are the industry standard lexicon for dialogue on fraud and related trends
- All fraud events (attempted and successful) are classified and reported according to the Model
- Intake, classification, analysis, and trending of fraud events occurs in a coordinated and timely manner, which promotes improved fraud detection, mitigation, and prevention
- Industry participants are actively using data and sharing insights across the industry to better understand fraud holistically across the ecosystem

Incorporation of Model into Industry Dialogue and Studies

- Industry uses Model classifications and definitions when describing fraud trends at fraud conferences, in surveys and white papers, etc.
- Payments studies leverage the Model to not only collect data, but also to articulate both emerging and realized trends across the industry

Integration of Model into Operational Processes

- Frontline fraud intake functions (e.g., call centers, customer support, etc.) are classifying all newly reported fraud according to Model
- Fraud investigation teams are leveraging Model to provide additional context and insight to reported fraud events
- Better data produces the ability for fraud rules to be more quickly and dynamically adjusted in response to a changing fraud environment
- More responsive business strategy and risk decisions based on timelier, improved data

Integration of Model into Technology Projects, Products, etc.

- New and existing products incorporate Model and supporting definitions to:
  - Facilitate and simplify the intake and classification of fraud events
  - Automate fraud trending and analysis through machine learning/AI
  - Generate synthesized data/reporting
- Data aggregated across industry through technological mechanisms (e.g. APIs) to advance ability to compare and synthesize fraud data in a more real-time fashion
- Timely anomaly detection and implementation of responsive, dynamic authentication through machine learning/AI and APIs
Industry Adoption Roadmap

Roadmap Overview

**CRAWL**
Within an organization, classify fraud activity according to the Model with at least one payment type, for at least a subset of the organization’s fraud data.

**WALK**
Within an organization, classify all fraud activity according to the Model for ACH, wire, and check with the ability to analyze and present findings externally on an ad hoc basis.

**RUN**
Across the industry, classify all fraud activity for ACH, wire, and check according to the Model and share this fraud information on a recurring basis in an automated manner, enabling improved industry analysis and mitigation.

**Coordination and Oversight**
Establish approach for planning and executing the adoption efforts (to include Model maintenance)

**Communication, Socialization, and Driving Adoption**
Educating the industry on the Model and influencing adoption

**Fraud Information Sharing and Analysis**
Determine how to best share, analyze, and act on fraud information classified by the Model across the industry
AI/ML Section
FRAUD AI/ML

FEEDZAI GENOME

VISUALIZING COMPLEX FINANCIAL CRIME SCHEMES
Visualizing Fraud with Data Science

Financial case across markets which went undetected where organized criminal money shops across seas were giving local currency in exchange for digital payments in "fake" online shops in euros.

Timelapse evidence of a repetitive pattern in transactions and load balancing across the multiple merchants with changing IPs to avoid detection.
FRAUD AI/ML

Feedzai Genome: Powered by AI

For alert reviewers
Integrate & Extend your alert system

For investigators and data scientists
Explore & find hidden connections
FRAUD AI/ML
Benefits of UDML
Low vs. high-order decision making
User Defined Machine Learning
AI automates the simple stuff
Frees up humans to focus on the important stuff
And it works really well!
(Proven 80% efficacy)
Synthetic Identity Fraud

Synthetics Loans
Create realistic profiles by combining real + fake data
“Bust out” fraud
Write-offs 4–5x higher

AML / BSA – National Security
Fake loans washed and moved
Shell Persons for organized crime / terror transactions
Credit card purchases made to look legitimate (airline / hotel / supplies)

Source: Federal Reserve Bank of Boston Whitepaper (July 2019)
Congressional Engagement

**Senate Banking Committee**
Combating Money Laundering and Other Forms of Illicit Finance (Nov’18)
Draft ILLICIT CASH Act

**House Financial Services Committee**
AI Think Tank letter
FinCEN Modernization Meeting (June’19)
Boston FinTech Week and AI Think Tank

Sign up for updates: info@coalesce.ai / www.coalesce.ai
Approach to Stakeholder Engagement
FedPayments Improvement (FPI) Community
All ~7,000 Subscribers

FPI Fraud Definitions Community Interest Group
Subset of FPI Community members interested in the fraud definitions topic (~1,100)

Fraud Definitions Industry Work Group
Small, nimble working group of industry leaders with specific industry expertise
FedPayments Improvement
Fraud Definitions Community Interest Group

This group will have the opportunity to:

- Participate in input and feedback opportunities throughout the work group effort
- Obtain regular updates on work group progress
- Meet with Fed SMEs and/or work group members

Join the Fraud Definitions Community Interest Group by submitting or updating your FedPayments Improvement Community profile and selecting “ACH, Wire and Check Fraud Definitions” as a topic of interest.
Stay Engaged!

To learn more about the Fraud Definitions Work Group:

Visit FedPaymentsImprovement.org

Follow FedPayments Improvement social media channels:

FedPayments Improvement

FedPayImprove

Email us at FedPaymentsImprovement.org