US Faster Payments Council

FPC FALL MEMBER MEETING 2026



US Faster Payments Council

Fraud & Sanctions at the Speed of Money

Managing Financial Crime Risk in Real-Time Payments

As payments move in seconds, fraud and sanctions decisions must move just as fast. The challenge is shared, effective controls across the ecosystem without adding unnecessary customer friction

US Faster Payments Council

Fraud & Sanctions at the Speed of Money



Laura Sullivan

Senior Director - Product Management

CSI



Jamie Florio

Dir, Account Executive

Fincom



Gursharan Singh

Product Manager

Form3

US Faster Payments Council



https://cvent.me/YINwzy

FPC FALL MEMBER MEETING 2026

Instant Payment Fraud Statistics

85% of US payment professionals expect fraud to increase as instant payments scale

According to the Association for Financial Professionals, **63%** of firms experienced check fraud in 2024, compared with just 2% reporting incidents on RTP or FedNow

35 million RTP transactions in April 2025, **only 123 were fraudulent**—a fraction of a percentage point

96% of banks back the introduction of Confirmation of Payee-style identity verification checks, which have cut APP fraud in the United Kingdom by more than half

Instant Payment Fraud Characteristics

Instant payment fraud types

- Authorized Push Payment scams
- Account takeover and credential abuse
- Mule networks and rapid cash-out

Take advantage of three structural properties of instant rails

- Speed
- Finality
- Push-based authorization

Controls should operate before release due to

- No built-in chargeback mechanism
- No standardized dispute window
- Very limited scope for clawbacks



Instant Payment Fraud Focus Areas*

- **Customer and behavioral signals:** Baselines for typical amounts, frequency, counterparties, and timing, plus behavioral biometrics such as typing and navigation patterns
- **Device and session intelligence:** Device fingerprinting, IP and geolocation checks, VPN and emulator detection, and “impossible travel” controls across sessions
- **Transaction analytics and velocity monitoring:** Rules and models that look for spikes in value, new-recipient payments, or rapid-fire transfers across multiple accounts
- **Payee and network intelligence:** Risk scores for beneficiaries based on account age, past activity, consortium watchlists, and graph analysis of fund flows

*Source Branch report 6/4/26 **RTP Fraud Prevention: Best Practices for Real-Time Payments**

Financial crime controls are becoming a board-level obligation

Recent enforcement: weak monitoring and slow action have real consequences

US | Bank of America

$750m OCC penalty (Oct 2026) for BSA/AML program deficiencies, including longstanding control weaknesses.

UK | Nationwide

£44.1m FCA fine (Dec 2025). FCA said weak controls missed red flags, including £27.3m of fraudulent furlough payments into one customer's accounts.

Europe | ABN AMRO

€8.5m DNB fine (Jul 2026) for structural shortcomings in ongoing monitoring of higher-risk customers and transactions.

Takeaway

The expectation is shifting from "*have a control*" to "*prove the control works and triggers action*."

These examples are broader financial-crime / AML enforcement. Not all are payment-fraud cases, but the supervisory lesson is directly relevant to real-time payments.

UK APP fraud: responsibility now sits on both sides of the payment

Mandatory reimbursement changed the incentive model

VICTIM →

Sending PSP

Customer warnings • behavioral / transaction controls • reimbursement obligation

50 / 50
cost share

Receiving PSP

Mule-account detection • inbound monitoring • account intervention • 50% reimbursement contribution

→ FRAUDSTER

Why this matters for instant payments

Fraud prevention cannot stop at the sender. The receiving institution has unique context about the beneficiary account, and now a direct financial incentive to act on them.

UK Faster Payments reimbursement protections took effect 7 Oct 2024; in-scope APP fraud reimbursement cost is shared 50:50 between sending and receiving PSPs.

Nacha 2026: ACH fraud monitoring becomes a network-wide responsibility

The US is moving in the same direction. Receiving FI's are expected to detect credit-push fraud



New rule principle

Establish and implement risk-based processes and procedures reasonably intended to identify ACH entries suspected of being unauthorized or authorized under "False Pretenses."

Phase 1 • Mar 20, 2026

All ODFIs + larger Originators/TPSPs/TPSs; RDFIs receiving ≥10m ACH entries (2023 volume).

Phase 2 • Jun 19 / practical Jun 22, 2026

Extends requirements to all remaining non-consumer Originators/TPSPs/TPSs and all remaining RDFIs.

US Faster Payments Council

What Nacha expects: risk-based monitoring on both outbound and inbound ACH credits

Originating side | prevent fraudulent initiation

ODFI, non-consumer Originators, TPSPs and TPSs

- Identify unauthorized entries and entries induced by false pretenses
- Controls should reflect the role each party plays
- Review processes at least annually
- No prescribed technology—and not every entry must be screened individually

Receiving side | detect suspicious credits

RDFIs

- Monitor incoming ACH credits using account + transaction context
- Potential signals: velocity, anomalies, account age, average balance
- Define handling for suspicious credits
- May return an entry or contact the ODFI to validate it

Important nuance

Nacha does not mandate pre-processing screening but explicitly notes that monitoring before processing provides the greatest opportunity to prevent fraud.

The emerging model: shared responsibility + controls that move at payment speed

A practical control framework across ACH, FedNow and RTP

1	2	3	4	5
KNOW	**DETECT**	**DECIDE**	**ACT**	**LEARN**
Customer / account risk context	Behavior • velocity account anomalies	Fraud • sanctions limits • policy	Allow • reject review / intervene	Outcomes • returns recovery • tuning

The key design principle

Do not slow real-time payments to make them safer. Make the risk decision fast enough and share enough intelligence that the payment can remain real-time.

UK APP reimbursement and Nacha's 2026 rules both point toward the same outcome: fraud risk is increasingly a shared ecosystem responsibility, not just a sender problem.

Sanction Screening – Who, what and when?

Who

- Customers and members
- Counterparties
- Financial institutions

What

- Names and identifiers
- Locations and addresses
- Relevant payment details, including free text

When

- Onboarding
- Ongoing review
- Payment processing

Takeaway

Set coverage from risk assessment, not current system limitations

Where does customer/member screening provide coverage, and what else in the payment introduces risk?



Screening Quality Determines the Workload

Recognize meaningful variations

- Phonetic matches, spelling abbreviations, and transliteration
- Different scripts and languages

Use context to resolve ambiguity

- Consider available identifiers
- Distinguish similar names
- Preserve evidence for the decision

Improve Tech for Improves STP

- Tune to effectiveness, not STP rate
- Suppression should be consistent and provable

Objectives

Evaluate detection effectiveness *and* STP rates together.
We don't have to accept high alerts rates based on old technology.

Are we improving results and STP rates, or simply turning out alerts? Is AI augmenting or deciding?



An Alert Still Needs a Decision

1

Potential match

Identify the concern

2

Evaluate context

Review all payments fields, customer data and matched record data and context.

3

Decide

Clear or escalate

4

Act and record

Apply the defined response

Auditable, Documented Processes

Define the handling for resolving alerts before they occur, creating an auditable, consistent process.

What justifies reusing yesterday's decision? Are whitelists sanitized? What should trigger a fresh review?

Expect More From Vendors and Technology

Define the required outcomes

Risk tolerance, detection, speed, and customer impact
Alert rates without miss-hits

Challenge your vendors

Require evidence and an auditable decision
Accountability for results and improvements

Test results

Matching, alerts, list changes, vessels and free text
Outages and escalation

What we Should Expect

Your risk tolerance should drive technology results, not the other way around.

Don’t’ water down your process to meet the limitations of the technology.

Are we accepting “that’s how the It’s always worked”?

