US Faster Payments Council

Instant Payments Fraud Dispute Resolution: Guiding Principles for the U.S.

Fasterpaymentscouncil.org

May 2026

Instant Payments Fraud Dispute Resolution: Guiding Principles for the U.S.

In the U.S., reported fraud and scam losses have been rising in recent years.[1] This trend is occurring alongside the continued expansion of instant account-to-account payments across payment rails. The irrevocable[2] nature of these rails creates challenges for dispute resolution, and lack of clarity about dispute resolution can affect user confidence and adoption.

The principles outlined in this report offer industry guidance on designing dispute resolution frameworks for both consumers and businesses.

Purpose

This report proposes *a set of principles* for handling disputes in instant payments. The goal is to strengthen consumer and business confidence by outlining dispute-related components that could encourage broader adoption and pointing out which ecosystem participants may be best positioned to mitigate fraud. *These principles are meant to be directional — not prescriptive — to support flexibility across institutions and use cases.*

As a set of *principles*, it does not include specific use cases, codes, or scam categories.

Context: Why Dispute Capabilities Matter

Instant payments are credit-push and irrevocable. These characteristics support many valuable use cases but limit the types of recourse familiar from credit cards and other payment channels. Unauthorized fraud is addressed in the RTP® Network and the FedNow® Service rules, including application of Reg E where a consumer is involved. Fraudulently induced authorized payments fall into regulatory gaps, and dispute handling across providers varies widely. Consumers expect predictable dispute paths, and businesses require operational clarity. These dynamics can create uncertainty that impacts broader use-case adoption.

Key challenges include:

- Reputational and financial risk created by Authorized Push Payment[3] (APP) scams.
- Ad hoc and/or inconsistent approaches across instant payment providers as opposed to a common approach.[4]

Scope and Assumptions

This set of principles is limited to fraud-related disputes in instant payments (RTP Network and FedNow Service). They apply to account-to-account credit-push transfers and recognize that these rails are not interoperable today. Key assumptions underpinning the principles include:

- A focus on fraud-related disputes, such as:
    - Unauthorized fraud (e.g., resulting from account takeover)
    - Authorized but fraudulently induced payments (APP scams)
    - First-party fraud
    - Request-for-Payment (RfP) fraud
- Use of the Federal Reserve ScamClassifier® and Fraud Classifier® models to support consistent categorization.
- Acknowledgment that Reg E and UCC 4A differ significantly in coverage and expectations; and
- Incorporation of ISO 20022 messaging capabilities, where appropriate, including:
    - camt.056 (request for cancellation/return)
    - camt.029 (response to investigation)
    - pain.013/pain.014 (payment status/return requests)
    - pacs.004 (payment returns)

    These messages provide structured ways to exchange information, reason codes, timestamps, and dispute-related metadata.

What Consumers and Businesses Expect

The work group recognizes that consumers and businesses expect simple and predictable dispute paths that mirror the ease and clarity of more familiar payment methods. They need to understand what is covered, how to seek help, when to expect a response, and what instant protections are in place to reduce scam exposure. Effective dispute handling must:

- Work even when the sending and receiving institutions differ in capabilities
- Support practical recourse options for both consumers and businesses

Guiding Principles for Instant Payment Dispute Resolution

The principles are outlined below, followed by brief explanations.

1. Recognize All Parties Have Important Roles in Mitigating Fraud and Scams
2. Focus on the Party Best Positioned to Mitigate Fraud, Dependent on Use Case
3. Preserve the Integrity of Instant Payment Design
4. Establish Structured Dispute Resolution Workflows
5. Provide Instant Fraud Mitigation and User Awareness
6. Define Core Responsibilities for Sending Institutions
7. Define Core Responsibilities for Receiving Institutions
8. Set Clear Expectations for Merchants and Processors

9. Support Small Businesses and Vulnerable Consumers
10. Promote Transparency and ISO 20022-Aligned Exchange of Information
11. Apply Practical Lessons from Global and Domestic Precedents

Principle 1. Recognize that All Parties Have Important Roles in Mitigating Fraud and Scams

All parties involved in payments, including sending and receiving financial institutions, merchants and billers, networks and payments system operators, regulators and legislators, and payment initiators and recipients—can help mitigate fraud and scams to varying degrees, and should take appropriate responsibility for relevant roles. Each party's level of involvement depends on its capabilities and the use case.

Principle 2. Focus on the Party Best Positioned to Mitigate Fraud

While all parties should have responsibilities for mitigating fraud, the participants best equipped for mitigating fraud possess authentication and behavioral insight, onboarding and monitoring obligations, visibility into transaction and device patterns, and the ability to detect anomalies instantly. These capabilities can differ not only by party, but also by use case. Designing dispute handling around capabilities, and encouraging parties to share data, keeps the focus on mitigation rather than liability.

Principle 3. Preserve the Integrity of Instant Payment Design

Instant payments must retain their core characteristics of speed and irrevocability. Within that constraint, dispute processes should:

- Maintain irrevocability and settlement certainty
- Support post-transaction recourse without undermining system speed
- Use risk-based delays or confirmation prompts only when justified by fraud detection/mitigation

Principle 4. Establish Structured Dispute Resolution Workflows

Dispute resolution routing should be based on fraud/scam classification and available evidence, aligning with network rules and how institutions can most efficiently respond. The dispute resolution workflow should also capture and report suspected fraud claims at the time they are initiated, even before final adjudication, so that these signals can inform broader ecosystem awareness of potentially high-risk receiving accounts.

- Expedited Path: For clear, well-documented cases or small-value claims.
- Full Investigation Path: For high-value, ambiguous, or recurring disputes.

Principle 5. Provide Instant Fraud Mitigation and User Awareness

Pre-transaction fraud detection/mitigation features reduce the volume of fraud or scams schemes before they reach the payment rail. Some examples of these features include:

- First-time payee warnings
- Confirmation of payee
- Behavioral risk prompts
- Alerts for high-risk or unusual patterns
- Trusted-contact or elder-protection mechanisms
- Subscription visibility and easy cancellation in RfP contexts

Principle 6. Define Core Responsibilities for Sending Institutions

Sending institutions typically possess the strongest view into user authentication history and device and behavioral biometrics, e.g., account access patterns, sender payment patterns, and communications with sender. They are therefore well-positioned to:

- Potentially slow, question, impose limits on, or reject a payment request if fraud is suspected[5]
- Promptly report fraud claims to the payment network or other central database repository
- Classify the dispute using standard fraud and/or scam taxonomy
- Route disputes into expedited or full pathways based on factors such as transaction value, scam indicators, and complexity (straightforward or well-documented cases may be managed through an expedited process, based on cost-benefit analysis and institutional risk tolerance)
- Share structured evidence with receiving institutions
- Support customers through resolution and education

Principle 7. Define Core Responsibilities for Receiving Institutions

Receiving institutions have visibility into:

- Account opening, identity verification, and KYB/KYC for accounts potentially receiving fraudulent funds
- Inbound payment velocity and other payment patterns
- Potential mule or synthetic indicators

They are therefore well-positioned for:

- Monitoring and risk detection
    - Monitor Requests for Payment (RfP) by its customers and take steps to prevent fraudulent RfPs
    - Evaluate inbound/outbound account risk signals, and, as appropriate, take action indicated by that evaluation, including slowing/halting payment activity to receiving accounts
- Operational response to suspected fraud
    - Take action based on risk evaluation, including slowing or halting payment activity to receiving account
    - Freeze or return funds[6] when contractually and legally supported
- Dispute resolution and information sharing
    - Respond within agreed-upon timelines using ISO 20022-based messaging
    - Share relevant metadata for investigation
    - Incorporate reporting of suspected fraud claims into the dispute resolution process so that claims, whether ultimately confirmed or not, contribute to shared signals about potentially high-risk receiving accounts
- Account lifecycle management
    - Incorporate receiver account data and analysis into improved KYC/KYB
    - Take steps to close accounts or prevent re-onboarding when an account holder is confirmed to have engaged in fraud, with appropriate investigation and recourse mechanisms[7]

Principle 8. Set Clear Expectations for Merchants and Processors

For consumer-to-business instant payments, dispute frameworks should clearly define the information, transparency, and cooperation expected from merchants and processors when resolving fraud-related disputes, which may differ between purchase and bill-pay transactions. These expectations support dispute evaluation without assigning fraud detection or monitoring responsibilities to merchants[1]. Key expectations include:

- Clear refund and cancellation paths for goods or services
- Review of delivery, fulfillment, and transaction metadata that support dispute evaluation
- Transparent subscription and recurring-payment practices
- Responsiveness to dispute-related inquiries from the sending or receiving institution

Principle 9. Support Small Businesses and Vulnerable Consumers

Develop and Promote:

- Plain-language dispute initiation
- Reduced documentation burden for simple cases
- Mobile-first and accessible design
- Processes that do not require legal sophistication or extensive back-office resources

Principle 10. Promote Transparency and ISO 20022-Aligned Exchange of Information

Standardized dispute-relevant data exchange should use ISO 20022 messages such as:

- camt.056 for initiating a return or cancellation request
- camt.029 for structured responses
- pain.013 request for payment
- pain.014 payment status request
- pacs.004 payment returns

These messages enable consistent reason codes, timelines, evidence packaging, and audit trails. This supports predictable communication between sending and receiving institutions without requiring rail-to-rail interoperability.

Principle 11. Apply Practical Lessons from Global and Domestic Precedents

- **UK CRM Code**[9] and subsequent **PSR reimbursement framework**[10] provide an example of clear, consistent dispute processes, expectations, and outcomes in APP fraud.
- **Brazil Pix**[11] illustrates how network-defined obligations for responding institutions and timely responses to dispute-related inquiries can improve both customer confidence and fraud mitigation. Pix also highlights the importance of enhanced mule-account detection through analytics that evaluate unusual account behavior, velocity, and onboarding patterns.
- **Nacha 2026 Credit-Push Enhancements**[12] show how standardized fund-freeze protocols, clear obligations for receiving institutions to act on red flags and required fraud-reporting mechanisms can strengthen dispute resolution for push payments. These enhancements demonstrate how structured responsibilities and consistent follow-up expectations can reduce fraud losses and support recovery.
- **Credit Card Networks**[13] provide examples of consistent evidence templates, predictable timelines, and early-resolution processes that reduce friction for straightforward cases. These elements are useful structural models for instant payments, not as analogies to debit-card protections under Reg E, but as examples of how predictable workflows and documentation

- Zelle's[14] publicly described practices emphasize pre-transaction use of network receiver statistics for fraud decisioning, fraud-awareness prompts, risk-based transaction controls, and efforts to return funds when they remain available. These elements offer insight into consumer-facing measures and operational behaviors that can reduce fraud exposure without relying on unpublished or proprietary rulebook details.

Summary

The principles outlined in this report offer a framework for strengthening trust, reducing fraud exposure, and ensuring consistent dispute handling across the U.S. instant-payments ecosystem. By combining clear responsibilities, structured workflows, and enhanced fraud-mitigation capabilities, these principles aim to support safe adoption of instant payments for both consumers and businesses.

Key elements include:

- Clear, consistent principles defined by fraud category
- Defined mitigation responsibilities across participants
- Instant fraud detection/prevention features before payments reach the rail
- Tiered, predictable resolution pathways
- Transparent communication supported by ISO 20022 message structures
- Industry-defined obligations for sending and receiving institutions
- Practical merchant participation in commerce-related disputes.
- Approaches proven in other markets and domestic rails that can be adapted to U.S. needs

This set of principles provides a foundation for designing dispute processes that strengthen trust, protect consumers, and support broader adoption of instant payments.

Acknowledgements

Thank you to the members of the FPC Fraud and Scam Mitigation for Faster Payments Work Group (FSWG) who contributed to this report.

FSWG Leadership

PayGility Advisors, LLC	Lee Kyriacou, Work Group Chair
JPMorgan Chase	Shelley Rojano, Work Group Vice Chair

FSWG Report Subgroup Members

PayGility Advisors, LLC	Deborah Baxley, Co-Lead
PayGility Advisors, LLC	David True, Co-Lead
Corporate One	Beckie Nourse
National Consumer Law Center	Carla Sanchez-Adams
NEACH	Kathleen Shea
UMACHA	Kimberly Stachak

FSWG Members

1st Source Bank	Dana Giszewski
ACI Worldwide	Marc Trepanier
Alloya Corporate FCU	Theresa Bruckner
American Bankers Association	Paul Benda
BetterBuyDesign	Steve Mott
Commerce Bank	Chris Garcia
Ebryx	Christopher Kelly
FNBB	Jessica Johnson
FNBB	Leah McDonald
Guidehouse	Erik Prvitt
Jack Henry & Associates	Rene Perez
JJ4Tech	Caroline Cypriano
Lumin Digital	Ashley Weinke
Mastercard International	Stephen Keefe
Nasdaq Verafin	Liam Cooney
National Consumer Law Center	Cathy Mansfield
Plaid, Inc.	Will McDowell
The Banker's Bank – OK	Malinda Rickel
The Clearing House	Lokesh Dani
ValidiFI	David Barber
Visa	Elena Litani
Visa	Esha Deshpande
Wespay	Chris Selmi
Zumigo, Inc.	Nicole Sedita

About the Fraud and Scam Mitigation for Faster Payments Work Group

The FPC Fraud and Scam Mitigation for Faster Payments Work Group focuses on collectively addressing fraud and scam issues involving faster payments, which can affect fundamental trust in faster payment systems and require heightened or different operational controls, risk management, and end-user education.

About the U.S. Faster Payments Council

The U.S. Faster Payments Council (FPC) is an industry-led membership organization whose vision is a world-class payment system where Americans can safely and securely pay anyone, anywhere, at any time and with near-immediate funds availability. By design, the FPC encourages a diverse range of perspectives and is open to all stakeholders in the U.S. payment system. Guided by principles of fairness, inclusiveness, flexibility and transparency, the FPC uses collaborative, problem-solving approaches to resolve the issues that are inhibiting broad faster payments adoption in this country.

References

[1] Federal Trade Commission. (2025, March). *New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024*. https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024.

[2] Per the U.S. Faster Payments Council, an irrevocable payment is one that is final and typically has no recourse for correction or reversal. Retrieved May 12, 2026, from https://fasterpaymentscouncil.org/Glossary-of-Terms.

[3] Per U.S Faster Payments Council, When fraudsters deceive consumers or individuals at a business to send them a payment under false pretenses to a financial institution account controlled by the fraudster. Typically involves social engineering attacks and scams which may include false assertions of need or promises of benefit. Retrieved May 12, 2026, from https://fasterpaymentscouncil.org/Glossary-of-Terms.

[4] Per the U.S. Faster Payments Council, an electronic payment solution available 24x7x365, resulting in the immediate interbank clearing of the transaction and crediting of the payee's account with confirmation to the payer within seconds of payment initiation. Retrieved May 12, 2026, from https://fasterpaymentscouncil.org/Glossary-of-Terms.

[5] If a sending institution rejects a payment due to suspected fraud, the sending institution should have policies and procedures in place to respond to any subsequent dispute by the sender as to why the payment was rejected.

[6] If a receiving institution freezes or returns funds due to suspected fraud, the receiving institution should have policies and procedures in place to address any subsequent dispute from a recipient that the funds were frozen or returned in error and/or were not fraudulently sent.

[7] Account closure or restrictions should follow appropriate investigation and internal review. Institutions should maintain processes that allow account holders to challenge or appeal determinations where no fraud occurred, recognizing the risk of unintended financial exclusion.

[8] When a merchant account is itself suspected of fraudulent activity, responsibility for detection, monitoring, and enforcement rests with the receiving institution, platform provider, and applicable network rules governing merchant onboarding and lifecycle management.

[9] Payment Systems Regulator. (n.d.). *The Contingent Reimbursement Model (CRM) Code*. Retrieved May 12, 2026, from https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024.

[10] The UK Contingent Reimbursement Model (CRM) Code was an industry-led framework for APP scam reimbursement that has since been superseded by the Payment Systems Regulator's mandatory reimbursement requirements. Payment Systems Regulator. (May 2025). *APP scams reimbursement – consolidated policy statement*. https://www.psr.org.uk/media/rhelv4op/ps25-5-app-scams-reimbursement-consolidated-policy-statement-may-2025.pdf.

[11] Banco Central Do Brasil. (2024, May). *Pix Frequently Asked Questions: What is the Special Return Mechanism (MED) and how does it work?* https://www.bcb.gov.br/en/financialstability/pixfaqen.

[12] Nacha. (2026, March 20). *Nacha Operating Rules: RISK MANAGEMENT TOPICS – (Fraud Monitoring Phase 1)*. https://www.nacha.org/rules/risk-management-topics-fraud-monitoring-phase-1.

[13] Visa. (n.d.). *Resolve disputes quickly*. Retrieved May 12, 2026, from https://usa.visa.com/support/small-business/dispute-resolution.html; and Mastercard. (n.d.). *Dispute Resolution Cycle*. Retrieved May 12, 2026, from https://developer.mastercard.com/mastercom/documentation/getting-started/.

[14] Wells Fargo. (n.d.). *Zelle® Questions*. Retrieved May 12, 2026, from https://www.wellsfargo.com/help/online-banking/zelle-faqs/; and First Entertainment Credit Union. (2025, October 10). *How to Cancel or Dispute a Zelle Payment*. https://www.firstent.org/blog/how-to-cancel-or-dispute-a-zelle-payment/.