



Operational Considerations for Non-Value Messages

Table of Contents

Section 1: Introduction	4
Section 2: Overview of Non-Value Instant Payment Messages	5
2.1. Overview of Non-Value Instant Payment Messages	5
2.2. Definition and Importance of Non-Value Instant Payment Messages of Financial Institutions	5
2.3. Types of Non-Value Messages	5
2.4. System Support: RTP vs. FedNow Differences	6
2.5. Comparison Chart and Uses	6
Section 3: Request for Payment	8
3.1. Business Opportunities for Financial Institutions	8
3.2. Operational Flow	9
3.3. Technology Integration	10
3.4. Compliance and Regulatory Requirements	11
3.5. Risk and Fraud Management	12
3.6. Servicing and Operational Readiness	14
3.7. Launch Readiness and Continuous Improvement	15
Section 4: Request for Return of Funds	16
Section 5: Other Non-Value Messages	21
5.1. Operational Considerations for Request for Information (RFI) – U.S. Instant Payments (RTP and the FedNow Service)	21
5.1.1. Operational Readiness for Timely Responses	22
5.2. Recordkeeping and Compliance Considerations	23
5.3. Operational Flow of RFI Messages	24
5.4. Compliance and Network Rule Requirements	24
5.5. Exception Handling Workflows and Business Value	25
5.6. Remittance Messages	26
5.7. Administrative System Messages	29
5.8. Retrieval, Reporting, and Investigation Messages	32

Section 6: Fraud, Risk, and Security for Financial Institutions as it applies in the Non-Value space ... 34

6.1. Fraud Scenarios Unique to Non-Value Messages..... 34

6.2. Authentication and Authorization of Senders 34

6.3. Monitoring and Anomaly Detection..... 35

6.4. FI Fraud Team Readiness..... 35

6.5. Summary 36

Section 7: Compliance & Rules Framework (in Non-Value space) 36

Section 8: Technology and Processing Considerations for ISO 20022 Non-Value Messages 42

8.1. Overview 42

8.2. Implementation Models: Core Direct vs. Payment Hub..... 42

8.3. ISO 20022 Message Schema Requirements..... 44

8.4. System Integration Best Practices..... 44

8.5. Performance, Uptime, and Latency 45

8.6. Vendor and Third-Party Dependencies..... 45

Section 9: Conclusion 46

Acknowledgements 47

References 48

This document provides best practices and considerations for financial institutions. The content is not intended to be exhaustive, and each institution should consult with its own legal, compliance, and other relevant professionals regarding implementation. The information presented is current as of the publication date.

The Clearing House Payments Company LLC did not prepare this document. The Clearing House is not responsible for any inaccuracies about the RTP® Network, the applicable laws, and regulations relevant to instant payments, or payment systems in general.

Section 1: Introduction

Financial institutions (FIs) adopting instant and high-value payment rails must operate far more than just the core “send” and “receive” payment flows. While value messages move money, significant day-to-day operational complexity also comes from the non-value messages and related functions that initiate, support, or resolve those transactions —such as requests for payment or return of funds, remittance advice, exception handling, responding to queries, managing disputes, and supporting customer and network investigations.

The U.S. Faster Payments Council Operational Considerations Work Group has previously provided detailed guidance on implementing and operating value-based payment flows, including receiving and sending payments and the messages directly associated with those actions. This document builds on that foundation by focusing specifically on the non-value message types that are essential to running these payment rails reliably in production.

This guide covers operational considerations for messages such as Request for Payment, Request for Return of Funds, Request for Information, and other non-value interactions used across instant and high-value payment networks. Although these messages do not move funds themselves, they play a critical role in customer experience, exception handling, regulatory compliance, and overall network stability.

By concentrating on the operational handling of non-value messages — including monitoring, workflows, ownership, and cross-team coordination — this document aims to help institutions design an operating model that supports the full lifecycle of instant payments to better enhance and support money movement for customers and operations.

With that foundation in mind, it is helpful for participants to ground the subsequent discussion in a shared understanding of what non-value messages are, how they are categorized, and where the RTP® Network and the FedNow® Service align and diverge in their support. The overview that follows establishes that common reference point before moving into the message-by-message operational guidance that comprises the bulk of this document.

Section 2: Overview of Non-Value Instant Payment Messages

2.1. Overview of Non-Value Instant Payment Messages

Non-value instant payment messages are communications exchanged within instant payment networks that do not settle but support, enhance, or enable the payment process. These messages are integral to both The Clearing House (TCH) Real-Time Payments (RTP) system and the Federal Reserve's FedNow Service. They facilitate operational efficiency, customer experience, and risk management by providing information, requests, and responses that surround the actual movement of money.

2.2. Definition and Importance of Non-Value Instant Payment Messages for Financial Institutions

Definition: Non-value messages are ISO 20022¹ based communications that do not initiate or settle a payment but serve other critical functions—such as requests for information, payment acknowledgments, remittance advice, and system notifications.

Importance: Customer Service: Enables real-time communication (e.g., payment requests, acknowledgments, remittance advice) that improves transparency and responsiveness for end users.

- Fraud Prevention/Risk Management: Supports dispute resolution, return of funds, and information requests, helping institutions quickly address suspicious activity or errors.
- Competitive Positioning: Institutions offering robust non-value messaging can differentiate themselves by providing enhanced digital experiences, faster resolution of issues, and richer data for clients.

2.3. Types of Non-Value Messages

Key non-value message types include:

- Request for Payment (RfP) – PAIN.013
- Response to RfP – PAIN.014
- Remittance Advice – REMT.001
- Acknowledgement (User to User/Bank to Bank) – CAMT.035
- Request for Return of Funds – CAMT.056
- Response to Request for Return of Funds – CAMT.029
- Request for Information – CAMT.026
- Response to Request for Information – CAMT.028
- Request for Payment Cancellation – CAMT.055
- Account Reporting Request – CAMT.060
- Account Reporting Response – CAMT.052
- Admin & System Notification Messages

2.4. System Support: RTP vs. FedNow Differences

RTP (TCH)

- **Comprehensive support** for ISO 20022 non-value messages.
- **Optional capabilities:** Certain features, such as Request for Payment (RfP), are optional for participating institutions to enable.
- **24x7x365 availability:** Requires continuous technical and operational capacity to receive and act upon non-value and administrative messages at all times.
- **Implementation differences:** Differs from FedNow in settlement structure, operational models, and interoperability, influencing how institutions implement non-value messages.

FedNow Service

- **Comprehensive support** for ISO 20022 non-value and administrative messages (including RFIs, RfR, and RfP), actively used across participants today.
- **Optional capabilities:** Features like Request for Payment (RfP) are fully supported in the message catalog but are optional for institutions to enable (not phased in over time).
- **24x7x365 availability:** Requires continuous technical and operational capacity to receive and act upon non-value and administrative messages at all times.
- **Implementation differences:** Differs from RTP in settlement structure, operational models, and interoperability, influencing how institutions implement non-value messages.

2.5. Comparison Chart and Uses

Message Type	ISO 20022 Code	Applicable Network	Typical Use Case
Request for Payment (RfP)	PAIN.013	Both	Requesting payment from payer
Response to RfP	PAIN.014	Both	Accepting/rejecting payment request
Remittance Advice	REMT.001	RTP Only	Providing payment details
Acknowledgement (User/Bank)	CAMT.035	RTP Only	Confirming receipt/processing
Request for Return of Funds	CAMT.056	Both	Initiating payment reversal
Response to Return of Funds	CAMT.029 ²	Both	Communicating reversal outcome
Request for Information	CAMT.026	Both	Seeking transaction details
Response to Request for Information	CAMT.028	Both	Providing requested information

Message Type	ISO 20022 Code	Applicable Network	Typical Use Case
Payment Status Request	PACS.028	FedNow Only	Request processing status of payment
Request for Payment Cancellation	CAMT.055	FedNow Only	Requesting cancellation of a previously sent Request for Payment
Account Reporting Request	CAMT.060	FedNow Only	Requesting account balance, activity, or related account reports
Account Reporting Response	CAMT.052	Both	Providing account balance, activity, and reporting information
Admin & System Notification	Varies	Both	System status/alerts

Expanded Customer Service Benefits

Non-value instant payment messages can play an important role in elevating customer service for financial institutions participating in instant payment networks such as RTP and the FedNow Service. These messages, while not directly moving funds, create a richer, more transparent, and responsive payment experience for both consumers and businesses. Here is how:

- **Enhanced Transparency and Communication:** Real-time notifications and remittance advice improve clarity and reduce uncertainty.
- **Faster Issue Resolution:** Requests for information and return of funds enable quick dispute handling and error correction.
- **Proactive Service and Support:** RfP and system notifications keep customers informed and engaged.
- **Personalized and Segmented Experiences:** Tailored messaging for wholesale and retail segments enhances satisfaction.
- **Reduced Manual Intervention:** Automated messaging minimizes the need for customer calls or branch visits.
- **Building Trust and Competitive Differentiation:** Robust messaging demonstrates transparency and responsiveness, strengthening customer trust.

Of all the non-value messages cataloged above, the Request for Payment has attracted the most strategic interest across the industry — both for the new revenue and engagement opportunities it unlocks and for the operational complexity it introduces. Because RfP touches customer-facing channels, billing systems, fraud controls, and core posting workflows in roughly equal measure, it warrants the most in-depth treatment. The section that follows examines RfP end-to-end, from business opportunity through launch readiness, with attention to where RTP and the FedNow Service take meaningfully different approaches.

Section 3: Request for Payment

Request for Payment (RfP) allows a payee to send a secure, real-time payment request through a digital network, enabling the payer to review and authorize payment before funds are sent instantly. Both RTP and FedNow include RfP as a core capability, while platforms such as Zelle and several fintech providers offer functionally similar request-based experiences.

Unlike traditional ACH rails—where authorization is typically established in advance—the FedNow Service and RTP RfP flows today generally require a manual, two-step process: The initiation of the request for payment by the payee is initiated by the payee followed by explicit payer review and approval. While this construct introduces additional user interaction, it also provides enhanced security and incremental fraud mitigation through affirmative customer consent at the point of payment.

For financial institutions, RfP represents a significant opportunity to modernize bill presentment, settlement, and liquidity management. When properly implemented, it strengthens customer engagement, improves cash flow certainty, and enables richer data exchange. At the same time, adopting RfP on real-time rails requires 24x7x365 operational readiness, mature fraud and risk controls, and disciplined regulatory compliance—demands that necessitate cross-functional coordination and sustained investment across technology, operations, and risk functions.

3.1. Business Opportunities for Financial Institutions

RfP allows financial institutions to redefine money movement, offering early adopters a distinct competitive advantage by embedding instant, data-rich payment experiences directly into digital ecosystems.

- **Revenue & Strategic Growth:** Drives new product growth through transaction-based fees, API monetization, and data-rich invoicing. Strategically, it modernizes cash flow management, deepens digital customer engagement, and improves long-term retention ("stickiness").
- **Implementation Challenges:** Success requires overcoming market awareness hurdles while upgrading legacy systems, billing infrastructure, and compliance frameworks to support continuous, data-intensive real-time operations.

Key Use Cases³

- Business-to-Business (B2B): Enables supplier invoice automation, trade payments, and simplified reconciliation.
- Account-to-Account (A2A): Supports immediate transfers between a customer's own accounts. This includes the funding and defunding of a wallet account or transfers between brokerage accounts.
- Consumer Bill Pay (C2B): Instant bill presentment and settlement replace legacy ACH or check-based payments. Requests made by Billers may submit requests for single consumer services.
- Consumer Down Payment, Security Deposit, or Final Payment (C2B): Request for a one-time payment that satisfies the outstanding balance of an obligation or initial deposit for opening a deposit account.
- Government Payments (G2C or G2B): Enables government agencies to request payment for an obligation owed by a consumer or business such as tolls, taxes, licensing fees, or fines.
- Healthcare Payments (B2C): Enables healthcare providers to collect payments for medical services related to healthcare expenditures or insurance premiums.
- Trusted Party (B2C): Permits trusted parties to originate from an RfP to a non-consumer receiver who has an established relationship with the sender. RfP is for payments on prior obligations and not a current sale.

3.2. Operational Flow

RfP operational flows present an opportunity to deliver a frictionless payment experience that bridges digital banking, clearing networks, and back-office systems. At the same time, success between the FedNow Service and RTP depends on overcoming complexity in message consistency, service level agreement (SLA) alignment, and exception handling across multiple instant payment networks. The RfP message specs themselves also differ slightly between the two networks. While both networks use the same pain messages, there are differences in the response types (for example, FedNow allows for ACTC - Accepted, PRES - Presented, RJCT - Rejected while RTP allows for RJCT - Rejected)—and they use different fields to reference the original payment. These nuances are important to understand when implementing the overall technical messaging solution.

As institutions expand instant payment offerings, the ability to manage routing logic, timeout scenarios, and standardized customer presentation becomes critical for scalability, trust, and customer satisfaction.

Process Overview

- Initiation: Payee or biller (via FI or service provider) creates and submits an RfP message.
- Routing: Request is transmitted via network (RTP, the FedNow Service).
- Validation: Receiving FI confirms enrollment, account status, and authenticity.
- Presentation: Payer reviews the request through their digital interface.
- Response & Payment: Payer accepts (triggers instant payment) or declines.
- Notification & Reconciliation: Both parties receive confirmations.

Initiation and Presentation Rules

- RTP: Only vetted, authorized billers or third parties under sponsoring FIs can send RfPs under defined “permissible use” rules.⁴
- The FedNow Service: Participants and their sponsored partners can send/receive RfPs once enabled by their FI, which manages permissions internally. In addition, the FI must opt in to FedNow’s “Receive Request for Payments” service before RfPs can be routed to the institution.
- RfPs must include clear requester identity, invoice details, and structured data, enabling customers to verify authenticity and reducing fraud risk.

It should be noted that in the current RfP environment providing accurate data required for the identification of and routing to a request recipient is the responsibility of the payment initiator and the initiating FI. Different data directory repositories exist for different sectors, payment types, and networks, but no central directory of recipients exists on either RTP or FedNow networks. Several initiatives are underway to create such a directory or link existing directories, but FIs considering offering RfP services should be aware that additional identity due diligence for RfP recipients will be required.

3.3. Technology Integration

Payments made in response to RfPs are generally final, but both systems allow exception-based returns for errors or suspected fraud. Financial institutions handle these through defined message flows and bilateral coordination between sender and receiver.

Again, due to the differences in the networks, it is important to note that the process for referencing and closing the RfP differs. The FedNow Service enforces the use of End-to-End ID to reference the payment and the RfP, while RTP allows for End-to-End ID or RMTInf or OriginalMSg ID. Therefore, matching payments can be a little more complicated and must be considered.

3.4. Compliance and Regulatory Requirements

RfP operations are bound by regulatory and network-specific frameworks that safeguard consumer rights, data privacy, and transaction integrity. While automation creates opportunities for efficiency and transparency, maintaining compliance in real time remains a core challenge.

Financial institutions that integrate automated screening, recordkeeping, and exception tracking into their RfP systems can reduce manual overhead and improve audit readiness—but must ensure these controls operate within sub-second timeframes to avoid transaction delays.

Core Compliance Domains

Operating an RfP program requires institutions to satisfy obligations that span network rules, consumer protection statutes, sanctions and anti-money laundering controls, privacy mandates, and recordkeeping requirements. Each domain interacts with the others, and gaps in one area frequently surface as findings in another.

Network Rules. The RTP Network Operating Rules⁵ and the FedNow Service Operating Procedures⁶ define permissible message types, formatting requirements (ISO 20022), response codes, timing expectations, and dispute and exception-handling processes. Participating institutions are bound by the rules of the network through which an RfP is sent or received and are responsible for ensuring that messages routed on their behalf — whether by a service provider, processor, or corporate originator — conform to those rules.

Consumer Protection. Regulation E⁷ governs consumer-initiated electronic fund transfers and establishes error-resolution rights, disclosure obligations, and liability limits when a consumer authorizes a payment in response to an RfP. UCC Article 4A governs commercial credit transfers and allocates liability among sender, receiving bank, and beneficiary based on the authenticity and authorization of the payment order. Because an RfP is a request — not a payment — the consumer protection analysis attaches to the credit transfer that fulfills the request, not to the request itself. Institutions should ensure their disclosures, terms of service, and dispute workflows clearly distinguish the two.

Privacy. The Gramm-Leach-Bliley Act (GLBA)⁸, the California Consumer Privacy Act (CCPA)⁹, and analogous state regimes require secure storage of nonpublic personal information, limited sharing with third parties, and clear customer disclosures regarding data use. RfP messages carry structured remittance and reference data that may include identifying details about both the requester and the payer; institutions should treat this data with the same controls applied to other payment metadata, including encryption in transit and at rest, role-based access, and tokenization where supported by the network.

Sanctions and AML. OFAC screening¹⁰, BSA monitoring¹¹, and FinCEN¹² reporting obligations apply to the underlying credit transfer that settles an RfP. Because the credit transfer settles in seconds and is final and irrevocable, screening must occur in near-real time and be integrated into the authorization decision rather than performed as a post-settlement reconciliation step. Institutions should confirm that their sanctions and transaction-monitoring controls operate within the latency budget of the network and that exception handling — including rejection codes and customer communication — is defined in advance.

Audit Trails. Network rules and prudential expectations require immutable, time-stamped logs for each RfP message, response, and corresponding payment. Records should preserve the full message lifecycle, including modifications, expirations, rejections, and the cryptographic linkage between the RfP and the credit transfer that satisfies it. Retention periods should align with the longer network rules, applicable consumer protection statutes, and the institution's broader recordkeeping policy.

Automation supports compliance with greater speed and consistency, but it does not reduce the underlying obligation. Institutions should plan for continuous investment to keep policies, controls, and systems synchronized with evolving regulatory expectations and network rule changes.

3.5. Risk and Fraud Management

RfP expands the attack surface for fraud by introducing open, request-initiated payments into channels that previously relied on payer-initiated flows. This creates a dual imperative: strengthen authentication and enhance fraud analytics while preserving the customer experience that makes RfP attractive in the first place.

Network-level visibility and the structured data carried in ISO 20022 RfP messages create new opportunities to identify and mitigate risk proactively — pattern detection across requesters, velocity checks on rejected requests, and cross-institution intelligence sharing all become more tractable than in legacy rails. While an RfP message is delivered in real time, it does not execute a payment by itself. The actual payment occurs only after the payer approves the request and the financial institution initiates a separate credit transfer, allowing institutions to apply automated screening, permission checks, and validation steps prior to routing the funds. However, because the resulting credit transfer settles instantly once sent, risk defenses must be highly automated, adaptive, and applied consistently at every stage of this multi-step lifecycle.

To date, network-level fraud has not emerged as a material risk, consistent with the experience of other instant payment frameworks. The exposure that warrants the most attention is account-level fraud — particularly business email compromise (BEC), authorized push payment (APP) scams, and account takeover¹³ — where a legitimate customer is induced to authorize a payment in response to a fraudulent or manipulated request. Even where event frequency is low, the irrevocability of the underlying credit transfer means each event can produce outsized customer harm.¹⁴

Gatekeeper Responsibilities. Institutions that elect to offer RfP origination to their account holders serve as critical gatekeepers to the network. They ensure that RfP messages are initiated only for legitimate and permissible purposes, and that the population of senders on the network does not erode the trust that makes RfP commercially viable.

A comprehensive onboarding process should include an enhanced review of the account holder's intended use cases to confirm alignment with the institution's program parameters and with the allowable reasons for initiating an RfP under applicable network rules. Consistent with the onboarding standards applied to Originators in the ACH network, institutions should collect supporting documentation that substantiates the need for RfP services, perform appropriate due diligence on the account holder and its principals, and establish clear, documented criteria for approval.

Following onboarding, institutions should maintain monitoring procedures designed to surface indicators of misuse — including unusually high volumes of rejected requests, atypical velocity, mismatches between requested and historical payment patterns, or customer complaints alleging unsolicited or fraudulent requests. When potential abuse is detected, or when reports of abuse are received from a receiving institution or from the network, the originating institution should promptly investigate and take appropriate corrective action, up to and including suspension or termination of RfP origination privileges.

Institutions should also conduct annual reviews of each RfP-enabled account holder to verify that activity remains consistent with the originally approved use cases. Where activity patterns have diverged, the institution should engage with the account holder to understand the underlying drivers and determine whether the activity continues to fall within the institution's program parameters.

Risk and Control Framework

Authentication. Validate sender legitimacy before a message is routed. Strong customer authentication — including multi-factor or FIDO-aligned credentials for digital channel access — should be applied to both the initiation of an RfP and the authorization of the responsive payment. Step-up authentication is appropriate for higher-value or out-of-pattern requests.

Spoofing and Social Engineering. Detect unusual patterns, duplicate requests, lookalike requester identities, and inconsistencies between requester display names and underlying account information. Where networks support verified requester information, institutions should display it prominently in the customer channel and visually distinguish unverified requests.

Dispute Management. Enable transparent, rapid resolution channels with defined service levels, standardized data sharing¹⁵, and clearly assigned roles between sending and receiving institutions, and consistent customer-facing messaging. Liability allocation between participants should be documented in advance and aligned with network rules, with defined escalation paths for cases where rules do not cleanly assign responsibility.

Fraud Reporting. Leverage RTP and FedNow fraud-reporting tools to enable near real-time collaboration with counterparty institutions and the networks. Timely reporting supports recovery efforts, informs network-level analytics, and contributes to the shared intelligence that benefits all participants.

Consumer Education. Empower users to verify requests safely within digital channels. Education should address common scam typologies, encourage out-of-band verification of unexpected requests, and reinforce the irrevocability of the underlying payment so that customers approach authorization with appropriate care.

Continual Monitoring. Maintain ongoing oversight of the full RfP lifecycle — issuance, delivery, acceptance, rejection, expiration, and settlement. A key control is verifying that the executed payment matches the original request. Institutions and networks should use unique identifiers or structured reference data to link each payment to its corresponding RfP, confirming that the payment fulfills the intended request and preventing duplicate or misdirected transactions. Monitoring should also flag exceptions such as multiple payments tied to a single request, mismatches between request details and the executed payment, payments that settle outside the requested window, and patterns suggestive of coordinated abuse.

Strong collaboration across financial institutions and networks — supported by shared fraud intelligence, AI-based analytics, and consistent application of preventive controls — is essential to reducing systemic risk while preserving the operational speed that defines instant payments.

3.6. Servicing and Operational Readiness

Operating an RfP service requires continuous coverage, technical resiliency, and cross-functional coordination. Always-on operations present an opportunity for FIs to demonstrate service excellence and reliability, but they also increase costs, complexity, and dependency on real-time monitoring.

Institutions must design infrastructure and staffing models for scalability and uptime while embedding proactive service management, capacity forecasting, and rapid-issue resolution frameworks.

Operational Focus Areas

- Capacity Management: Ensure infrastructure elasticity during volume spikes.
- Staffing Models: Provide 24/7 operational coverage and specialized training.
- Customer Support: Deliver consistent, initiation of RfPs when needed, real-time dispute handling, and education.
- Multi-Network Consistency: Maintain uniform customer experience across distinct networks.

Automation, redundancy, and AI-driven monitoring can improve operational stability, but must be coupled with disciplined governance and workforce readiness to meet 24x7x365 expectations.¹⁶

3.7. Launch Readiness and Continuous Improvement

Launching RfP represents both a technology milestone and a cultural shift toward real-time banking. The opportunity lies in showcasing innovation leadership and building new partnerships, while the challenge is ensuring organizational alignment and post-launch agility.

Institutions must adopt iterative improvement cycles, gather data and feedback to optimize performance, and mitigate risk. Launch success depends as much on internal readiness as on technical execution.

Implementation Framework

Pilot Testing: Validate flows with internal teams, select customers, and other participating financial institutions.

- Training: Equip staff across functions with process and compliance knowledge.
- SLAs: Define uptime and performance metrics with vendors and networks.
- Continuous Monitoring: Track adoption, transaction latency, and exception rates.
- Governance: Maintain structured change management and quality oversight.

Financial institutions that combine disciplined launch governance with agile post-launch evolution will be positioned to sustain momentum and lead in the maturing instant payments ecosystem.

Whereas Request for Payment is concerned with the orderly initiation of funds movement, the Request for Return of Funds (RFRF) addresses what happens when a payment should not have moved at all or should not have moved in the form it did. Because instant payments are irrevocable upon settlement, the RFRF is the primary mechanism available to participants and their customers when errors, suspected fraud, or warranty breaches occur. The following section examines RFRF use across both networks, with particular attention to the fraud-related (FRAD) and warranty-breach (WNTB/UPAY)¹⁷ flows where operational discipline matters most.¹⁸

Section 4: Request for Return of Funds

The instant payment networks, RTP and the FedNow Service, enabled the transfer of funds in real time that are irrevocable and final. While the immediacy provides significant efficiency, it also necessitates a robust mechanism for error resolution and funds recovery. When errors occur during the initiation of a payment, both the RTP and FedNow networks enable participants to attempt to recover the funds through a Request for Return of Funds (RFRF). Both networks allow these requests for any reason but also use these requests for additional specific use cases.

A critical requirement within both networks is that participants report fraudulent payments to the network and specify that the report should be made by sending a return request with the FRAD reason code. Sending the request with the FRAD reason code serves two purposes:

- Enables the networks to track incidences of suspected fraudulent activities.
- Communicates to the receiving financial institution that the payment was initiated under fraudulent circumstances, triggering a mandatory investigation of its receiver.

Unlike traditional payment rails, the FedNow Service and RTP explicitly require financial institutions to conduct investigations and provide a response to the sending institution.

In addition to fraud-related return requests, both networks support return requests made arising from a warranty breach (WNTB code for the FedNow Service and UPAY code for RTP). These claims occur during the execution of a request for payment (RfP) where a sender warrants that the request is made for a legitimate purpose.

When a receiver of an RfP responds by sending the payment and later discovers that the sender of the RfP breached this warranty, they can make a claim, and the financial institution will send a request for return with the WNTB reason code.

Operational Flow

1. The sender (an individual or business) or internal department initiates the request for return of funds with the financial institution through an interface or directly with the operational department.
2. Financial institution authenticates the sender and validates the sender's return request. The sending financial institution will need to consider the reason for the request to ensure that the request is sent with the appropriate reason code. Upon reviewing the request, the sending financial institution initiates a request for return of funds to the network (camt.056).
3. The networks (RTP Network and FedNow Service) will perform a series of formatting, process, and business rule validations before the message is routed to the receiver's financial institution.

4. The network sends the transaction to the receiver's financial institution and monitors for a response. The receiver's financial institution then receives the request from the network and conducts its own validations (KYC/BSA) to ensure its correctness and security.
5. The receiver's financial institution will evaluate the request and determine the appropriate response. Financial institutions may elect to present the request to their account holder electronically or contact the account holder directly to assist in their determination of the appropriate response.
6. The receiver's financial institution will initiate a response to the return request (camt.029) with the appropriate response code.
7. The network will receive a response to the return request. The network will again perform a series of formatting, process, and business rule validations. Upon completion of the validation, the network will send the response to the sender's financial institution.
8. The sender's financial institution notifies the sender of the return request response.

It should be noted that RTP and the FedNow Service again use slightly different messaging to support the request for return responses. Where RTP allows for agreeing or decline, the FedNow Service has ISO codes like IPAY and RJCR as well as how they allow for partial returns and linkages in the ISO messaging. These nuances should be noted when planning out the messaging and support for these flows.

When the receiver's financial institution receives instructions from the receiver or determines internally that the funds should be returned, it will need to determine how the funds should be returned.

- FedNow Service participants, regardless of their participant level, can return the funds through the network using the pacs.004.
- RTP Network participants' ability to return the funds will depend on their participant profile. Sending participants will initiate a pacs.008 to return the funds through the RTP Network. Institutions that are receive only¹⁹ may need to arrange an alternative method to return the funds via a wire or ACH entry.

Compliance & Rules

The instant payment systems introduce operational challenges for financial institutions, particularly in managing returns, refunds, recalls, and fraud. Unlike traditional payment rails, instant payments offer near-immediate finality, leaving little room for error correction and dispute resolution. Institutions must navigate strict scheme-defined time windows, standardized reason codes, and evidence requirements while ensuring compliance with consumer protection regulations such as Regulation E, which governs unauthorized electronic fund transfers, and Regulation Z,²⁰ which applies to credit-linked transactions.

These complexities require organizations to implement a robust operational framework that combines clear governance, automated SLA tracking, and set audit trails with strong preventive measures. This includes implementing 24x7 operational coverage, integrated case management systems, and advanced fraud detection tools capable of real-time monitoring. Customer education and transparent communication are equally critical to mitigate social-engineering risks and maintain trust.

A well-designed operating model, compliance frameworks, and audit-ready documentation will ensure timely resolution of exceptions, adherence to regulatory obligations, and resilience against emerging fraud threats. By aligning scheme rules with regulatory requirements and embedding strong controls, financial institutions can balance the promise of instant payments with the operational rigor needed to safeguard customers and maintain compliance in an environment where transaction finality is immediate.

Technology Integration

Technology integration for non-value messages in the RFRF is critical to achieving real-time interoperability in instant payment ecosystems. Institutions must adopt ISO 20022 messaging standards and implement API-first architectures to enable seamless exchange of requests and responses, such as payment inquiries and status updates. Modern payment systems rely on flexible technology to keep services always running smoothly. To keep customer data and transactions secure, strong protections like encryption, digital verification, and secure access methods are essential. These measures ensure that instant payment networks remain reliable, safe, and ready to meet customer expectations.

Technology integration should also include sub-second processing, SLA monitoring, and robust observability tools for end-to-end visibility. Compliance alignment with Reg E and Reg Z, as well as AML/KYC²¹ and sanctions screening,²² requires structured data and immutable audit logs. Future trends of technology point toward full ISO 20022 migration, AI anomaly fraud detection, and open banking integration, positioning non-value messaging as a cornerstone for secure, efficient, and interoperable instant payment networks.

Customer Impact

Customer impact in the context of non-value messages within the RFRF for instant payments centers on transparency, trust, and usability. Operational considerations like 24x7 availability, intuitive user interfaces (UI), and clear exception handling directly influence customer experience, while structured ISO 20022 data improve clarity and reconciliation for both consumers and businesses. Regulatory protections under Regulation E ensure error resolution and liability limits for unauthorized transfers, and Regulation Z applies when credit features are linked to instant payment

accounts, requiring clear disclosure of terms. Institutions must also prioritize fraud prevention, data privacy compliance, and dispute resolution to maintain trust. Looking into the future, personalization through AI, open banking integration, and global ISO 20022 standardization will further enhance customer convenience and security, making non-value messaging a cornerstone of a positive instant payment experience.

Operational Challenges

Financial institutions face several operational challenges when handling Requests for Return of Funds, especially given the 24x7x365 nature of instant payments and the low transaction volumes today that can mask readiness gaps.

Staffing & Skill Requirements

- RFRF processing often spans multiple teams (operations, fraud, treasury, and customer support), yet very few institutions have clear ownership or cross-training in place.
- Because RFRFs are infrequent, frontline teams may lack familiarity with decision criteria, documentation requirements, or escalation pathways.
- Off-hours support is inconsistent across institutions, increasing the risk of missed return windows or delayed responses.

Timeliness & Service Levels

- Both RTP and the FedNow Service set expectations for timely responses, but many institutions still rely on manual reviews and email-based handoffs that slow decision-making.
- Financial institutions must validate the legitimacy of the request, the identity of the initiating FI, and the underlying transaction details—processes that may not be automated in today's environments.
- Partial returns add additional complexity, requiring interpretation of network rules and customer agreements.

Business Continuity & Exception Handling

- During outages or planned maintenance, institutions may lack automated fallback processes for receiving, reviewing, and responding to RFRFs.
- If the FI cannot process a return in-rail (e.g., not enabled for Send on RTP), operations must pivot to alternative rails such as ACH or wire, introducing risk and inconsistency.
- Operational documentation and playbooks are essential to ensuring continuity, yet many institutions have not updated them since initial instant payments onboarding.

Vendor and System Dependencies

- Core providers, third-party processors, and instant payment gateways vary widely in their support for RFRF functionality, leading to fragmentation in how requests are displayed, queued, and acted on.
- Some FIs do not have UI access to send, receive, or respond to RFRFs and must rely on vendor staff to interpret or relay non-value messages, creating operational bottlenecks.

Monitoring, Reporting, and Visibility Gaps

- Low volumes create complacency. Many institutions see few RFRFs, leading staff to assume “nothing ever happens,” which masks readiness gaps until an instant payment exception occurs.
- Reporting is often limited to accounting teams. Most institutions only review RTP and FedNow reports for liquidity or balance purposes, not operational exceptions.
- No RFRF-specific exception reporting. Few systems generate operational dashboards or alerts for RFRF receipt, aging, response deadlines, or duplicate requests.
- Lack of active monitoring for incoming RTP messages is important. Without alerts, institutions may miss RFRFs submitted overnight or near cutoff windows, creating financial and operational risk.
- Alerts and automated notifications are emerging best practices. Institutions with mature 24/7 operations use workflow alerts, mailbox monitoring, and automated aging reports to ensure timely handling.

Strategic Value

When implemented consistently across RTP and the FedNow Service, standardized Request for Return of Funds processes address not only compliance, but they also deliver tangible operational and customer experience benefits.

Efficiency Gains

- Streamlined handling of return requests reduces reliance on email-based exceptions, hallway escalations, and manual multi-team reviews.
- As more institutions automate validation, workflow routing, and decision capture, response times shrink and accuracy improve.

Reduced Operational Risk

- Standardized RFRF workflows lower the likelihood of processing errors, missed return windows, and miscommunication across teams or vendors.
- Consistent interpretation of network rules builds institutional muscle memory, reducing dependence on individual employees or ad hoc knowledge.

Improved Customer & Partner Trust

- Customers expect clarity when a payment needs to be returned. A structured RFRF process ensures predictable handling and transparent communication.
- Stronger governance builds trust with peer institutions by signaling reliable response patterns, accurate decisioning, and consistent documentation.

Foundation for Future Automation

- Laying a clear operational foundation now enables future adoption of automation, including exceptional dashboards, workflow tools, and AI-assisted response logic.
- Unified processes across networks also position institutions to integrate additional capabilities, such as enhanced RfP flows, directory services, or multi-rail orchestration.
- RfP and RFRF represent the most heavily exercised non-value message flows in the ecosystem today, but they are by no means the only ones participants need to support. A broader family of non-value messages — Request for Information, remittance, administrative, retrieval, and reporting messages — surrounds and supports the core payment flows. The subsections that follow address each of these in turn, beginning with the Request for Information, which provides a structured mechanism for participants to ask clarifying questions about a payment without rejecting or returning it.

Section 5: Other Non-Value Messages

5.1. Operational Considerations for Request for Information (RfI) – U.S. Instant Payments (RTP and the FedNow Service)

Modern payment messaging standards, such as ISO 20022, significantly enhance the capabilities of Faster Payments systems beyond simple value transfers. Platforms like the FedNow Service and RTP leverage these standards to enable rich, structured communication between financial institutions. This includes sending messages that request additional details about credit transfers, payment returns, or Request-for-Payment (RfP) instructions, checking the status of payments requests, and providing timely responses. Additionally, these advanced features ensure that all parties involved have access to comprehensive data, which helps resolve inquiries, disputes, and security concerns efficiently.

Requests for Information (RFI) business value

RFIs allow an FI to ask another FI for clarification after the payment has been submitted, without rejecting or returning the transaction. Use cases include:

- Missing or incomplete remittance details
- Data mismatches between customer-provided and FI-validated information
- Clarifying intended purpose, account ownership, or beneficiary details
- Confirming legitimacy of transactions flagged for risk

These messages support collaborative resolution, reducing friction, and improving customer experience. It can help to address variety of exceptions including those related to investigation or additional data required for:

- Fraud Mitigation
- AML
- Sanctions
- Risk Analytics and Insights

5.1.1. Operational Readiness for Timely Responses

Instant payment networks require real-time operational readiness. Since responses to non-value messages must be handled quickly—often within seconds—FIs must design systems and staffing accordingly.

Real-Time Monitoring & Automation

Financial institutions must deploy capabilities that detect and process RFI and other inquiry/exception messages instantly and consistently. This includes:

- Monitoring inbound RFI and clarification messages in real time
- Automatically routing RFIs to the correct operational, fraud, or compliance teams
- Triggering automated responses when information is available without manual review
- Integrating RFI workflows with fraud, sanctions, and customer-data systems to support rapid decision-making

Effective automation ensures RFIs are handled within network timeframes, prevents backlogs, and maintains service quality across 24x7x365 instant payment operations.

Staffing and Training

Support teams must be equipped to handle:

- Rfl messages
- Name mismatch, missing data, AML/ Fraud risk/ Sanctions review
- Off-hour and weekend operations (24x7x365 obligations)

Training should include message interpretation, exception prioritization, and technical troubleshooting.

Business Continuity Planning

Because instant payments operate continuously, operational readiness requires:

- Redundant systems and failover capabilities
- Clear fallback procedures for exception handling
- Ability to continue responding to RFls during outages
- Coordinated contingency escalation across operations and technology teams

5.2. Recordkeeping and Compliance Considerations

RTP and FedNow participation includes strict obligations for message retention, sanctions of compliance, and auditability.

Message Logging and Retention

All non-value messages—including RFls, RfPs, refunds, and return responses—must be:

- Logged
- Stored
- Retained according to regulatory and network requirements

This supports dispute resolution, audit trails, and compliance validation.

A risk-based approach, supported by internal controls, testing, and continuous monitoring, is recommended.

Structured Data for Compliance

ISO 20022's enhanced data fields allow:

- More accurate sanctions screening
- Improved fraud detection
- Reduced false positives
- Better alignment with AML monitoring systems

5.3. Operational Flow of RFI Messages

A typical RFI workflow includes:

- Initiation – FI identifies a discrepancy and sends an RFI message.
- Routing – Message travels through RTP or FedNow rails to the sending FI. (the routing file should be used to understand which financial institutions accept RFIs and which do not for RTP).
- Validation – The FI that sent the original value message reviews the request, compares to internal data, and investigates.
- Response – FI provides information, clarification, or approval/denial which may require additional info to be sent.
- Resolution – Sending FI uses the returned data to complete posting or pursue the next steps.

The camt.029 – Information Request Response reports the processing status of a previously received camt.026 Request for Information. Response codes include:

- Pending (PDNG): Information request is being reviewed
- Payment instruction is duplicate (IDUP for the FedNow Service and DUPL for RTP)
- Additional information will be sent (INFO) in an additional payment information message (camt.028)
- Payment Initiated (IPAY)
- NINF – no further information available response

More broadly, camt.026 / camt.028 – Request for Information / Response supports structured exceptions & investigations: when the receiving bank needs more data to understand a payment's purpose or resolve an inquiry, it sends a camt.026 Request for Information; the responding FI replies with a camt.028 if additional detail is required, or a camt.029 Information Request Response using one of the codes above.

RFI can be used in the process of manual exception handling, as well as feed into AI-based anomaly detection models.

This workflow reduces unnecessary returns and supports efficient dispute management.

5.4. Compliance and Network Rule Requirements

Both networks require FIs to:

- Follow exception-handling timelines and message rules
- Maintain robust operational controls
- Respond promptly to RFI and return-related messages
- Provide auditable logs and documentation
- Meet customer disclosure and error resolution obligations

Failure to meet expectations can create compliance gaps or operational risk exposure.

5.5. Exception Handling Workflows and Business Value

Exception handling is one of the most important operational components of instant payments. Because payments settle instantly and irrevocably, FIs must rely on structured messaging to manage discrepancies, validate information, and resolve issues after submission.

Accept Without Posting

Both RTP and the FedNow Service support an “Accept Without Posting” response, which allows the receiving financial institution (FI) to acknowledge receipt of a payment message without immediately crediting the funds to the beneficiary’s account. This functionality is particularly important in scenarios where additional verification or manual review is required before final settlement to the end customer (posting). ACWP is only allowed for use in compliance and fraud monitoring and is not allowed to be used for maintenance or other “downtime.” For example:

- Additional time is needed to review a message for compliance and/or legal concerns.
- AML, OFAC/ sanctions screening hits require further investigation
- Fraud alerts or risk flags require validation
- Suspicious activity monitoring identifies anomalies

By doing so, institutions maintain operational flexibility and mitigate risk without rejecting the payment outright, which could disrupt customer experience or create unnecessary delays. This mechanism ensures that instant payment systems can balance speed with security and regulatory obligations, providing a safeguard against fraudulent or suspicious activity while preserving the integrity of instant payment networks.

ISO 20022 Exception Messages

Instant payment systems rely on ISO 20022 message types²³ to support structured, automated workflows. While these are not the only messages within the system, some of the key messages include:

- pacs.028 – Payment Status Request: Request the participant to provide further information on a previously sent customer credit transfer (pacs.008), payment return (pacs.004), or request for payment instruction (pain.013).
- camt.056 – Return Request: FI-to-FI Payment Return Request - Processing status of a previously sent return request.
- camt.026 - Request for Information

- camt.055 - Request for Payment Cancellation: Used by a FedNow participant to request cancellation of a previously sent Request for Payment. The receiving participant communicates its response through a camt.029 message.

These standardized notices (status reports, inquiries, and responses) are to create a structured, automated communication layer between financial institutions that supports transparency, compliance, and operational efficiency in instant payment systems like RTP and the FedNow Service.

While Rfls enable participants to ask questions about a payment after the fact, remittance messages address the upstream goal of ensuring those questions need not be asked in the first place. Rich, structured remittance information allows businesses and their financial institutions to reconcile transactions automatically, reducing the volume of downstream inquiries and exceptions. The next subsection examines how RTP and the FedNow Service approach remittance — both embedded within pacs.008 and, in RTP's case, as a stand-alone remt.001 message.

5.6. Remittance Messages

As instant payments expand across the United States, ISO 20022 has emerged as the global standard for payment messaging. It offers a structured, data-rich format that improves interoperability, automation, and reconciliation. While most discussions focus on value messages, ISO 20022's ability to carry remittance information—whether embedded in payments or transmitted separately—delivers major benefits for both financial institutions and businesses.

For corporate and business banking customers, ISO 20022's structure represents a leap forward in data consistency and automation. Its remittance capabilities enable businesses to:

- Streamline reconciliation by embedding invoice numbers, purchase orders, and structured remittance references directly in payment messages.
- Reduce manual intervention and exception handling with consistent, machine-readable identifiers.
- Enhance decision-making by integrating payment and remittance data directly into ERP, treasury, and accounting systems.

Traditional formats such as ACH constrain remittance data. ISO 20022 removes many of those limits, allowing richer and more structured remittance content. This supports straight-through reconciliation, improved auditability, and better exception management.

Financial institutions can use ISO 20022's standardized model to deliver a unified payment and remittance experience across RTP and the FedNow Service—so clients can see payments and remittance details together in real time.

Remittance Handling (pacs.008 and remt.001)

Message / Function	RTP Support / Behavior	FedNow Support / Behavior	Differences / Implications
pacs.008 — Customer Credit Transfer	Primary payment message used to move funds between participants. Supports remittance information under CdtTrfTxInf/RmtInf, in either unstructured (Ustrd) or structured (Strd) form. RTP participants can include short text or limited structured references.	Used for all FedNow customer credit transfers. Supports both structured and unstructured remittance fields, as well as reference remittance information, such as a hyperlink pointing to a document or invoice repository.	Both networks allow embedded remittance data within pacs.008. FedNow enforces stricter field-length and character-set rules, while RTP allows for slightly more flexibility. In both cases, keep pacs.008 remittance concise to meet real-time SLA requirements.
remt.001 — Remittance Advice	RTP defines a 'Stand-Alone Remittance Advice' (remt.001) message for detailed invoice-level remittance. However, it is not mandatory, not widely implemented, and most participants do not currently use or receive it. FIs should treat it as optional and plan accordingly.		RTP includes remt.001 in its ISO 20022 definitions, but adoption is low. The FedNow Service does not support it. FIs should consider that one internal remittance process for consistency may be best.
Payment ↔ Remittance Linkage	The EndToEndId in pacs.008 is used to associate a remt.001 message with its corresponding payment.	Same linkage method—EndToEndId or equivalent reference ties any remittance advice to its payment.	Identical linking concept across both rails; adopting consistent identifiers simplifies reconciliation and integration.
Message Size / Payload Best Practice	ISO 20022 guidance recommends limiting in-message remittance to around 140 characters of free text or a few structured repeats and using remt.001 for extended detail if required.	Same general best practice: concise embedded remittance in pacs.008	FIs should design reconciliation logic that works even when only pacs.008 remittance is received

Field Usage and Structure

Both RTP and the FedNow Service use ISO 20022 remittance fields, but differ slightly in field lengths, character sets, and structured field rules. The FedNow Service applies stricter validation and format checks, while RTP allows flexible unstructured text but still enforces ISO 20022-compliant encoding. Financial institutions should harmonize ERP and payment-hub mappings to support both rails consistently.

Reconciliation and Workflow Design

Payments include minimal remittance data within pacs.008, while detailed advice can be delivered via remt.001 when supported. Since remt.001 usage on RTP is minimal and optional, FIs should not depend on receiving it for reconciliation. Instead, design workflows that reconcile using EndToEndId, extract remittance fields, and handle missing or delayed remittance advice gracefully.

Alignment Across RTP and the FedNow Service

Financial institutions operating on both rails should establish a single remittance-handling model: embed concise remittance data directly in pacs.008, use remt.001 only if both sender and receiver support it, and normalize remittance and reconciliation processes so ERP, API, and portal logic work identically across RTP and the FedNow Service. Since the FedNow Service does not support remt.001 and RTP has shared there is limited usage, FIs may want to consider not supporting/counting on that message in their reconciliation processes.

Optionality and Implementation Planning

RTP remt.001 exists but is not mandatory and rarely used. Participants may support it for completeness but should plan scenarios where it is not exchanged. It is best to align around pacs.008-based remittance as the baseline process for both rails.

Summary

Both RTP and the FedNow Service employ ISO 20022 to support richer remittance data through the pacs.008 (Credit Transfer).

- pacs.008 embeds concise remittance information directly in the payment.
- remt.001 provides detailed remittance advice but is only supported on RTP and is optional.
- RTP defines remt.001 but it is not widely used or required.
- The FedNow Service supports structured remittance fields and reference remittance within pacs.008.

To minimize complexity and improve interoperability, FIs should align one consistent remittance-handling process across both RTP and the FedNow Service. Reliance on pacs.008 is recommended to ensure all critical reconciliation data is captured.

Transaction-level messaging — whether moving funds, requesting them, returning them, or describing them — only functions when the underlying connection to the network is healthy and well-monitored. That responsibility falls to a separate class of administrative and system messages that communicate participant availability, system events, and operational status. The subsection that follows describes these messages and the monitoring obligations they create for participating financial institutions.

5.7. Administrative System Messages²⁴

FedNow Service	
FedNow Service	FedNow admin messages are used by the FedNow Service and participants to communicate message processing failures, operational status changes, system-wide notifications, participant-initiated status updates, retrieval of prior messages, and daily participant information.
admi.002 – Message Reject	This message type is sent when either FedNow or a participant cannot interpret an incoming message due to technical or structural issues.
admi.007 – Receipt Acknowledgement	Receipt Acknowledgement messages confirm successful receipt of a non-value message (e.g., pacs.028, camt.056). The FedNow Service sends an admi.007 to the Sender when the message has passed required validations and has been delivered to the Receiver. Likewise, the Receiver FI generates its own admi.007 to acknowledge receipt back to the Sender.
admi.004 – FedNow Broadcast	The FedNow Service broadcasts communicate operational updates to all participants, including events such as a FedNow funds-transfer business-day extension or rollover, changes to transaction limits, the availability of new public keys, and other service-related notices. They also announce participant status changes—specifically sign-on (FPON) and sign-off (FPOF) events.
admi.004 – Participant Broadcast	Participant Broadcasts allow a FedNow participant to notify the FedNow Service of the occurrence of a participant event (i.e., sign-on or sign-off, connection point disconnection or reconnection) or to query whether there is a connection to the FedNow Service (i.e., ping). When Signed Off, a participant cannot receive pacs.008 or pacs.004 messages but continues to receive system messages—including broadcasts—and must still monitor and respond to its message queues.

FedNow Service	
admi.011 – FedNow System Response	FedNow system response message used to confirm receipt and successful processing of a participant’s admi.004 broadcast (e.g., sign-on, sign-off, connectivity check, or connection-point actions).
Admi.006 – Retrieval Request	A Retrieval Request is used by a FedNow participant to obtain copies of one or more previously sent or received messages. A single request may include multiple message IDs and can retrieve both value and non-value messages from the current or prior seven business days.
Admi.998 - FedNow Participant File	This is the daily Participant List message that provides all active FedNow Participants who can receive, or send and receive, instant payments (pacs.008 and pacs.004) or receive Requests for Payment. The FedNow Service automatically sends this list at the start of each cycle day. The Participant List can also be retrieved through the FedNow interface or via an API request.

RTP	
RTP	RTP Administration messages are divided into three groups: System event and notification, Sign-On/Off, and Echo. Like FedNow, they are used to indicate operational statuses, communicate system-wide information, and notify technical problems.
admi.004.001.02 System Event Notification	These messages most important operational function is system-wide advertisement of participant (or, quixotically, system) availability or unavailability. Other system-wide notices such as reconciliation window closings and openings are also conveyed via this message type. Additionally, they are how the system operator communicates participant-specific events directly to participants. Examples include funding account balances, warnings, or limiting changes. Additionally, these messages are the method by which the system can convey information to the participating FI that is not available in any other message type – a “catch-all” with no data format restrictions.
admi.002.001.01 – Message Reject	As the title implies, this message type is sent either by the system or by a participant to indicate an inability to interpret a received message. This is distinct and different from a negative response to other transactional messages and indicates a technical problem with either the ability to parse the message or some part of it or the message’s Digital Signature.

RTP	
admn.001.001.01 – Sign-On Request admn.002.001.01 – Sign-On Response admn.003.001.01 – Sign-Off Request admn.004.001.01 – Sign-Off Response	Sign-On and Sign-Off Requests are exactly what they appear to be, an indicator, sent at the Participant level, to the system of a Participant's availability to send or receive messages. It is important to note that Third-Party Service Providers may send these requests on behalf of Participants, but only the Participants themselves may Sign-On and Sign-Off. Sign-On and Sign-Off Responses are messages from the System operator that Accept or Reject a request.
admn.005.001.01 – Echo Request admn.006.001.01 – Echo Response	Echo messages are used to verify Participant responsiveness, usually during periods of no transaction activity. They can be sent by either the System or another Participant and must be responded to by the receiver. If no response is received, the System marks the Participant Connection as unavailable and sends a System-wide broadcast to that effect. The next successful request/response exchange will cause the system to change the status of the Connection and broadcast the changed status.

Operational Responsibilities and Continuity Considerations

Financial institutions participating in either the FedNow Service or RTP Network are responsible for monitoring and acting upon system-generated and participant-generated administrative messages, as necessary. Rules for both networks require participants to evaluate receiver participation profiles and availability status before transmitting value messages. Participants are also required to notify changes in their own status in a timely fashion and adhere to connectivity uptime requirements. It is important for a Participating FI to consider the differences between participating in these networks vs. other payment networks when it comes to 24x7 availability, the ability to transmit, receive, and act upon non-value messaging, and set RTO requirements in compliance with network rules for both Continuity and Disaster scenarios.

Beyond the administrative messages that keep participants in sync with the networks, both RTP and the FedNow Service expose a set of retrieval, reporting, and investigation messages that provide a critical lens into participant activity, master and joint account positions, and the disposition of specific transactions. These messages often live outside day-to-day payment operations but are indispensable to reconciliation, liquidity management, and exception research — and they warrant equal operational attention.

5.8. Retrieval, Reporting, and Investigation Messages

In addition to administrative and system notifications, both the FedNow Service and RTP support non-value messages that enable retrieval, reporting, reconciliation, and formal payment investigations. These messages can be critical for operational visibility, exception handling, compliance, and audit readiness.

Financial institutions should actively monitor these message types and are well-advised to ensure their accessibility outside of normal operational functions and workflows.

FedNow Service

Accounting and Reporting Messages

FedNow accounting and reporting messages support participant reconciliation, liquidity monitoring, and transaction-level visibility.

- camt.060 – Account Reporting Request: Sent by a participant to request any FedNow account report, including account activity totals or details, account balance, and correspondent activity totals or details.
- camt.052 – Account Report: The account reporting message the FedNow Service uses to deliver account or correspondent reports—such as balance, activity totals, activity details, and intraday reports—generated in response to a camt.060 request.
- camt.054 – Debit/Credit Notification: Real-time debit/credit notification sent by the FedNow Service to a Correspondent to report settled credit or debit entries posted to a participant’s master account. Only settled transactions generate a camt.054; rejected transactions do not.

Operational Considerations: These messages are often most valuable to Accounting or Treasury functions tasked with managing liquidity. Participants can combine camt.052 and camt.054 outputs into dashboards and monitoring tools and create a functional end-of-day or end-of-processing-cycle “statement” of master account activity.

Payment Status Message

pacs.002 – Payment Status Report: These messages communicate the processing status of all FedNow value messages (pacs.008, pacs.004, and pacs.009). A receiving participant uses it to indicate whether a payment or return has been accepted or rejected, and the FedNow Service uses it to indicate whether a message has settled or has been rejected for business-rule reasons. FedNow also issues pacs.002 messages when a payment fails FedNow validations—such as negative-list hits, duplicate messages, or other business-logic rule violations. A pacs.002 therefore provides the authoritative final status of a transaction within the FedNow Service.

Operational Considerations: It is important that pacs.002 messages be monitored in real time, as they provide the authoritative final status of every FedNow value message. Timely ingestion and correlation of pacs.002 messages are essential for accurate settlement, liquidity monitoring, exception processing, and reconciliation.

pacs.028 - Payment status request: Used by a participant to request the current processing status of a previously sent payment—such as a pacs.008 customer credit transfer or pacs.004 payment return. The FedNow Service acknowledges the request with an admi.007 and returns the applicable pacs.002 status report. A pacs.028 may only be used for transactions from the current or immediately preceding FedNow cycle day; older transactions are not eligible for pacs.028 inquiry.

RTP

Accounting and Reporting Messages

- RTP provides reporting messages to participants that are used for reconciliation and monitoring of participant activity.
- **camt.052 – Account Report:** Used for continuous liquidity visibility into the participant's RTP joint account; contains balance, credit and debit entries, and funding and defunding activity.
- **camt.054 – Debit/Credit Notification:** When a debit or credit transaction is posted to a participant joint account, the RTP Network sends a camt.054 notification.

Operational Considerations: As with the FedNow Service, RTP reporting messages are often consumed primarily by Accounting and Treasury functions for liquidity management purposes. Debit/Credit Notification messages are extremely valuable in several operational areas — they are an excellent vehicle for downstream (e.g., customer) notifications; for reconciliation, exception handling, and research can rely on their presence or absence as definitive when determining if a particular transaction is settled; and they are often used to initiate or trigger posting to the participant's core system.

Payment Status Message

pacs.002 – Payment Status Report: Similar to the FedNow Service use above, pacs.002 messages are ubiquitous in RTP. They communicate from the network to a participant about the acceptance, rejection, or processing status of a payment transaction and any related messages.

pacs.028 - Payment status request: Used by a participant to request the current processing status of a previously sent payment—such as a pacs.008 customer credit transfer.

Summary

Retrieval, reporting, and investigation messages represent a foundational layer of non-value messaging for both the FedNow Service and the RTP network. These messages are crucial to reconciliation, liquidity management, and structured investigation of exceptions and anomalies. With the full inventory of non-value messages now described, a broader point comes into focus: each of these messages — whether initiating, returning, clarifying, reporting on, or describing a payment — represents a potential vector for fraud or operational compromise. Because they frequently inform or trigger downstream value movement, the controls applied to them warrant the same level of rigor traditionally reserved for value messages themselves. The next section turns to fraud, risk, and security considerations specific to the non-value space.

Section 6: Fraud, Risk, and Security for Financial Institutions as it applies in the Non-Value space

6.1. Fraud Scenarios Unique to Non-Value Messages

Non-value messages can be exploited as entry points for fraud or as mechanisms to mask unauthorized activity. Common scenarios include:

- Spoofed or Manipulated Requests for Payment (Section 3)
- Fraud actors may issue fraudulent RfPs to initiate APP-style payments or redirect corporate invoices.
- Weak validation of requestors increases exposure for both consumers and commercial clients.
- Unauthorized or Fraudulent Requests for Return of Funds (Section 4)

RFRFs can be misused to trigger unwarranted returns, particularly where FIs rely on manual review or do not have clear approval of workflows.

Information Harvesting via RFI

Fraudsters may impersonate FIs to request transaction details, account information, or customer identifiers.

6.2. Authentication and Authorization of Senders

Strong authentication safeguards are essential across all non-value messages:

- System-level authentication (certificate-based controls, mutual TLS) ensures only authorized endpoints can submit or receive non-value messages.
- User-level access control is critical for actions such as issuing RfPs, responding to RFIs, and approving RFRFs.

- Vendor access must follow least privilege and auditable controls, as many institutions rely on processors for message ingestion, routing, or display.
- Dual control should be considered for high-impact actions like approving RFRFs or releasing responses after manual review.

These controls align closely with the operational and decisioning workflows described in Request for Payment (Section 3) and Request for Return of Funds (Section 4).

6.3. Monitoring and Anomaly Detection

Effective fraud monitoring for non-value messages requires:

- Message-Level Monitoring
- Alerts for unusual RfP or RFRF volumes, after-hours activity, or unrecognized senders.
- Pattern detection for repeated RFIs or malformed messages.
- Cross-Message Correlation

Linking non-value messages with value messages (e.g., RfP → pacs.008; RFRF → ACH/wire fallback) to identify discrepancies.

Consistency checks between stop-points described in Request for Payment (Section 3) and adjudication paths in Section 4 (RFRF).

Network-Specific Timing Controls

Monitoring must align to FedNow and RTP windows for response deadlines, returns, and “accept-without-posting” flows.

Automation Opportunities

Automated rule sets can accelerate decisioning, reduce manual errors, and shorten response timelines.

6.4. FI Fraud Team Readiness

Fraud teams must be prepared to interpret and act on non-value messages in real time:

- Training & Familiarity: Teams must understand each message type's purpose and required actions, particularly for RfP and RFRF workflows covered in Sections 3 and 4.
- 24/7 Operational Coverage: Instant payments operate continuously; fraud escalation paths must match that cadence.

- Coordination Across Teams: Fraud, Operations, Treasury, and customer support should have shared playbooks and consistent definitions of decisioning criteria.
- Preparedness for Manual Exceptions: Clear procedures are needed for “accept-without-posting,” partial returns, and out-of-band return scenarios.

6.5. Summary

Non-value messages expand an FI’s operational surface area and can be exploited if authentication, monitoring, and decisioning controls are not aligned. Institutions that invest in clear entitlements, defined workflows, automated monitoring, and staff readiness can materially reduce their exposure to fraud and operational loss—and will experience smoother RfP and RFRF handling throughout; see Request for Payment (Section 3) and Request for Return of Funds (Section 4).

Fraud, risk, and security controls do not operate in a vacuum; they sit within a layered framework of network operating rules and federal regulation. RTP and the FedNow Service have each defined obligations specific to non-value messaging — particularly around Request for Payment and Request for Return of Funds — that differ in important ways and intersect with longstanding consumer-protection regimes such as Regulation E and UCC 4A. The section that follows draws these threads together so participants can align internal compliance programs accordingly.

Section 7: Compliance & Rules Framework (in Non-Value space)

Rule Framework: Although the RTP network and the FedNow Service both support non-value ISO 20022 messages, the two systems differ in how their operating rules define, regulate, and enforce these message types. These differences have meaningful implications for financial institutions designing customer experiences, compliance controls, and operational workflows. The following section summarizes the most consequential distinctions in the treatment of Request for Payment (RfP) and Return Requests.

RTP

- TCH RfP Sender Registration – All Request for Payment participants must comply with the RfP registration process for their senders. This process includes completing the RfP Sender Registration Input Form,²⁵ which includes identifying the permissible use case that each sender will utilize the service for. TCH will assign an RfP Sender ID for each registered sender and add them to a central registry of all RfP Senders. If a sender’s permissible use case has changed, TCH must be notified prior to such changes occurring.

- TCH RfP Permissible Use Cases: TCH has defined the permissible use cases²⁶ that are allowed on the network. It is particularly important that Financial Institutions review and understand what is allowed.
- TCH Request for Payment Warranty Claim Process – The Request for Payment (RfP) Warranty Claims Process establishes how a receiving financial institution may seek recovery when a Request for Payment is believed to have been issued improperly or unlawfully. The process defines prerequisites, documentation standards, claim initiation methods, participant responsibilities, and, if required, the arbitration mechanism administered by The Clearing House (TCH).

Prerequisites for initiating a warranty claim - A Message Receiving Participant may assert a breach of the RfP Warranty only when all conditions below are met:

- A Responding Payment was made based on the disputed RfP.
- The claim is initiated within 95 calendar days of that Responding Payment.
- A Customer Statement is obtained by the Message Receiving Participant.
- The participant has validated that the Customer Statement, if true, supports a potential breach of warranty.

Customer Statement Requirements - Before any claim may be initiated, the receiving institution must maintain a signed or authenticated statement (or equivalent recorded information) from the customer. The statement must include:

- Message Sender's name
- Message Receiver's name and account number
- Date of the Responding Payment
- Narrative explaining why the RfP may have breached the warranty

Claim Initiation Process - Claims must be submitted using the Request for Return of Funds message using the UPAY code as defined in RTP technical specifications. A claim is considered initiated once the sending institution has received all required information. By initiating a claim, the receiving institution warrants that the prerequisites have been satisfied, and that alleged facts support a potential breach. When initiating a claim, the receiving institution must provide:

- The Customer Statement information
- The specific RfP Warranty component allegedly breached
- The Responding Payment's Transaction ID and End-to-End ID
- Any supplemental documentation (optional but allowed until arbitration begins)

Obligations of the Message Sending Participant – Upon receiving the claim, the sending institution must investigate the alleged breach.

Response (Within 20 business days)

The sender must issue either:

- Positive response – agreeing to pay the claim
- Negative response – declining the claim

Requirements for a Negative Response - A valid negative response must:

- Explain why no warranty breach occurred or document that the sender already refunded the customer.
- Not rely solely on the inability to recover funds or the receiving institution's credit decisions.
- Be backed by the sender's certified representation that its investigation supports the response.

Return of Funds - If the sender issues a positive response:

- Funds equal to the Responding Payment must be returned by the next business day.
- The receiving institution must then credit the customer no later than the following business day.

Arbitration – If the dispute cannot be resolved, the receiving financial institution may file for arbitration when:

- The sender provides a negative response or fails to respond within 20 business days, and
- Good-faith resolution efforts have ceased

Claim must be filed with TCH within 45 calendar days of the negative response or expired response window.

FedNow Service

- Zero-Dollar RfP – Zero-Dollar RfP: FedNow provides an option for participants to initiate zero-dollar RfPs to verify whether an end user is technically enabled to receive and act upon RfPs before sending actual payment requests. While not required, this process is recommended to improve the biller/customer onboarding experience. Zero-dollar RfPs are handled solely between financial institutions and are not relayed to the customer; they are intended as a technical enablement check, not as a customer consent or opt-in mechanism.
- RfP Payment Cancellation Request – FedNow utilizes the Camt.055 message, whereas RTP utilizes camt.56.
- RfP Warranties and Expectations – RfPs must only be sent for a legitimate payment purpose supported by an actual underlying transaction. Financial institutions are responsible for ensuring that billers or customers use RfPs appropriately and in accordance with established requirements.

- **Monitoring** – At minimum, FIs must include risk-based procedures to track the volume of RfPs sent by customers to identify potential anomalous activity. Additionally, Sender FIs must review and incorporate within their monitoring any reports or other information received regarding a customer's use of RfP.
- **Procedures** – FIs must have procedures in place to investigate anomalous RfP activity. These procedures must include contacting the relevant customers to confirm that their use of RfP aligns with requirements established by the Sender FI. They should also define any remedial actions the FI may take to address misuse of RfP by customers.
- **Suspected Breaches of RfP Warranty** – If a participant determines that the RfP Warranty was breached after a responding credit transfer has settled, the participant may seek a return of funds by utilizing the Request for Return of Funds message (camt.056) and using the WNTB reason code.
- **As is the case with RTP**, a claim must be submitted within 95 calendar days of the date the credit transfer was settled.
- If no credit transfer was sent in response to an RfP that the receiver FI believes may have been sent in breached the RfP warranty, the Receiver FI should still notify the Sender FI so the Sender FI can incorporate the report into its monitoring procedures.
- If utilizing the Return Request is not sufficient to resolve the dispute, the matter must be addressed outside of the FedNow Service. The Federal Reserve will not make a determination or evaluate the claim.
- The Sender FI of the RfP must respond to the claim within 20 business days of receipt with either IPAY (accepting the return request) or RJCR (rejecting the return request).
- If the Sender FI rejects the return request, it must provide either: (i) a statement explaining why no RfP Warranty breach occurred, or (ii) a statement, supported by documentation as applicable, confirming that the Sender FI has already provided the Receiving FI a remedy in at least the full amount of the payment.

FedNow Service vs RTP – Request for Payment (RfP) Rule Comparison

Category	FedNow Service	RTP network
RfP Message Standard	ISO 20022 pain.013 (request) and pain.014 (response)	ISO 20022 pain.013 and pain.014
RfP Capability	Optional feature of the FedNow Service	Optional functionality for RTP participants
Sender Registration	No central sender registry	Required – RfP senders must be registered with TCH
Sender Identification	Managed by the FI	Each sender receives an RfP Sender ID from TCH

Category	FedNow Service	RTP network
Permissible Use Cases	General rule: request must be legitimate	Explicit permissible use cases defined by TCH
RfP Warranty	Sender warrants request is legitimate	Sender provides RfP Warranty under RTP rules
Monitoring Requirement	FI must monitor customer RfP activity	FI must monitor sender behavior and compliance
Customer Eligibility	FI determines which customers can send or receive RfP	FI determines which customers can send or receive RfP
Central Directory	None for RfP senders	Central RfP Sender Registry maintained by TCH
Fraud Controls	FI responsible for monitoring misuse	FI responsible for monitoring misuse
Warranty Breach Process	Receiver may submit return request using WNTB code	Receiver may initiate formal warranty claim process
Dispute Resolution	Handled outside FedNow Service	TCH arbitration process available
Sender Due Diligence	FI responsibility	FI must perform onboarding and register sender with TCH
Customer Enablement Requirement	RfP may be enabled for subset of accounts or channels	RfP typically limited to approved senders/billers
Operational Oversight	FI establishes monitoring procedures	FI must monitor senders and update registry if use cases change

Request for Return of Funds

Submission Requirements – Return Requests on both the FedNow Service and the RTP network should be submitted within 60 calendar days²⁷ of the original credit transfer.

Regulations and Rules associated with Non-value Messages:

- Regulation E: Instant payments sent from consumer accounts are subject to Reg E. Sending participants are responsible for investigating and resolving alleged errors/unauthorized transactions from consumer accounts.
- UCC4-A²⁸: Sending participants may have liability for unauthorized instant payment transactions initiated by commercial customers under UCC4A.
- RTP Operating Rules
- FedNow Service Operating Procedures
- Operating Circular 8

Disclosures: Disclosures serve as a method to promote transparency and help to mitigate risk within the Faster Payment systems. All FIs must provide disclosures that pertain to all products/services and are written in a clear and concise manner, as well as ensuring customers comprehend the user requirements of Faster Payments.

The RTP network requires the disclosures of daily reconciliation reports, exceptions handling, and pricing for participants. FedNow mandates that participating financial institutions maintain transaction records and report investigated fraud data to the network.

Error Handling: Regulation E applies to electronic fund transfers, including errors related to the electronic fund transfer associated with a non-value message, since the regulation attaches to the credit transfer, not the message itself. Financial institutions must investigate and resolve errors promptly, even if the account is closed, and provide documentation upon request.

Reporting: Both RTP and the FedNow Service offer detailed reporting tools. Non-value messages do not include an accounting entry and could contain status of a value-message, report, or request for information, request for payment, and request for return of funds. The FedNow Service provides real-time notifications and end-of-day reports for all message types, including non-value messages, to support reconciliation and compliance.

Fraud and Risk Management: The Office of Foreign Assets Control (OFAC)²⁹ is responsible for administering and enforcing economic sanctions based on US foreign policy and is responsible for developing, administering, and managing US sanctions programs. Financial Institutions are required to screen account holders for OFAC compliance and are responsible for screening non-value messages for fraud and sanctions risks. OFAC compliance and internal controls must be applied consistently across both networks.

FedNow participants are required to maintain compliance programs—including anti-money laundering, sanctions screening (such as SDN list checks), and customer due diligence—in accordance with applicable laws and supervisory standards. The FedNow Service provides risk management tools, such as transaction limits, negative list functionality, and account activity thresholds, to support participants in managing their own risk.

RTP network has fraud control measures in place, including fraud monitoring before submitting a payment message. The fraud and risk-screening process must be available 24/7. Additionally, participants are required to review fraud alerts and act promptly in their investigation tactics.

Recordkeeping and audit requirements

The RTP Rules require that each participant conduct a self-audit at least annually, which includes non-payment messages. Within the self-audit workbook, there are several rules related to request payment, non-payment messages, and Request for Return of Funds. This workbook can also be a valuable resource for financial institutions that are looking at enabling non-payment messages. Unlike RTP, there is no explicit requirement for a FedNow self-audit; however, Financial Institutions should incorporate audits of the FedNow Service within their existing audit programs.

As consumer instant payment transactions are covered by Reg E, the retention requirement is at least two years.

Even the most carefully designed operational and compliance frameworks ultimately depend on the technology that ingests, validates, translates, and routes ISO 20022 non-value messages in real time. Whether an institution opts for direct core integration, a payment hub model, or a hybrid approach, the architectural decisions made today will shape its ability to absorb future network changes, deliver consistent customer experiences, and meet the latency and availability expectations that instant payments demand. The following section examines those technology and processing considerations.

Section 8: Technology and Processing Considerations for ISO 20022 Non-Value Messages

8.1. Overview

Implementing ISO 20022 non-value messages (e.g., pain.013 Request for Payment, camt.055 Request for Payment Cancellation, camt.060 Account Reporting Request, and camt.052 Account Report) requires a robust technology framework that extends beyond simple message parsing. While these messages do not carry funds, they are the operational backbone of transparency, facilitating straight-through processing (STP) and enabling the "always-on" nature of instant payment ecosystems.

This section outlines key architectural, processing, and integration considerations for financial institutions and service providers.

8.2. Implementation Models: Core Direct vs. Payment Hub

When architecting the environment for non-value messages, FIs generally choose between two primary implementation models. The choice of model significantly impacts how non-value messages are ingested, translated, and routed.

Payment Hub / Gateway Integration: The FI employs a specialized Payment Hub (internal or third-party) that sits between the core and the payment networks. The Hub acts as an orchestration layer, normalizing ISO 20022 messages before they reach the core. This model often allows for greater flexibility in handling optional fields and facilitates easier integration with peripheral systems (such as fraud or digital channels) without overburdening the core banking platform.

In a Core Direct model (aka Core Banking), non-value messages flow directly between the payment network and the core banking platform with minimal intermediary processing. The core is responsible for ingesting ISO 20022 messages, interpreting optional and conditional data elements, and managing routing and responses. This approach can reduce architectural complexity and latency by eliminating an external orchestration layer; however, it often places additional development and maintenance burden on the core platform. Variability in non-value message formats, evolving scheme requirements, and network-specific optionality can require frequent core enhancements, increasing dependency on core release cycles and potentially limiting flexibility in responding to future payment network changes or integrating peripheral systems.

Both implementation models are viable and widely adopted across the industry, with trade-offs that align differently to each institution's technology strategy, operating model, and change tolerance.

A key consideration is the financial institution's existing payments processing architecture. If the FI is already using a payments hub, there is little reason to process non-value messages in the core, and several strong arguments against doing so:

- Non-value messages may not need to touch the core at all, instead triggering other payments directly within the payment engine.
- It simplifies the linkage between related messages (e.g., a pain.013 and the resulting pacs.008).
- It avoids duplicating ISO 20022 parsing.
- It eliminates the need to reimplement scheme connectivity.

However, if the core is already processing payments, the decision becomes more complex. While it would be beneficial to implement non-value messages closer to the payments they reference inside the core, doing so would require a massive modernization effort. The alternative is introducing a non-value message processing sidecar, which risks losing out on many of the opportunities these messages present. This sidecar would either need to be built in-house (entailing significant effort and risk) or procured as an off-the-shelf solution, which adds complexity to the tech stack (e.g., requiring new integrations with risk systems and introducing another UI for which operators can work). Ultimately, this highlights why it may be better to separate payment messaging from the core entirely.

8.3. ISO 20022 Message Schema Requirements

Adherence to the schema is a baseline requirement, but operational excellence requires a strategic approach to data fields.

- **Mandatory Elements & Integrity:** Systems must strictly validate mandatory fields (e.g., Message ID, Creation Date/Time, Business Service) to ensure message integrity. For example, a pacs.002 must accurately reference the original transaction ID to permit automated reconciliation.
- **Strategic Use of Optional Fields:** While not required for validity, optional fields offer significant operational value. Financial institutions should evaluate their capacity to ingest and display extended remittance information or proprietary business codes. Utilizing these fields can drastically reduce manual support queries by providing corporate clients with enriched data for their own cash application and reconciliation processes.

8.4. System Integration Best Practices

Seamless interoperability across the internal technology stack is required to fully leverage the speed of non-value messages.

Core Banking Synchronization

Whether using a Hub or Direct model, the link to the core is critical.

- **Integration Method:** API-based or message queue integrations are recommended over batch processes to ensure real-time account reflection. However, when interacting with the FedNow Service and RTP – messaging/MQ must be utilized. A third-party service provider can help remove that burden from the FIs.³⁰
- **Translation:** Middleware must maintain data fidelity when translating ISO 20022 XML to core-native formats (e.g., fixed-width or COBOL-based structures) to prevent data truncation. When translating, consider the ability to utilize data that may not be easily retrievable.³¹

Fraud and Risk Management

Non-value messages are vital signals for risk systems.

- **Event-Driven Architecture:** Fraud systems should be integrated via event-driven architectures rather than reliance on end-of-day reports.
- **Dynamic Triggers:** Messages such as camt.056 (Cancellation Request) should instantly trigger exception workflows. Real-time ingestion of these messages allows fraud models to update risk scores dynamically based on the success or rejection of related transactions.

Channel Delivery (Mobile & Online)

The value of a non-value message is realized when it reaches the end-user.

- User Experience (UX) Translation: User interfaces must translate technical ISO codes (e.g., "RJCT") into clear, business-friendly language (e.g., "Payment Declined"). Historically the FedNow Service and RTP did not have rules, only recommendations on what this UX should look like. However, RTP now has more firm requirements in this space to be effective from February 1, 2027.³²
- API Exposure: Secure APIs should be available to push status updates to mobile and web channels immediately, reducing call center volume regarding transaction status.

8.5. Performance, Uptime, and Latency

Because non-value messages support the visibility of the payment, their processing speed must align with the payment rail itself.

- Availability: Systems processing these messages should target 99.99% availability or higher. Downtime in status reporting can lead to perceived payment failures and duplicate transaction attempts by customers.
- Latency Standards: End-to-end processing—including validation, translation, and channel delivery—should occur within milliseconds to seconds. Financial institutions must ensure their infrastructure (or their partner's infrastructure) allows for elastic scaling to handle bursts in message volume without latency degradation.
- Monitoring: Continuous performance monitoring and proactive alerting are essential to quickly identify and remediate bottlenecks specifically for non-value message types, which are often overlooked in favor of value-bearing transaction monitoring.

8.6. Vendor and Third-Party Dependencies

For Financial institutions leveraging third-party technology providers for their Payment Hub or connectivity:

- ISO 20022 Readiness: FIs must verify that vendors support the specific maintenance releases and versioning required by networks (e.g., the FedNow Service, RTP).
- SLA Alignment: Service Level Agreements must define distinct metrics for non-value message processing times, independent of funds transfer SLAs.
- Resiliency: Critical third-party systems must have redundancy and failover protocols. Financial institutions are responsible for ensuring their vendors maintain strict data governance and security controls over the message content.

Having walked through the operational, compliance, fraud, and technology dimensions of non-value messaging across RTP and the FedNow Service, a few unifying themes emerge that financial institutions should carry forward as they design and mature their programs. The closing section pulls

Section 9: Conclusion

Non-value messages are a critical part of operating instant and high-value payment rails at scale. While they do not move funds, messages such as Requests for Payment, Requests for Return, and Requests for Information directly impact exception resolution, customer communication, regulatory response, and network trust. How these messages are handled operationally often determines whether issues are resolved efficiently or escalate into customer dissatisfaction and operational risk.

This guide has outlined the key operational considerations financial institutions should address when supporting non-value messaging. These include establishing clear ownership and accountability across operations, technology, and customer support teams; implementing effective monitoring, alerting, and reporting to ensure timely visibility into message flows; and defining consistent, repeatable workflows for investigation, response, and resolution. The guidance also emphasizes the importance of standardization across payment rails, minimizing manual intervention, and ensuring non-value message handling aligns with broader resilience, availability, and compliance requirements.

As payment networks continue to expand their use of non-value messages and introduce new use cases, early preparation is essential. Financial institutions that proactively design and test their operational models — rather than treating non-value messaging as an afterthought — will be better positioned to scale safely, respond to network and regulatory change, and deliver consistent customer experiences.

By addressing these considerations early and embedding non-value message handling into day-to-day operations, institutions can reduce future operational risk, improve efficiency, and ensure they are ready to support the full lifecycle of instant and high-value payments as adoption accelerates.

Thank you to the members of the FPC Operational Considerations for Instant & Immediate Payments Work Group (OCWG) who contributed to this guide.

OCWG Leadership

Form3 US Inc.

Miriam Sheril, Work Group Chair

U.S. Bank

Dustin Martin, Work Group Vice Chair

OCWG Members & Contributors

7T World

Anthony Serio

Alloya Corporate FCU

Lisa Richmond

American Express

Margaret Rae

Corporate One

Martha Dixie

Ebryx

Christopher Kelly

Fincom

Kirsten Lemke

FNBB

Jessica Johnson

Interra Credit Union

Whitney Yoder

JJ4Tech

Caroline Serejo Cypriano

Nacha

Mark Dixon

North American Banking Company

Ryan McNaughton

RedCompass Labs

Stephen King

Thought Machine

Yoav Ash

Wespay

Nathan Carman

About the U.S. Faster Payments Council and the Operational Considerations for Instant & Immediate Payments Work Group

The 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. To further this vision, the Faster Payments Council established the Operational Considerations for Instant & Immediate Payments Work Group to provide financial institutions with guideposts to effectively manage operational changes that instant and immediate payments have on bank operations.

References

- [1] ISO 20022. (n.d.). *ISO 20022 Universal financial industry message scheme*. Retrieved October 16, 2026, from <https://www.iso20022.org/>.
- [2] Note: In FedNow, the camt.029 message is used for multiple response types, including responses to Requests for Information (camt.026) and Requests for Payment Cancellation, to indicate investigation status, information availability, or whether a cancellation request will be honored.
- [3] Network Rule Note: While the FedNow Service does not restrict the types of use cases permitted for Request for Payment (RfP), The Clearing House (TCH) limits RfP messages on the RTP network to specific, defined categories to manage risk and fraud. These authorized applications are governed by the *RTP Rules Interpretation: Permissible Uses for RFPs (Effective April 15, 2025)* (for more information see: https://www.theclearinghouse.org/-/media/New/TCH/Documents/Payment-Systems/RTP_Rules_Interpretation_Permissible_Uses_for_RFPs_effective_April_15_2025.pdf).
- [4][25][26] The Clearing House. (n.d.). *RTP® Rules Interpretation: Permissible Uses for RFPs (Effective April 15, 2025)*. Retrieved October 16, 2026, from https://www.theclearinghouse.org/-/media/New/TCH/Documents/Payment-Systems/RTP_Rules_Interpretation_Permissible_Uses_for_RFPs_effective_April_15_2025.pdf?rev=921ffabef8d240ef868887a12f19efaf&hash=5074E7C4D3F86EAA8CF3CDB147A895E7.
- [5] The Clearing House. (n.d.). *Always Ready. The RTP® Network, Trusted by Financial Institutions Nationwide*. Retrieved October 16, 2026, from <https://www.theclearinghouse.org/payment-systems/ntp>.
- [6] The Federal Reserve Financial Services. (n.d.). *Operating Circulars*. Retrieved October 16, 2026, from <https://www.frbfinancialservices.org/resources/rules-regulations/operating-circulars.html>.
- [7] eCFR. (n.d.). *12 CFR Part 1005 – Electronic Fund Transfers (Regulation E)*. Retrieved October 16, 2026, from <https://www.ecfr.gov/current/title-12/chapter-X/part-1005>.
- [8] Federal Trade Commission. (n.d.). *Gramm-Leach-Bliley Act*. Retrieved October 16, 2026, from <https://www.ftc.gov/legal-library/browse/statutes/gramm-leach-bliley-act>.
- [9] California Privacy Protection Agency. (n.d.). *Regulations*. Retrieved October 16, 2026, from <https://coppa.ca.gov/regulations/>.
- [10] U.S. Department of the Treasury. (n.d.). *Sanctions List Service*. Retrieved October 16, 2026, from <https://ofac.treasury.gov/sanctions-list-service>.
- [11] FinCEN. (n.d.). *The Bank Secrecy Act*. Retrieved October 16, 2026, from <https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act>.
- [12] FinCEN. (n.d.). *Filing Information*. Retrieved October 16, 2026, from <https://www.fincen.gov/resources/filing-information>.
- [13] FedPayments Improvement. (2026, April 22). *Federal Reserve Releases Account Takeover Fraud Mitigation Toolkit and Enhancements to Existing Toolkits*. <https://fedpaymentsimprovement.org/news/blog/federal-reserve-releases-account-takeover-fraud-mitigation-toolkit-and-enhancements-to-existing-toolkits/>.
- [14][15][18] Faster Payments Council. (2026, May 15). *Instant Payments Fraud Dispute Resolution: Guiding Principles for the U.S.* <https://fasterpaymentscouncil.org/blog/17138/Instant-Payments-Fraud-Dispute-Resolution-Guiding-Principles-for-the-U-S-Report>.

- [16] Faster Payments Council. (2025, January). *Guideline.02: Operational Considerations for Instant Payments Send-Side Primer*. https://fasterpaymentscouncil.org/userfiles/2080/files/OCWG_Operational%20Considerations%20for%20Instant%20Payments%20Send%20Side%20Primer_01-13-2025%20Final.pdf; and (2023, October). *Guideline.01: Operational Considerations for Instant Payments Receive-Side Primer*. <https://fasterpaymentscouncil.org/blog/12405/Operational-Considerations-for-Instant-Payments-Receive-Side-Primer>.
- [17] Note: These alphanumeric reason codes are derived from the global ISO 20022 External Code List for payment cancellation and return reasons, as operationalized within the *Federal Reserve Financial Services FedNow ISO 20022 Implementation Guidelines* and *The Clearing House RTP Technical Specifications*.
- [19] Note: A similar participant-profile consideration applies to Request for Payment. Although an institution may be able to receive an RfP on behalf of its customer, fulfilling the request requires the institution to have the capability to send the corresponding payment over the applicable network.
- [20] eCFR. (n.d.). *12 CFR Part 1026 – Truth in Lending (Regulation Z)*. Retrieved October 16, 2026, from <https://www.ecfr.gov/current/title-12/chapter-X/part-1026>.
- [21] FFIEC. (n.d.). *BSA/AML Examination Manual: Assessing Compliance with BSA Regulatory Requirements*. Retrieved October 19, 2026, from https://bsaaml.ffiec.gov/manual/AssessingComplianceWithBSARegulatoryRequirements/01_ep.
- [22] FFIEC. (n.d.). *BSA/AML Examination Manual: Office of Foreign Assets Control*. Retrieved October 16, 2026, from <https://bsaaml.ffiec.gov/manual/OfficeOfForeignAssetsControl/01>.
- [23] ISO 20022. (n.d.). *Message Definitions: Payments Clearing and Settlement (pacs)*. Retrieved October 16, 2026, from <https://www.iso20022.org/advanced-search#q=message%20types%20pacs>.
- [24] The Federal Reserve Financial Services. (2025, June). *FedNow® Service Operating Procedures*. <https://frbervices.org/binaries/content/assets/crsocms/resources/rules-regulations/062425-fednow-service-operating-procedures.pdf>.
- [27] Note: For FedNow, return requests used to report fraud or an RfP warranty breach are not subject to the 60-day guideline.
- [28] Uniform Law Commission. (n.d.). *Uniform Commercial Code*. Retrieved October 16, 2026, from <https://www.uniformlaws.org/acts/ucc>.
- [29] U.S. Department of the Treasury. (n.d.). *Office of Foreign Assets Control*. Retrieved October 16, 2026, from <https://ofac.treasury.gov/>.
- [30] Faster Payments Council. (2023, October). *Guideline.01: Operational Considerations for Instant Payments Receive-Side Primer*. https://fasterpaymentscouncil.org/userfiles/2080/files/Operational%20Considerations%20for%20Instant%20Payments%20Guideline_10-11-2023_Final.pdf#:~:text=As%20such%2C%20this%20document%20serves%20as%20a,Processes%20for%20Reconciling%20Incoming%20Funds%20in%20Real%2DTime.
- [31] StoneX. (n.d.). *What is ISO 20022?* Retrieved October 16, 2026, from <https://www.stonex.com/en/business/financial-glossary/iso-20022/>.
- [32] The Clearing House. (n.d.). *RTP® Network*. Retrieved October 16, 2026, from <https://www.theclearinghouse.org/payment-systems/rtp/document-library>.