Operational Considerations for Instant Payments Send-Side Guidelines

Fasterpaymentscouncil.org

September 2025

Table of Contents

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.

This document was not prepared by The Clearing House Payments Company LLC. The Clearing House is not responsible for inaccuracies about the RTP® network, applicable laws, and regulations relevant to instant payments, or payment systems in general.

Introduction

The rapid evolution of instant payments in the U.S. has ushered in a new era of instant transaction capabilities for financial institutions (FIs). With the launch of FedNow® service alongside the existing RTP® network, institutions now have unprecedented opportunities to enhance payment experience for their accountholders. However, sending payments across these networks introduces new complexities that must be carefully managed. Unlike traditional payment rails, FedNow and RTP operate independently, meaning they do not interoperate. This lack of interoperability presents financial institutions with both a challenge and an opportunity— successfully implementing a strategy requires a thoughtful approach that enables seamless utilization of both networks while optimizing operational efficiency.

To take full advantage of instant payments, institutions must consider several critical factors, including liquidity management, reconciliation processes, fraud mitigation, and compliance. Liquidity management is essential, as funds must be readily available in separate accounts for each network to facilitate real-time settlement. Reconciliation processes must also be adapted to manage 24x7x365 transactions with immediate finality, requiring institutions to modernize their back-end operations. Without proper planning, institutions risk inefficiencies, increased operational costs, and potential accountholder dissatisfaction.

These guidelines provide a deep dive into all the operational considerations financial institutions must address when implementing send capabilities for instant payments[1]. It explores the strategic decisions necessary to ensure seamless adoption of the FedNow service and the RTP network, including how to balance liquidity, optimize reconciliation, and manage risk in an environment where payments clear within seconds. By taking a comprehensive approach, institutions can not only navigate the complexities of these networks but also unlock the full potential of instant payments to drive innovation, efficiency, and accountholder satisfaction.

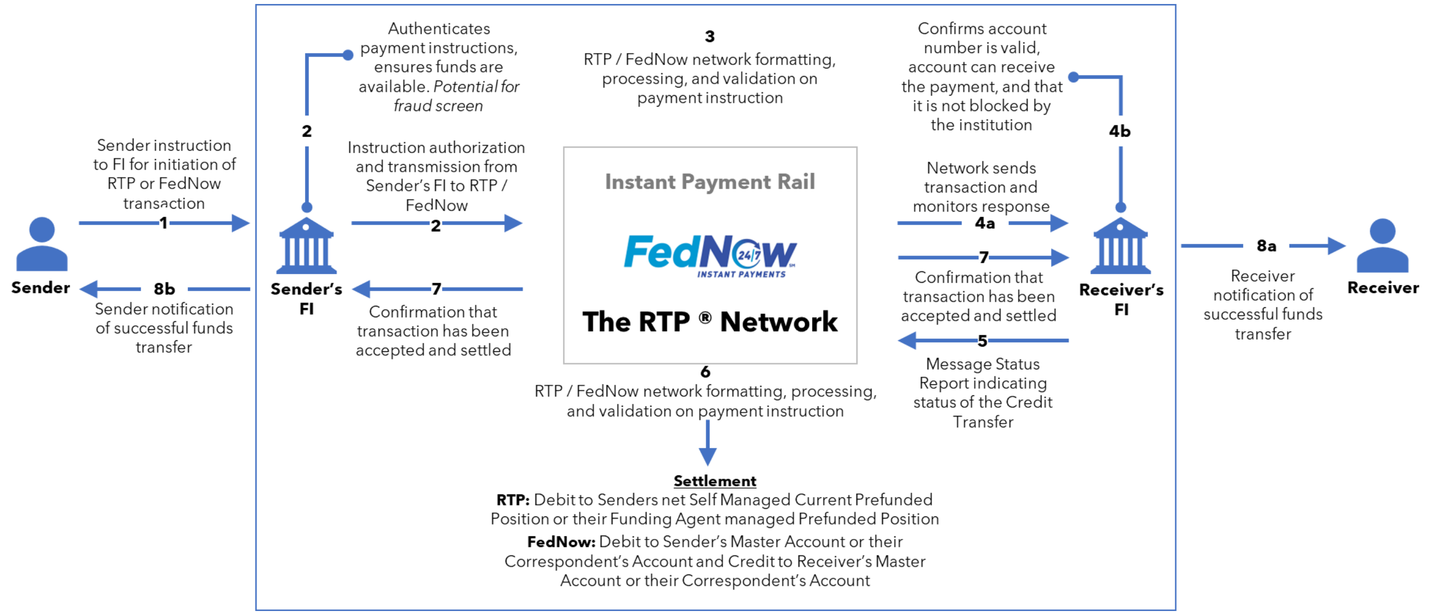
1) Instant Payment Send Flow

With the inception of instant payments, it is key for financial institutions to understand how messages and money are exchanged within the instant payments schemes and how this differs from traditional rails such as the Automated Clearing House (ACH) and wire transfers. ACH payments are electronic transfers through the ACH network that may take several days to settle, or if processed as Same Day ACH, can settle as quickly as a few hours. Wire transfers can take anywhere from a few minutes to more than twenty-four hours to settle with the end party depending on the financial institutions involved in the transaction. Both ACH and wire transfers are one-way communication where the originating institution initiates an ACH file or initiates a wire payment but does not receive confirmation that the receiver's account was credited.

Unlike ACH and wire payments, the RTP Network and the FedNow Service require an immediate response from the receiver's financial institution confirming its decision to either Accept, Reject, or Accept without Posting. This core feature provides payment certainty to both financial institutions as well as the sender and receiver of the transaction.

Each payment rail provides the opportunity for the receiver's financial institution to reject a payment for distinct reasons. However, the instant payment rail supports an automated, immediate rejection prior to settlement, whereas ACH and wires can only accommodate rejection as a manual review that results in a return sent through the network after settlement has occurred. This immediate rejection allows sending institutions to review rejected payments and respond quickly, including communicating with senders, correcting errors, and resending payments.

Successful Instant Payment Flow


Authenticates payment instructions, ensures funds are available. Potential for fraud screen
3
RTP / FedNow network formatting, processing, and validation on payment instruction
Confirms account number is valid, account can receive the payment, and that it is not blocked by the institution
2
4b
Sender instruction to FI for initiation of RTP or FedNow transaction
1
Instruction authorization and transmission from Sender's FI to RTP / FedNow
2
Instant Payment Rail
FedNow INSTANT PAYMENTS
The RTP ® Network
Network sends transaction and monitors response
4a
7
Confirmation that transaction has been accepted and settled
5
Message Status Report indicating status of the Credit Transfer
8a
Receiver notification of successful funds transfer
Sender
8b
Sender notification of successful funds transfer
Sender's FI
7
Confirmation that transaction has been accepted and settled
Receiver's FI
Receiver
6
RTP / FedNow network formatting, processing, and validation on payment instruction
Settlement
RTP: Debit to Senders net Self Managed Current Prefunded Position or their Funding Agent managed Prefunded Position
FedNow: Debit to Sender's Master Account or their Correspondent's Account and Credit to Receiver's Master Account or their Correspondent's Account

This section will point out considerations for sending financial institutions throughout the process flows but will not provide the level of detail that was covered for receiving financial institutions in the Operational Considerations for Receiving Instant Payments Guidelines.[2]

1. The sender (an individual, business, or government entity) initiates payment with their financial institution (FI), who is a participant in the instant payment network, through an interface provided by the financial institution or third-party provider such as an online or mobile banking application. When building out user experiences for the senders to create payment transactions FIs may include functionality (i.e., directories) that will validate the payment instructions match the intended payee. This will be covered in more detail in the User Experience section of this document.

2. The sender's financial institution authenticates the sender, the senders' payment instructions, ensures funds are available to cover the payment and sends a credit transfer message (ISO 20022 message pacs.008) to the payment network. Sending financial institutions will need to consider what actions will be taken and messaging presented to senders in cases where funds are not available to cover the transaction, when a transaction exceeds the senders approved limits, or when fraud screening has flagged a transaction for additional review. Options for inserting these risk mitigation techniques into the payment flow and for managing these exception cases will be covered in more detail in other sections of this document.

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 (pacs.008 message). Some of those validations include:
    - The message is properly formatted and not future-dated.
    - The routing number belongs to a network participant.

4. A) The network sends the transaction to the receiver's financial institution and monitors for a response.

    B) The receiver's financial institution then receives the Credit Transfer message (ISO 20022 message pacs.008) from the network and conducts several of its own validations to ensure its correctness and security. Currently, the response must come back within the respective network's timeout clock, including processing time, any sanctions/fraud related activities, and check on account number validity. Financial institutions that have chosen to perform screening of incoming payment messages, such as for fraud or OFAC, will need to consider how to react to messages that have generated an alert. The financial institution may choose to respond to the incoming message with the "accept without posting" response which would instruct the network to settle the payment between the banks, but not to the receivers account, and allow the financial institution additional time to review the alert and make a final determination to reject the payment or make funds available to the receiver. During this review time, the sender could utilize network functionality to request information on the payment status. Operational considerations for managing these exceptions, including systems and staffing, will be discussed in more detail in the Exception Processing section of this document.

5. Once the message is validated, the receiver's financial institution sends the network a Message Status Report (ISO 20022 message pacs.002) indicating the credit transfer has either been accepted, accepted without posting, or rejected.

6. The network will receive a confirmation Message Status Report (ISO 20022 message pacs.002) from the receiver's financial institution that it has accepted the payment. The network will again perform a series of formatting, process, and business rule validations. Upon completion of validation, the network will process a debit from the sender's financial institution and credit the receiver's financial institution except in the instance of a rejected response. For the RTP network, this will be using the joint account[3] held by the Clearing House at the Federal Reserve where credits and debits process against the RTP ledger. For FedNow, this will be the sender's and receiver's Master Account at a Reserve Bank that the FedNow participant uses to settle obligations that arise in connection with FedNow Service. In both networks, settlement could occur through Funding Agents[4]/correspondent bank (i.e., banker's bank or corporate credit union) and not through the financial institution's accounts. Settlement and funding considerations will be discussed in detail later in this document.

7. The network sends confirmation to the sender's financial institution indicating that the transaction has been accepted or accepted without posting and settled or rejected.

8. A) If the payment has been accepted the receiver's financial institution immediately posts the funds to the receiver's account and makes the information contained in the payment available to the receiver using the financial institution's channel application.

   B) When confirmation of acceptance or rejection of the message is received from the network, the sender's financial institution can notify the sender of the status of the payment. If the payment has been rejected the Sending FI could provide the reason for the rejection based on the code received from the Receiving FI. Senders could then use this information to correct the error and reinitiate the payment. If the payment has been accepted without posting, the Sender may be presented with options to request information to determine if the payment has ultimately been posted or it will be rejected and returned to the Sender. The Sending FI should also consider whether it will automatically request updates on the status of the payment and the frequency for these requests. Any update received will need to be communicated to the Sender.

2) Interoperability and Routing Considerations

Interoperability Models

Integration at the Network Level:

Currently, the FedNow service and the RTP network operate as separate networks with no direct interoperability, requiring financial institutions to implement custom routing solutions. In contrast, the ACH Network has long had full interoperability across operators, allowing seamless ACH transactions between networks. For instant payments, interoperability is not natively built-in, and financial institutions must develop their own strategies to enable cross-network transactions.

A key challenge in FedNow and RTP interoperability is the lack of a shared routing framework and centralized messaging standard. While both use ISO 20022, differences in governance, operations, and message handling require financial institutions to develop independent routing logic, leveraging network directories and third-party providers. Additionally, FedNow settles in real-time via master accounts, while RTP relies on pre-funded balances, making liquidity management and reconciliation more complex. To address this, institutions that implement the RTP network and the FedNow service should consider deploying a unified payment orchestration layer with API gateways to translate ISO 20022 messages and intelligent failover mechanisms to reroute payments during network downtime, congestion, or participant unavailability.

Routing Interoperability Model

A routing interoperability model enables financial institutions to connect to both the FedNow service and the RTP network, allowing payments to be sent and received through either network based on predefined rules. This approach enhances flexibility, optimizing costs, speed, and transaction limits while ensuring seamless processing across networks.

To implement this model effectively, financial institutions should:

- Monitor networks in real-time to track the availability and performance of FedNow and RTP.
- Develop dynamic routing logic that accounts for transaction amounts, network fees, recipient financial institution availability, and real-time conditions.
- Maintain updated network directories to ensure accurate routing decisions across both networks.
- Implement automated failover mechanisms to switch networks in case of downtime or congestion, minimizing disruptions.

By adopting these strategies, financial institutions can enhance payment reliability, reduce processing costs, and improve the accountholder experience across instant payment networks.

Accountholder Interface Design for Interoperability

To ensure interoperability, FIs could consider designing an accountholder-facing user interface that allows accountholders to utilize either or both instant payment networks, however, seamless routing not depending on the user to know the rails would likely be more appropriate. The interface could be designed to provide users with real-time feedback on the availability of both the RTP network and FedNow service, as well as network status, which will empower the accountholder to make an informed decision about which network to use. However, for optimal accountholder experience, the interface could build in all technical components and seamlessly route payments without requiring users to be aware of the underlying network used.

Additionally, institutions should consider implementing user-configurable preferences, allowing accountholders to prioritize factors such as speed, cost, or preferred network, ensuring a personalized and efficient payment experience.

Back-Office Systems for Multi-Network Support

For back-office systems, financial institutions should design their infrastructure to support both the FedNow service and the RTP network simultaneously. This includes integrating transaction management systems, compliance monitoring tools, and reporting frameworks that can manage both instant payments and settlement requirements for both networks. In addition, financial institutions should work with TPSPs to help simplify the integration process, standardize payment messages, and offer seamless payment settlement across different instant payment networks. To enhance operational efficiency, institutions should also implement automated exception handling and liquidity management tools that proactively monitor funding levels and prevent transaction failures.

Third-Party Service Providers

There are several third-party service providers (i.e., RTP TPSP and FedNow Service Providers) in the market that facilitate interoperability, offering services such as network routing, payment settlement, and standardization of messages. These providers typically offer a single set of APIs or integration platforms that FIs can leverage to route payments to either the RTP network or the FedNow service, reducing the burden of direct integration and ensuring that they can support both networks concurrently. By using a third-party service provider, FIs can simplify the operational complexity of managing connections with multiple instant payment networks. Financial institutions should evaluate TPSPs based on uptime reliability, API response times, and scalability to manage increased transaction volumes.

Routing Rule Drivers

There are several factors to consider when determining how and when to route instant payments across the FedNow Service and RTP network, including:

Financial Institution Availability: The availability of a financial institution on either RTP or FedNow is a critical factor for ensuring that payments are successfully delivered. An FI must be an active participant on both networks to send or receive transactions from both networks. To maximize the success rates of instant payments, FIs must have access to comprehensive and up-to-date directories to identify which FIs can receive payments on either network.

- FedNow Participant Status/Directory: The Federal Reserve's FedNow directory provides a daily list of participant Fis including RTNs, reflecting their capabilities (e.g., receiving customer credit transfers, sending, and receiving credit transfers, or receiving requests for payment). Financial institutions can use this data to determine the most appropriate network for sending or receiving payments, ensuring that transactions are sent to compatible endpoints. FedNow also utilizes a Broadcast Message (Admi.004) to provide real-time status updates, including if an institution is no longer available, or has signed back on to the network.

- RTP Participant Status/Directory: Similarly, The Clearing House (TCH) offers a directory for the RTP network, which includes Routing Transit Numbers (RTNs) for receiving FIs. These directories are updated regularly, enabling financial institutions to validate and confirm whether a given FI can receive payments. RTP also provides intraday updates on participant statuses, but through System Notification Messages (the same admi.004).

Network Fees: Financial institutions must thoroughly evaluate the fee structures of both the FedNow service and the RTP network when setting routing rules for transactions. Key considerations include:

- Per-Transaction Fees: Both networks charge per-transaction fees, which vary based on type of transaction [e.g., request for payment (RfP)]. FIs must determine which network offers the most competitive fees based on their transaction volumes and cost structure.

- Volume-Based Pricing: Volume-based pricing could make one network more favorable than the other for high-volume transactions, as FIs may receive discounts or more favorable terms based on their usage.

- Other Network Fees: In addition to per-transaction fees, FIs should account for any overhead or additional costs associated with network access, settlement, and third-party service providers (e.g., fraud, sanctions etc.).

Dollar Limitations at the Network Level: RTP and FedNow have different transaction dollar limits that FIs must consider when determining routing preferences:

- FedNow Service: The transaction limit per payment is $1,000,000.[5]
- RTP Network: The transaction limit per payment is $10,000,000.[6]

FIs should design routing rules to ensure high-value transactions are directed to the appropriate network, avoiding failed payments due to exceeding network limits.

Financial Institution Preference:

FIs will often develop their routing preferences based on factors such as:

- Business Strategy: Some FIs may prefer to use a specific network due to existing relationships with the network operator or due to strategic initiatives (e.g., focusing on certain market segments). For instance, an FI that has invested more heavily in instant payment integration may prefer to prioritize instant payment transactions unless other factors outweigh this preference

- Technical Capability: FIs' internal systems may be optimized for one network over the other.

- Accountholder Demand: If accountholders frequently use one network over the other, FIs may choose to route payments through that network for an enhanced user experience.

- Liquidity needs: FIs' may route based on liquidity need between the RTP network joint account and federal reserve master account – as well as around the availability of Fedwire.

Contingency Planning – Alternative Payment Methods

When Instant Payments Are Unavailable

If both the RTP network and the FedNow service are unavailable due to system maintenance, network congestion, or technical failures, financial institutions must have fallback options to ensure continuity. The two primary alternatives are ACH and wire transfers, each with distinct advantages and limitations.

Automated Clearing House:

- Advantages of ACH: ACH is a widely adopted alternative with minimal dollar limitations and lower fees. It is particularly valuable for recurring payments or when a cost-efficient solution is required for non-time-sensitive payments. Same Day ACH enables faster settlement compared to standard ACH, allowing many payments to settle within hours on the same business day, thereby narrowing the gap between ACH and instant payment networks.

- Challenges of ACH: However, ACH is a deferred net settlement system, meaning that it does not offer instant capabilities like the RTP network or the FedNow service. Transactions are settled in batches, which can result in slower processing times (typically within one to two business days). Additionally, ACH does not support 24x7x365 operations and may be unsuitable for urgent payments or time-sensitive use cases.

- Use Cases for ACH Fallback: ACH is a viable fallback when time is not of the essence—such as for payroll processing, bill payments, or large batch payments. However, ACH may not be suitable for cases requiring real-time payment confirmation, such as in-person retail transactions or emergency fund transfers.

Wire Transfers:

- Advantages of Wire Transfers: Wire transfers provide faster settlement than ACH, often clearing within hours and sometimes within minutes, especially for domestic transactions. They are also widely available for high-value transactions.

- Challenges of Wire Transfers: Wire transfers come with higher fees compared to ACH or instant payment networks and are generally not available 24x7x365. Furthermore, they do not have the same automation capabilities, which could complicate accountholder experience.

- Use Cases for Wire Fallback: Wire transfers are ideal for high-value transactions or when the urgency of settlement outweighs the cost. They are particularly useful for international payments where other networks may not be available.

Decision-Making for Fallback Options

When selecting a fallback method, financial institutions should assess transaction size, urgency, cost sensitivity, and accountholder expectations:

- For instant payments requiring immediate confirmation (e.g., emergency fund transfers) → Wire transfers are preferable despite higher costs.
- For larger, non-urgent payments → ACH is a more practical choice due to lower fees.

By proactively integrating contingency plans, financial institutions can ensure uninterrupted payment processing and minimize disruptions when instant payment networks are unavailable.

Future of the RTP Network and the FedNow Service Interoperability

As instant payments continue to evolve, achieving full interoperability between RTP and FedNow will be desirable for enhancing efficiency, reducing fragmentation, and expanding adoption across financial institutions. While current interoperability relies on custom routing logic and third-party service providers, future developments could include standardized routing frameworks, direct network integration, and regulatory initiatives to facilitate seamless cross-network transactions. Advancements in API standardization, liquidity management, and settlement mechanisms will further improve transaction processing, ensuring a more unified and resilient instant payments ecosystem. Financial institutions should proactively monitor these developments and adapt their infrastructure to remain competitive in the evolving payments landscape.

3) User Experience & User Interface – Instant Payments Application

Accountholder User Experience & User Interface

The send side demands a streamlined and user-friendly interface to facilitate quick and seamless payment initiation. Since account holding users actively engage with the payment system to initiate transactions, the user experience (UX) and user interface (UI) for send-side processes must be highly intuitive and optimized for different channels, such as mobile and web applications. This is less critical on the receive side, where end-users are often passive recipients of funds.
Unsuccessful payments can lead to accountholder frustration and reputational risks for financial institutions. To mitigate this, institutions should utilize accountholder dashboards and establish proper alert systems for failed transactions. These tools enable real-time visibility into payment statuses and facilitate prompt resolution of issues.

Further, security is a top concern for both accountholders and financial institutions in instant payments. While robust security measures protect users from fraud and unauthorized transactions, poor UX/UI design can make security features feel intrusive, confusing, or intimidating. The key to an effective send payments experience is clear, reassuring communication about security, explaining safeguards in a way that builds trust without causing unnecessary friction. While some friction will be necessary to create "speed bumps" for users to confirm their payments.

The Business Case for Clear Security Communication: Improving security communication is not just about compliance. It directly impacts accountholder retention, trust, and fraud prevention. Business benefits are as follows:

- Reduced Transaction Abandonment: When security steps feel natural, user's complete transactions instead of dropping off.
- Increased Trust & Engagement: Accountholders are more likely to use instant payments if they feel protected.
- Lower Support Costs: Clear messaging prevents unnecessary accountholder service calls.
- Stronger Fraud Prevention: Educated users are less likely to fall for scams when security guidance is proactive.

Operational Staff User Experience & User Interface

While accountholder experience is critical, the UX/UI for financial institution staff is equally important for managing instant payment workflows effectively. Instant payments introduce new operational challenges in which transactions are final, require immediate reconciliation, fraud review, and demand instant exception handling. A well-designed operational interface ensures that FI staff can monitor payments in real-time, identify and resolve issues quickly, and maintain regulatory compliance without friction.

Dashboard Design for Instant Payment Oversight: Operational teams need clear, real-time data to track payments, manage exceptions, and ensure compliance. A cluttered or delayed dashboard can slow response times and increase error rates. We recommend the following dashboard components:

- Real-Time Transaction Monitoring: Show live payment statuses (e.g., "Processing," "Completed," "Failed"). Use special designation alerts for flagged transactions that require intervention. For example, use a red warning icon for failed transactions, a green checkmark for successful payments.

- High-Priority Alerts & Notifications: Display critical alerts at the top (e.g., fraud flags, missing compliance checks). Allow customizable thresholds so that staff sees only the most relevant alerts. For example, use "5 high-risk transactions need review" with a one-click action button.

- Customizable Views & Filters: Let staff filter transactions by payment type, risk level, accountholder segment, or processing status. Support saved filters for frequently used views. For example, a fraud analyst may need to see only high-value payments flagged as risky.

- Search & Quick Lookup Features: Enable instant search by transaction ID, accountholder name, or account number. Provide autocomplete suggestions to speed up queries.

- Data Visualization for Quick Insights: Use graphical summaries (e.g., transaction trends over time, success vs. failure rates). For example, a heatmap showing peak transaction hours may help with staffing decisions. A well-designed operational dashboard reduces response times, improves staff productivity, and prevents errors before they escalate.

Streamlining Workflows for Faster Exception Handling: Staff interfaces should enable quick decisions and automate routine tasks. By simplifying workflows and automating routine tasks, FI staff can manage exceptions faster, reduce operational risk, and improve overall payment system reliability.

- Predefined Templates for Common Actions: Provide one-click actions for frequent tasks like resending failed payments, reversing incorrect transactions (where possible), or escalating issues. Example: A pre-configured “Retry Payment” button with automated checks before submission.

- Guided Workflows for Error Resolution: For complex issues, offer step-by-step guided workflows. Example: A "Failed Payment Resolution" wizard that walks staff through possible fixes based on error codes.

- AI-Powered Recommendations: Use AI-driven insights to suggest next steps based on transaction history and risk patterns. Example: “This failed transaction was due to an expired recipient account. Would you like to contact the sender for an updated account number?”

- Integrated Support & Documentation: Embed helpful tooltips explaining technical error codes. Provide quick access to accountholder service scripts for resolving user issues. Example: Clicking on a failed payment shows "Possible Cause: Recipient account closed. Recommended Action: Contact sender to update details."

- Role-Based Access Control: Ensure staff only see data relevant to their role (e.g., compliance officers see regulatory flags, payment processors see transaction statuses). Example: A fraud analyst dashboard hides operational payment routing details but highlights suspicious activity.

Unified Payment Operations for Instant Payments: With multiple payment rails available, operational staff should not have to juggle multiple platforms. A unified operational interface reduces confusion, training costs, and processing delays while increasing staff efficiency. Please reference Section 2) Interoperability & Routing Considerations for more details on designing and maintaining interoperability of payment rails. Design considerations & recommendations for an interoperable environment include:

- Consolidated Payment Dashboard: Show all transactions across different payment rails in one place. Example: Instead of separate tabs for RTP and FedNow, display them under a unified "Instant Payments" view.

- Visual Distinctions for Different Rails: Use a special designation or tags to differentiate RTP, FedNow, and alternative payment methods.

- Cross-Rail Exception Handling: Provide standardized workflows for troubleshooting across different payment types. Example: An RTP error and a FedNow error should have similar resolution processes instead of requiring different interfaces.

- Consistent Data Fields & Terminology: Ensure payment entry fields remain the same regardless of payment rail. Example: Keep "Recipient Account" and "Bank Routing" fields uniform across all instant payment options.

- Comparisons to Show Payment Speed & Costs: Accountholders may not understand the differences between payment rails. A side-by-side comparison chart makes these distinctions clearer. Best Practice: Highlight the most relevant details (speed, cost, reversibility) without overloading users with technical terms.

4) Liquidity Management

Liquidity management is a crucial component of participating in instant payment systems. The instantaneous nature of these systems means that financial institutions must ensure that they always have adequate liquidity available to settle transactions without delays. Instant payments require a system of liquidity management that is responsive, efficient, and secure. This section will explore the different components that make up an effective liquidity management strategy for these payment networks, including alerting and monitoring, effective forecasting, and a recap of liquidity tools like watermarks, funding strategies, and options for utilizing correspondent banks or Funding Agents.

Network Level Liquidity[7]**:** Specifically, when it comes to sending instant payments, liquidity management becomes even more important and needs to be managed differently in the RTP network versus the FedNow service. To send transactions, FI's must ensure they have enough liquidity to initiate the payments. For the RTP network this means that the FI must ensure they meet the prefunded position required by the RTP network based on their asset size and other factors. To do this they must fund using the joint account that the Federal Reserve Bank of NY has for TCH. They also must manage their liquidity level using alerts and notifications from the RTP network. These alerts are intended for when they are getting close to their limit or when they are getting an influx of liquidity allowing them to both fund and defund their account as needed. In some cases, a participant may be a non-funding participant and may use a Funding Manager[8]. In those cases, the Funding Manager must manage and ensure the participant leveraging them has enough liquidity to manage their transactions.

The FedNow service settles via the FI's master account or leverages a correspondent banks master account. Managing the liquidity in the master account is managed via the accounting services at the Federal Reserve. FedNow does offer an account balance report both in ISO and on the FedNow user interface to support financial institutions managing their liquidity and ensuring they do not have any credit risk. The correspondents who may offer their liquidity to FedNow participants, have additional reports and notifications that FedNow may send them allowing them to manage and monitor the liquidity being used by the respondents. Correspondents can also take advantage of FedNow's Correspondent Net Send Limit control which enables correspondents to manage exposure from their respondents' activity and better manage their master account balances.

In addition, both the RTP network and the FedNow service offer the ability to transfer funds between FIs for the purpose of liquidity management. Where one FI may need to ask another FI for liquidity support. The pacs.009 message is used by both systems to support this. FedNow provides a Liquidity Management Tool (LMT) which financial institutions can leverage it in support of liquidity needs associated with instant payment activity, including supporting the funding/defunding through the joint account for the RTP network.

Financial Institution Liquidity Management: For Funding Managers/Agents and correspondent banks, one big consideration is how to manage the liquidity that their accountholders are utilizing. Due to the nature of these rails, the money is credited and debited from the account of the Funding Manager/Agent or correspondent. Therefore, managing liquidity becomes a more difficult prospect. Both systems offer diverse ways for the funders to manage this. The RTP network offers messaging and API access that allows for notification of the payments and for the Funding Managers to manage specific pools of liquidity for each of their accountholders who utilize the service. FedNow offers a camt.054 message which allows for a notification of each credit or debit to go to the correspondent. FedNow also offers correspondents the ability to set net send limits which are limits on the total dollar amount of payments, less any funds received that can be set at the respondent financial level, allowing the correspondent additional management of their Federal Reserve master account balance and credit exposure from respondents' activity. For Funding Providers to take advantage of these various functionalities, they would need to build out solutions on their end to utilize these solutions and automate the management of settlement/posting to their accountholders.

Internal Alerts and Monitoring: Instant payment transactions demand immediate action and precise control over available funds. To ensure smooth operations, internal alerts and monitoring systems are essential. By leveraging API's, FIs can continuously track account balances, providing an up-to-date view of liquidity at any given moment. These systems should be configured to trigger notifications for potential issues, enabling the right employees to act swiftly and prevent disruptions. To maintain responsiveness, these alerts must be monitored around the clock. It is essential that FI's have escalation procedures established and documented to resolve any issues as quickly as possible. This includes understanding what to do when certain alerts are received as well as who needs to be notified to resolve the issue. Another important aspect to monitor would be anomalous send activity which could require prompt attention and the ability to instantly sign off the network if an issue arises.

Forecasting: Forecasting instant payments requires a comprehensive approach to predict account activity and funding levels, with a particular focus on several key periods that may impact liquidity. A multiple-day view is essential to assess trends and anticipate needs, especially during periods like three-day weekends, holidays, year-end, and quarter end, when payment volumes can fluctuate significantly. These times demand careful attention, as they can introduce delays or surges in transaction activity which may require a financial institution to increase the funds held in their account to cover the instant payment needs. It is important to understand both anticipated send and receive volume as both aspects are critical to understanding funding requirements and liquidity needs. Additionally, as a financial institution enables use cases, they should understand their accountholders' potential volume and dollar amounts, how frequently they plan to send, so that information can be incorporated into liquidity management forecasting. Last, institutions should also be aware of and carefully plan around wire transfer hours to ensure funding can take place when needed.

Prefunding: As mentioned in the Send Primer[9], understanding funding requirements and how each network operates is essential. When participating in the RTP Network, FIs are required to prefund their RTP account via the joint account to facilitate real-time settlement of transactions. The FedNow service does not require prefunding as existing Master Accounts are used to settle FedNow transactions. The Clearing House determines prefunding requirements based on tiers structured around U.S. transaction deposit ranges for each FI. This prefunding ensures that funds are immediately available for settlement when transactions occur. Transactions will be processed if funds are in the joint account, however, if the transaction brings the account below zero, the transaction(s) will be rejected.

Watermarks: To help FIs manage their liquidity and funding requirements, The RTP network offers watermarks. Participants can set specific watermark values based on their needs and when they want to be alerted that their funding is low and requires attention.

Liquidity Management Transfer: FedNow offers a service called Liquidity Management Transfers (LMT), which enables FIs to send funds to each other, either directly or through service providers, to support their instant payment liquidity needs. LMTs are available from 7 PM ET to 7 AM ET on weekdays and 24 hours a day on weekends and Federal Reserve holidays (intended to cover the gap with Fedwire hours.)

Funding Agents/Correspondent Accounts for Enhanced Liquidity Management: Another tool or option available to financial institutions is utilizing Funding Agents or correspondent banks to help manage and meet their liquidity needs.

Managing liquidity is not new for financial institutions, and in many cases, FIs can leverage the tools and resources already in use today. Where instant payments differ is in their 24x7x365 nature, which requires sufficient liquidity management to be in place overnight and on weekends.

5) Real-Time Reconciliation for Outgoing Funds

Instant payments have become a transformative force in the global financial landscape, facilitating instantaneous transfer of funds between entities. As financial institutions increasingly adopt instant payments send capabilities to meet accountholder demands for speed and convenience, the importance of robust real-time reconciliation practices for outgoing funds has grown.

Automated real-time reconciliation of outgoing funds offers significant advantages over traditional batch reconciliation by providing immediate visibility into transaction statuses and cash positions. This real-time insight enables faster identification and resolution of errors, reduces the risk of fraud, and enhances liquidity management. For example, real-time reconciliation increases liquidity visibility and an organization's ability to capitalize on liquidity opportunities. Unlike batch processes that delay updates until end-of-day cycles, real-time reconciliation supports more accurate forecasting and decision-making, ultimately improving operational efficiency and strengthening financial control.

Real-time reconciliation ensures that outgoing transactions are accurately tracked, balanced, and compliant with regulations as they happen. The objectives of real-time reconciliation include ensuring accuracy, maintaining speed and efficiency, providing transparency into financial movements, and adhering to regulatory requirements. With rapid transaction processing, managing outgoing funds in real-time is crucial to minimizing errors, preventing fraud, and ensuring liquidity.

Core Components of Real-Time Reconciliation

Instant Data Management: Central to the success of real-time reconciliation is the ability to capture and process data instantaneously. With the dynamic nature of instant payments, outgoing funds must be reflected in ledgers and transaction records as soon as they are initiated. This ensures financial positions are always up to date, reducing the risk of discrepancies and ensuring transparency. Maintaining an accurate ledger is fundamental. A delay in recording transactions can lead to mismatches between actual and reported balances, resulting in operational risks or compliance failures.

Automation and Efficiency: Automation plays a key role in ensuring real-time reconciliation is both efficient and accurate. Automated systems reduce the need for manual interventions, which can introduce human errors and cause delays. Through instant synchronization of ledgers and accounts, financial institutions can ensure that outgoing payments are reflected across all relevant financial systems instantly. This allows for continuous monitoring of transaction flows and makes reconciliation faster and more dependable.

Compliance and Regulatory Adherence

Real-time reconciliation of outgoing funds must adhere to a variety of regulatory requirements, depending on the jurisdiction and the financial institution's operating environment. Regulations often stipulate the need for maintaining audit trails, accurate financial reporting, and the ability to detect and resolve discrepancies in a timely manner.

Compliance frameworks, such as the Payment Services Directive (PSD2) in Europe[10] or the Real-Time Payments framework in the U.S.[11], demand reconciliation practices that provide transparency and accountability for each transaction. Failure to comply can result in penalties or reputational damage, making instant payments compliance a critical component of reconciliation processes.

Exception Handling and Discrepancy Management

In any reconciliation process, handling exceptions is inevitable, and instant payment systems are no exception. Automated exception handling systems, often augmented by machine learning algorithms, are vital for identifying discrepancies. These systems can detect anomalies in transaction data, such as mismatched amounts or missing payments, and trigger workflows designed to resolve issues swiftly.

By using predefined rules and thresholds, organizations can set up automated alerts to notify teams of potential problems as soon as they arise. This real-time discrepancy management reduces the time spent on error correction and ensures that outgoing payments are accurately reconciled without disruption to straight-through processing.

Scalability in Real-Time Reconciliation

As financial institutions grow and transaction volumes increase, reconciliation processes must be scaled accordingly. Systems designed for small-scale operations may struggle to keep pace with the increasing complexity and volume of instant payment transactions. Real-time reconciliation systems should be built to manage growing workloads without sacrificing speed or accuracy.
Cloud-based technologies offer a scalable infrastructure for reconciliation, allowing financial institutions to manage large transaction volumes with flexibility. The cloud also supports business continuity by enabling instant payments data processing and storage without the need for substantial hardware investments.

Unifying Transaction Data for Real-Time Exception Management

Aggregating data from multiple sources to present a complete view of the transaction lifecycle enables a more holistic and accurate approach to reconciliation. By automatically performing a match and kill process—where matching transactions are identified and cleared—organizations can instantly flag discrepancies and exceptions for immediate investigation. This automation not only reduces manual effort and human error but also accelerates issue resolution, improves data accuracy, and strengthens overall financial controls.

Leveraging Existing Reconciliation Frameworks

Many organizations have established frameworks for reconciling incoming real-time payments, which can serve as a foundation for outgoing funds reconciliation. By extending these frameworks, financial institutions can build a comprehensive system that manages both inbound and outbound payments. Key processes, such as real-time message reconciliation, end-of-day balancing, and general ledger reconciliation, can be adapted to meet the specific needs of outgoing payments. For instance, a financial institution may implement a solution that automates the reconciliation of outgoing payments by integrating it with existing general ledger reconciliation processes.

Rules engines are another emerging trend to facilitate auto-reconciliation of instant payments. "Rules" refer to the application of predefined matching criteria to automatically identify and match corresponding transactions across different systems or data sources. Rules engines essentially streamline the reconciliation process by eliminating the need for manual intervention for most routine comparisons, significantly improving efficiency and accuracy.

Key aspects of using rules in real-time reconciliation:

- Matching logic: Rules define the specific criteria used to determine if two transactions from different systems are considered a match, including factors like transaction amount, date, payee/payer name, invoice number, and other relevant data points.
- Rule hierarchy: Rules are often organized in a hierarchy, with more specific rules evaluated first, followed by broader rules to manage edge cases where exact matches might not be found.
- Automated matching: When a new transaction is received, the system automatically applies the defined rules to identify potential matches in the corresponding system, significantly reducing manual effort.
- Alerting for exceptions: If a transaction cannot be matched using the rules, the system generates an alert to flag potential discrepancies requiring manual review.

Examples of rules in real-time reconciliation:

- Exact match: Matching transactions where both the amount and the payee/payer's name are identical.
- Partial match: Matching transactions where only a portion of the data fields (e.g., amount and date) match, with some tolerance for minor variations.
- Date-based matching: Matching transactions based on a specific date range, useful for reconciling recurring payments.
- Invoice number matching: Using the invoice number to link a payment received to the corresponding invoice issued.

Benefits of using rules in real-time reconciliation:

- Faster reconciliation: Automated matching significantly reduces the time required to reconcile transactions.
- Improved accuracy: By applying consistent rules, the risk of human error is minimized.
- Proactive identification of issues: Alerts on unmatched transactions enable prompt investigation and resolution of discrepancies.

Important considerations when using rules in real-time reconciliation:

- Rule development: Carefully design rules to accurately capture the majority of transactions while minimizing false positives.
- Regular review and updates: Rules should be periodically reviewed and updated to reflect changes in business processes or data formats.
- Exception handling: Establishing clear procedures for reviewing and resolving unmatched transactions that fall outside the defined rules.

Best Practices for End-of-Day Reconciliation in a Real-Time World

Even with real-time reconciliation capabilities, end-of-day reconciliation remains a critical control point for financial institutions and their accountholders to validate final balances, confirm transaction completeness, and ensure alignment with scheme and settlement requirements. Best practices for end-of-day reconciliation include clear data formatting standards, defined cutoff times, automated exception reporting, and transparent communication protocols. Leveraging a multi-tenant platform enhances this process by giving both the FI and its clients a shared, real-time view of reconciliation status throughout the day. This centralized access to transaction data and reconciliation outcomes helps preempt end-of-day surprises, supports faster issue resolution, and builds trust by ensuring all parties are aligned on financial positions and outstanding items before closing the business day.

Conclusion

Real-time reconciliation of outgoing funds is a critical process that ensures accuracy, compliance, and operational efficiency in instant payment systems. By leveraging technology, such as automation, AI, and blockchain, financial institutions can enhance the transparency and reliability of their reconciliation processes. Integration with ERP systems, adherence to regulatory requirements, and the ability to scale with business growth are all key factors that contribute to the success of real-time reconciliation efforts.

As payment systems evolve, the importance of building a robust, scalable, and efficient real-time reconciliation system will continue to grow, enabling financial institutions to stay competitive and compliant in an increasingly fast-paced financial environment.

6) Business Continuity & Resilience

Due to their real-time nature, instant payments carry inherent risks and challenges that should be considered for business continuity and resilience planning.

- There is typically a financial driver behind the need to send funds in real-time, so if a transaction fails, there is a risk of financial hardship and/or reputational damage for the accountholder and the organization (e.g., fines for late payment, services shut down for late payment, eviction, an asset not secured due to untimely payment, etc.).

- Instant payment system disruption could have a wider impact resulting in significant financial losses, reputational damage for accountholders and organization.

To mitigate these risks, financial institutions should ensure adequate staffing with trained personnel who are familiar with instant payment operations. Understanding the escalation procedures and service level agreements (SLA) of vendor partners is crucial to maintain operational continuity in case of system disruptions. Understanding which vendors are critical to performance, and having back up, or failover plans.

Business continuity plans should be updated to include instant payments, incorporating considerations like liquidity management and reconciliation processes. It is important to have monitoring systems to be able to detect when there are system interruptions or transaction discrepancies on the sending and receiving of payments. If required, an authorized user should have the capability to override the system to bypass failure points caused due to technical issues or limitations. Additionally, the financial institution should have a process to shut down the instant payment transaction processing if/when necessary (e.g., fraud attacks). Another important consideration is the ability to access and address low-liquidity scenarios to ensure continuous operations.

Uptime Requirements

Instant Payment rails are intended to process on a 24x7x365 basis, and institutions connected must adhere to the associated payment rail requirements. The RTP network and FedNow service both have these requirements formalized. In this section, we explore key requirements for each rail's respective uptime and related processing.

The RTP Network Operating and Participant Rules

Under TCH's RTP Participation Rules for General Eligibility Requirements[12] a Participant must have the ability, directly or through a Third-Party Service Provider that has been approved by TCH, to operate and manage its RTP network activity on a continuous basis 24 hours a day, 7 days a week, 52 weeks a year, including holidays, in accordance with the RTP network's Operating Rules and Technical Specifications.

TCH has established a standard of 99.5% continuous connection measured monthly, which allows cumulative non-connectivity of roughly 3.6 hours per month. In addition, TCH will not consider the first 8 hours per calendar month of non-connectivity during a maintenance window each Sunday from 2 AM to 6 AM Eastern Time toward its assessment of the continuous operations standard.

Uptime is a critical requirement and is included in the scope of the RTP network's self-audit. All RTP network participants must complete an annual audit to verify compliance with the RTP network's Participation and Operating Rules, as required by RTP Operating Rule IX.A.2. Once the self-audit is complete, Participants must return the RTP network's Self-Audit Form to The Clearing House.

The Clearing House does not require the RTP network self-audit to be completed using any specific set of procedures or approach. The RTP Participant Self-Audit Workbook is an optional resource that Participants may wish to utilize to assist with the design and execution of the self-audit and may also be used to record answers, observations, and other information.

The FedNow Service Rules

According to Fed Operating Circular 8 (OC8)[13] under the Availability, Recovery, Resiliency, and Testing section, each FedNow Participant that sends or receives Instant Payment Messages shall maintain the ability to, as applicable based on the FedNow Service profile, to send and receive Messages through the FedNow Service, communicate with their accountholders to receive payment orders and provide notices, and comply with the FedNow Participant's obligations to make funds immediately available to its beneficiaries, in each case, on a 24-hour basis each calendar day, regardless of whether the day is a weekend or other holiday. Other FedNow Participants should maintain the ability to conduct the activities selected in their FedNow Service profile or perform for another FedNow Participant during the hours of those activities.

According to the FedNow service Operating Procedures on Participant and FedNow Service Availability Expectations,[14] Participants and Service Providers may need downtime for planned maintenance. Participants planned downtime should not exceed two consecutive hours or 24 hours total per quarter, and any planned downtime must be scheduled on Sundays between 2 a.m. and 6 a.m. ET. Participants and Service Providers are expected to take steps to reduce their need for planned downtime that better accommodates continuous operations over time.

FedNow Participants must retrieve any dropped messages that may have expired or show up in a message queue. The process to retrieve said messages involves using Account Activity Reports by comparing totals and the Ad hoc Query Tool, which filters messages sent to FedNow and validated before being sent to the Participant.

Weekend & Evening Support

When financial institutions embark on their instant payment journey, it is critical to establish both systematic and human oversight to promptly address technological issues and incidents. While the goal is to create an efficient straight-through processing environment, incidents and discrepancies requiring resolution will inevitably arise. A balanced approach is necessary to ensure smooth operations on both sides of the transaction: enabling the sender's accountholder to successfully initiate a payment and ensuring the receiving financial institution completes the transaction without disruption. Shared challenges may include:

- System and network connectivity
- Network payment failures and rejects
- Liquidity watermarks and funding requirements
- Release management
- Connectivity and availability of network participants

The always-on nature of instant payments necessitates continuous 24x7x365 oversight to ensure a seamless payment lifecycle. Unlike traditional payment systems, real-time payments demand immediate availability of funds to the recipient. Any delays or errors in processing can lead to accountholder frustration, uncertainty, and potentially reputational damage to the financial institution.

Furthermore, a considerable number of use cases rely on access to funds during non-traditional banking hours, including weekends and federal holidays. To uphold accountholder trust and operational reliability, it is crucial to address payment lifecycle challenges effectively during these periods. By ensuring robust oversight and operational readiness, financial institutions can mitigate risks and deliver the reliability expected from instant payment services.

Escalation Procedures

Well documented procedures are essential for managing escalations during systematic disruptions or other disaster scenarios. When system alerts indicate issues impacting accountholder-originated transactions, it is crucial to not only address accountholder inquiries and concerns but also to promptly initiate payment and technical escalations. This involves identifying abnormal payment behavior, analyzing the root causes within the systems, and escalating issues to the appropriate support levels. Such incidents must be treated with urgency to minimize operational and accountholder impact.

The always-on nature of instant payments (24x7x365) amplifies the need for seamless coordination between business line identification and technology support teams to ensure swift resolution. Effective escalation procedures reduce downtime, maintain accountholder trust, and uphold operational continuity in an instant payment environment.

Additionally, participants in the instant payment network must incorporate robust emergency planning. When network connectivity is disrupted, whether for outbound, inbound, or both types of transactions, participants should have protocols in place to temporarily Sign Off from the network. Performing a network sign-off ensures transparency by notifying all network participants that the affected institution is offline. This prevents impacted accountholders from initiating transactions and alerts others that inbound messages cannot be processed. Such measures maintain the integrity of the network and provide clear communication to accountholders at the application level, signaling that the service is temporarily unavailable.

Contingency Plan

Effective network management demands robust contingency planning to address scenarios that could compromise the integrity of key stakeholders and systems. These measures must ensure the continued functionality of participants, vendors, senders, intended recipients, and the overall payment network. By proactively identifying potential vulnerabilities and establishing actionable plans, financial institutions can reduce risks, maintain operational continuity, and uphold the trust placed in instant payment ecosystems.

Key contingency scenarios include various network issues that impact the sending or receiving of payments. For instance, a complete network disruption where both sending and receiving capabilities are down requires active-active configurations to minimize downtime. Other situations may involve partial disruptions, such as when the network can only receive but not send payments, or vice versa. Each scenario demands specific protocols to ensure that transaction flows remain as unaffected as possible.

In addition to network challenges, institutions must also prepare for mainframe outages. Effective strategies include implementing "store and forward" capabilities to retain and process transactions once systems are restored. Stand-in processing capabilities are equally important to maintain transaction functionality during these outages. These contingency measures ensure that disruptions to the payment lifecycle are minimized, and accountholder confidence is preserved.

Third-Party Risk Management

The Instant Payment rails have similar functionality and participation, but the primary and third-party roles associated with each vary. This variation is what creates unique third-party management considerations. Let's next explore some of the key participant and third-party types in each rail and then consider how third-party management applies.

RTP Network

The RTP Network: Enables FI Participants to connect to the rail for the purpose of sending, receiving, and leveraging the RfP functionality. The Network leverages a combination of the following roles to support connection and usage.

- Participant: Financial institution enabled to do a combination of sending, receiving, and request for payment (RfP) functions.

- Funding: The process by which RTP Participants manage their shared master account settlement balance and funding.

    - Funding Participant: A Participant (FI) that is required to maintain sufficient balance in its pre-funded account to cover its sending obligations.
    - Non-Funding Participant: A Participant (FI) that is not either directly responsible for managing its pre-funded balance or uses another provider to address its requirements.
    - Funding Agent: A depository institution that is a party to the Prefunded Balance Account Agreement and is either the Funding Manager or a Funding Provider.[1]
        - Funding Manager: A depository financial institution that has been approved by The Clearing House to be an agent for Non-Funding Participants to meet prefunded requirements and request disbursements.
        - Funding Provider: A depository financial institution that has been approved by The Clearing House to be an agent for Non-Funding Participants to provide funding for the prefunded balance requirements.

- Third-Party Provider: An entity that acts on behalf of participants regarding network function and compliance.

FedNow Service

- FedNow Participant: An FI authorized by a Federal Reserve Bank to send, receive or settle messages through the FedNow Service. Also referred to as a Participant.

- Correspondent: A financial institution (FI) that maintains a Master Account with a Federal Reserve Bank and has agreed to maintain a Settlement Account for another FedNow Participant.

- Service Provider: A party authorized by a FedNow Participant to do one or more of the following on the FedNow Participant's behalf; initiate, transmit or receive messages on behalf of that FedNow Participant; operate or otherwise manage the Electronic Connection used to send or receive messages on behalf of that FedNow Participant; select the security procedure, profile settings or processing options on behalf of that FedNow Participant; or obtain access to information related to the FedNow Participant through the FedNow Service.

Third-party relationships significantly impact financial institutions leveraging instant payments by requiring a comprehensive approach to managing third-party risks throughout the third-party lifecycle. This lifecycle includes planning, due diligence, contract negotiation, ongoing monitoring, and termination, all of which are critical for ensuring operational resilience in real- time payment ecosystems. Instant payments often depend on third-party technology providers, processors, and other partners to deliver 24x7x365 availability and seamless functionality.

Institutions must carefully plan for these relationships by identifying risks, conducting thorough due diligence to evaluate vendors' cybersecurity practices and operational capabilities, and negotiating contracts that clearly define performance standards, regulatory compliance, and responsibilities. Ongoing monitoring is essential to assess third parties' ability to manage real-time transaction volumes, maintain system security, and adapt to evolving risks. Finally, institutions must have robust termination plans to mitigate potential disruptions if a third-party relationship ends. Adhering to this guidance ensures that financial institutions can maintain secure, efficient, and resilient operations in the fast-paced instant payments environment. OCC's Third-Party Relationships Interagency Guidance on Risk Management may be leveraged as a resource.[16]

Business Resilience

As financial institutions adopt instant payments to meet the growing demand for real-time, 24x7x365 fund transfers, business resilience become essential to ensure reliability, security, and compliance. The always-on nature of instant payments requires robust infrastructure, proactive cybersecurity measures, and scalable operations to manage high transaction volumes without interruptions. Institutions must address challenges such as system reliability, fraud risks, and interoperability, all while meeting stringent regulatory requirements. Building resilience involves deploying redundant and cloud-based technologies, implementing advanced fraud detection, conducting regular stress testing, and fostering a culture of readiness through well trained teams and clear incident response protocols. Additionally, collaboration with ecosystem partners strengthens the operational framework and enhances interoperability. By prioritizing resilience, financial institutions can mitigate risks, maintain accountholder trust, and position themselves for sustainable success in the evolving payments landscape. Nacha's *Enhancing Operational Resilience for ACH Network Participants* may be leveraged as a resource.[17]

7) Staffing Needs & Training Requirements

As a financial institution prepares to enable the "send" function for instant payments, evaluating employee needs will be critical. Given the instant nature of these payments, many financial institutions have successfully supported their operations without increasing staffing levels. Depending on an organization's structure, existing departments may have the capacity to absorb operational needs, or there could be opportunities to enhance automation and alerting capabilities.

Key areas to be included in this evaluation are:

- Application and Accountholder Support: Supporting 24x7x365 processing.
- Operations: Processing return requests, reporting, and monitoring activity.
- Fraud Prevention: Managing fraud alerts and fraudulent-related return requests.

- Accounting/Treasury: Reconciliation and funding activities.
- Compliance/BSA: Audits, disclosures, and OFAC requirements.

Post go-live, it will be essential to continually monitor network activity and new use cases that may demand additional resources or support. As the organization gains familiarity with the network's functionality, assessing potential staffing impacts tied to enabling send, receive, and request-for-payment capabilities will become easier.

Employee training will also play a crucial role in ensuring the successful implementation of instant payments. The training scope may vary based on the FI's adoption of other faster payment products and employees' familiarity with those systems. For example, if the FI already offers Zelle®, employees may understand the concept of immediate funds availability but still require training on the unique functions of instant payment products like those leveraging the RTP network or FedNow service. A key distinction is that Zelle is a product, whereas RTP and FedNow are payment rails over which products can settle.

Regardless of broader awareness around faster payments, employees must comprehend the benefits of instant payments and how they are implemented within their organization. Training should focus on various use cases, helping employees understand the application of these payment rails and how accountholders can benefit once the institution goes live. The U.S. Faster Payments Council's *Use Case Repository*[18] serves as a valuable resource for exploring use cases that may align with the FI's accountholder base.

It is important to note that offering both "send" and "receive" instant payments requires deliberate organizational decisions. FIs must enable these functions at their institution, which may involve more than simply activating them through a service provider. This process can include building interfaces, developing user interfaces, implementing fraud monitoring systems, and more. While some FIs offer both send and receive functions, others opt to begin with receive-only services while deciding if or when to enable sending capabilities. A comprehensive list of participating financial institutions is available directly from each network, which can serve as a resource for both employees and accountholders.

For further reference, consult TCH's RTP network's Participating Financial Institutions list[19] and the Fed's FedNow service Participants and Service Providers list.[20]

Training for Frontline Employees on Instant Payments

From an accountholder service perspective, training materials and resources tailored to instant payments are crucial to ensure frontline employees can effectively assist accountholders. These resources should include well-structured documentation, a standardized script with clearly defined escalation triggers, and factually accurate information to address inquiries confidently.

Given the nature of instant payments, where speed and accuracy are critical, employees must be equipped with reliable workflows and an accessible system for follow-up when escalations or unresolved issues arise. All processes and escalation points should be thoroughly documented and readily available, enabling employees to provide seamless 24x7x365 support.

When accountholders are sending instant payments, staff must be prepared to address a range of potential issues promptly and effectively. These may include inquiries related to transaction limits, which can vary by accountholder or line of business; challenges with user interface access; or situations where funds have been sent incorrectly or erroneously.

To manage these scenarios professionally, it is essential for frontline employees to have access to clear guidance and step-by-step workflows to resolve issues efficiently. This includes:

- Transaction Limits: Staff should be knowledgeable about how limits are determined, why they may differ among accountholders, and the process of communicating and adjusting these limits when applicable.
- User Interface Access Issues: Employees need troubleshooting guides to assist accountholders in navigating technical challenges, such as login errors, system outages, or functionality concerns within the payment platform.
- Funds Sent Incorrectly or Erroneously: Clear protocols should outline steps for addressing misdirected payments, including verifying transaction details, initiating resolution procedures, and providing relevant timelines for corrective actions.

In addition to detailed documentation, training materials should emphasize empathy, active listening, and accountholder reassurance, as these situations can often cause stress or frustration for accountholders. Furthermore, escalation triggers must be clearly defined so that complex cases, such as fraud or compliance concerns, can be directed to the appropriate team without delay.

Consider providing a combination of training tools, such as:

- A comprehensive manual outlining instant payment processes.
- A list of frequently asked questions (FAQs) addressing common concerns about instant payments.
- Quick-reference guides or flowcharts for escalation scenarios.
- Short video tutorials to explain key concepts visually.
- An internal knowledge base or searchable resource hub.

By offering diversified, easily accessible training materials, frontline employees will feel confident in addressing accountholder inquiries about instant payments, ensuring a smooth and professional service experience.

Training for Sales Employees

Sales employees play a pivotal role in driving adoption of instant payments by educating accountholders and generating interest in new products and services. As more financial institutions progress from receive-only functionality to offering send capabilities, it will be critical for sales teams to effectively communicate the benefits of sending instant payments. Proper training will empower sales employees to highlight the value of this feature, paving the way for stronger accountholder relationships, deeper engagement, and opportunities to monetize instant payment solutions.

Branch and call center staff are often the first point of contact with both prospective and existing accountholders. These employees must be equipped to position the financial institution as an industry leader by highlighting the value of sending instant payments.

Key areas of focus for training include:

- Differentiating the Institution: Teach sales employees to highlight how instant payment capabilities set the financial institution apart from competitors, particularly those that have not yet implemented this service.

- Targeting Opportunities: Train staff to identify opportunities to convert non-accountholders into accountholders by demonstrating the convenience, speed, and reliability of sending instant payments.

- Deepening Relationships: Help employees explain how instant payment send capabilities can simplify personal finances and enhance everyday transactions for existing accountholders.

- Cross-Selling Opportunities: Emphasize how instant payments can create opportunities to offer complementary products and services, helping to drive revenue growth.

By focusing on these elements, branch and call center employees can create excitement around sending instant payments and elevate the financial institution’s reputation as a modern, accountholder-focused provider.

Treasury Management teams are responsible for engaging with commercial accountholders, where the ability to send instant payments represents a significant value proposition for businesses. These teams must be trained to articulate the strategic advantages of this capability while setting the stage for broader adoption of instant payment solutions.

Training for Treasury Management (TM) teams should focus on:

- Highlighting Business Benefits: Equip TM employees to explain how sending instant payments allows businesses to improve cash flow, reduce payment delays, and enable real-time irrevocable funds movement and settlement.
- Showcasing Competitive Advantage: Train TM employees to emphasize how instant payment send capabilities can differentiate the business accountholder from their competitors, improving accountholder satisfaction and loyalty.
- Explaining Irrevocability and Transparency: Ensure employees can clearly communicate the immediate, irrevocable nature of payments and the rich remittance information included with each transaction, enabling better reconciliation and record-keeping.
- Identifying Future Opportunities: Guide TM employees to use discussions about send capabilities to identify pilot programs and potential accountholders for additional instant payment products or services.

Through this targeted training, TM teams will be positioned to drive adoption of send capabilities among commercial clients while uncovering future sales opportunities.

To maximize effectiveness, training programs should incorporate a variety of resources, including:

- Product guides detailing the features and benefits of sending instant payments.
- Case studies and use cases relevant to consumer and commercial scenarios.
- Scripts and FAQs for addressing common objections or questions.
- Role-playing exercises to build confidence in explaining and selling the solution.

Focusing on the immediacy, security, and operational efficiencies of instant payments will empower sales employees to deliver compelling messages to accountholders. By emphasizing how send capabilities can streamline financial transactions and solve real-world challenges, sales teams will not only drive product adoption but also lay the groundwork for future innovations and revenue opportunities built on instant payment rails.

Training for Back-Office Groups

Specialized training will be essential for back-office employees to understand their roles and responsibilities when financial institutions offer instant payment sending capabilities. The nuances of the FedNow service and the RTP network require targeted training to prepare employees for operational, compliance, fraud, accounting, and IT considerations. Below are key areas to address in a training plan specifically focused on sending capabilities:

- Accounting/Finance:
  - Reconciliation: Employees must be trained to reconcile both settlement accounts and pre-funded balance accounts for the FedNow service and the RTP network. Sending capabilities will introduce additional complexity, requiring a deep understanding of how funds move out of these accounts.

  - Forecasting and Funding: When offering send capabilities, the appropriate teams must develop and implement forecasting and funding models to ensure sufficient balances for outbound transactions. Employees need to know how to monitor liquidity 24x7x365 and adjust funding as needed to prevent transaction delays or rejections.

- Operations:
  - Return Requests and Exceptions: Operations teams must be trained in handling requests to return funds, both incoming requests to return received items and processing accountholder requests on sent items. These may arise from errors or disputes initiated by the sender. This involves understanding the irrevocable nature of instant payments and the limited scenarios in which returns can be processed.

  - Troubleshooting Issues: Although rare, employees will need to troubleshoot cases where sending transactions are accepted but fail to post to recipient accounts, ensuring rapid resolution to minimize accountholder impact.

  - Real-Time Posting Adjustments: Operational staff must understand how to manage issues related to delayed or incorrect posting of outgoing transactions and work closely with applicable parties to resolve reconciliation discrepancies efficiently.

- Compliance:
  - Updated Rules and Regulations: Compliance employees must stay current with rules and regulations governing sending instant payments on both the FedNow service and the RTP network. Training should highlight specific obligations for outbound transactions, including disclosure updates and any new policy requirements introduced by sending functionality.

  - Risk Assessments: Sending instant payments presents risks, such as the potential for fraud or unintended errors. Compliance teams must be trained to perform regular risk assessments and adapt the institution's risk posture as necessary to align with the evolving regulatory landscape and the specific instant payments implementation.

    - Accountholder Communication: Ensure compliance employees understand how to draft and review clear, accurate, and compliant accountholder-facing materials.

- Fraud:
    - Fraud Monitoring Tools and Alerts: Fraud teams need training on monitoring tools and mechanisms designed to detect unauthorized or suspicious outbound transactions, particularly given the speed and irrevocability of instant payments.

    - Fraudulent Transaction Reporting: Employees must understand reporting requirements for fraudulent activity and how to submit reports to the respective network (e.g., the FedNow service or the RTP network).

    - Investigating Fraud Claims: Fraud investigators should be trained to handle cases where a sender claims a payment was sent fraudulently or in error. This includes understanding protections for senders, network rules for fraud resolution, and procedures for escalating cases internally.

    - Proactive Prevention: Training should cover best practices for educating senders on avoiding phishing scams, social engineering, and other fraud schemes related to instant payments.

- IT:
    - Message Flows and Network Specifications: IT employees must understand message flows, formatting specifications, and connectivity requirements for supporting outbound transactions across the FedNow service and the RTP network.

    - Escalation Procedures: Documenting protocols for identifying, troubleshooting, and resolving technical issues tied to sending transactions is vital. Employees should also know when and how to escalate issues to third-party service providers or network operators.

    - 24x7x365 Support: IT teams must be trained in maintaining system uptime for continuous transaction processing, managing load balancing, and performing real-time issue resolution without disrupting operations.

To prepare for the complexities of sending instant payments, training programs should focus on:

1. Role-Specific Learning: Tailor training to the specific needs of each department, ensuring employees have the knowledge and skills required for their responsibilities.

2. Scenario-Based Exercises: Use real-world examples relevant to sending capabilities (e.g., insufficient funds in pre-funding accounts, fraudulent transactions) to help employees apply their training effectively.

3. Ongoing Education: Provide regular updates as sending-related rules, regulations, and operational guidelines evolve, especially as the usage of instant payments grows.

4. Cross Department Coordination: Train employees to collaborate across teams (e.g., IT, fraud, compliance) to identify and resolve issues quickly and accurately. Formal training and accreditation such as the Accredited Faster Payments Professional (AFPP)[21] should be strongly considered for any key personnel.

By equipping employees with the expertise to manage sending capabilities for instant payments, financial institutions can ensure smooth operations, mitigate risks, and deliver excellent service to accountholders using this innovative payment functionality.

8) Accountholder Education & Disclosures

Education

Educating accountholders is a key component of enabling the ability to send instant payments. Proper education should focus on the convenience, security, and functionality of instant payments, while also providing clear guidance on best practices for using them effectively. FI's should prioritize creating accessible and effective educational resources, ensuring accountholders can easily reference them when needed.

Methods for Educating Accountholders:

- Onboarding process: The onboarding stage is an ideal opportunity to tailor education to each accountholder's specific use case for sending instant payments. Personalizing the experience helps ensure the information is relevant and impactful.

- Q&A Sessions and Resources: FI's can offer easily accessible Q&A templates, along with options for live webinars or pre-recorded video tutorials. These resources provide accountholders with opportunities to get their questions answered and learn at their own pace.

- Email Campaigns or Newsletters: Sending educational emails with tips, updates, and best practices on using instant payments can keep accountholders informed and engaged.

- Proactive Updates and Alerts: Push notifications and alerts can notify accountholders when new instant payment features or enhancements are available.

- Accountholder Support: When accountholders contact support, this presents an opportunity to educate them about instant payments. Support can be delivered in person, through chat, or over the phone.

Key Topics for Accountholder Education: FIs should ensure that education covers essential topics to ensure accountholders can effectively use instant payments:

- Define an Instant Payment: Offer a clear explanation of what instant payments are and how they work.

- Benefits of Instant Payments: Outline the advantages, such as speed, convenience, and real-time settlement.

- Security of Instant Payments: Address concerns by educating accountholders on the security measures in place to protect their transactions as well as the risk of fraud, including common scams and how to avoid them.

- How to Send an Instant Payment: Step-by-step guidance on the process of sending instant payments through the institution's platform.

- Costs and Fees: Transparency of any fees associated with sending instant payments.

- Use Cases for Instant Payments: Highlight use cases specific to the FI's services, such as personal transfers, business payments, or emergency transactions.

- How Return Requests Work: Explain the procedures for requesting returns in the event of an error or issue with a transaction.

- Limits and Exceptions: Educate accountholders on transaction limits and situations where payments may be delayed due to fraud prevention, compliance, or other factors.

Each FI will need to tailor its educational approach to the specific use cases they enable and the needs of their accountholder base. Additionally, as new features and functionality are introduced, FIs should ensure they have a plan for continuously updating and educating accountholders on these changes.

Disclosures

Financial institutions are subject to various regulations, guidance, and best practices regarding disclosures to accountholders who participate in electronic payment services, including the newer instant payment rails. If applicable, general areas of information for disclosure include transaction details, accountholder rights, error resolution procedures, fees and charges, protections over consumer privacy and data security, and confirmation of terms and conditions with opt-out optionality.

Description of Service

Financial institutions play a crucial role in empowering accountholders with the convenience and efficiency of instant payment services, and it is essential to provide a clear and comprehensive description of these services to ensure transparency and understanding. The description should outline the key aspects of the service, such as capabilities, benefits, and limitations of instant payments, and clarify the responsibilities of both the financial institution and the accountholder throughout the payment process. In the description of the instant payment services, financial institutions should highlight the following key aspects:

- Service Overview: Begin by providing a brief overview of instant payment services, explaining how they enable immediate fund transfers and payments between accounts in real-time.

- Features and Benefits: Detail the features and benefits of instant payments, including instant availability of funds, irrevocability, fast transaction processing, and enhanced convenience for accountholders.

- Eligibility and Enrollment: Specify the eligibility criteria for accessing instant payment services and outline the enrollment process for accountholders to activate and use the service.

- Transaction Limits: Clearly define the transaction limits and thresholds associated with instant payments, informing accountholders of any restrictions on transfer times and amounts.

- Charges and Fees: Disclose any applicable charges, fees, or pricing structures related to instant payment services, ensuring transparency in cost implications for accountholders. Additionally, any changes in the fee structure or pricing models should be communicated in a timely and transparent manner to avoid unforeseen charges for accountholders. Based upon whether the accountholder is a consumer or corporate, accountholders may be subject to different charges or fee structures and carry different degrees of legal liability in case of damages.

- Security Measures: Explain the security protocols and measures implemented to safeguard instant payment transactions, reassuring accountholders of the safety and integrity of the payment process.

- Responsibilities of Accountholders: Clearly outline the responsibilities and obligations of accountholders initiating, authorizing, and verifying instant payment transactions, emphasizing the importance of accurate and secure transaction details.

- Support and Assistance: Provide information on the available support channels, accountholder service contacts, and assistance options for accountholders seeking guidance or resolution for any issues related to instant payment services.

By offering a detailed description of instant payment services, financial institutions can empower accountholders with a clear understanding of the service offerings, benefits, and guidelines for using instant payment capabilities effectively. Clarity and transparency in communicating the key aspects of instant payments foster trust, confidence, and satisfaction among accountholders, enhancing their overall experience and engagement with the financial institution's innovative payment services.

Error Resolution

With the evolution of payment systems towards instant transactions, financial institutions must prioritize error resolution processes to uphold consumer protection and compliance with regulatory standards. Account disclosures should be meticulously reviewed and updated to include detailed procedures for error resolution in the context of instant payments. Compliance with Regulation E mandates thorough reporting and notification to consumers regarding the resolution status and remediation actions taken within specific timelines.

Error resolution mechanisms are crucial components of consumer protection in the realm of instant payments and must encompass a comprehensive scope of potential errors on the sending side of transactions. These errors may include instances such as incorrect electronic fund transfer to or from the consumer's account, the omission of an electronic fund transfer from a periodic statement, or computational or bookkeeping errors made by the financial institution in connection with an electronic fund transfer.

Financial institutions should ensure that their account disclosures provide clear and transparent guidelines on how consumers can report errors, the steps taken by the institution to investigate and resolve these errors, and the timelines within which consumers can expect resolution outcomes. Prompt and accurate error resolution processes instill trust, reliability, and confidence in the instant payment services offered by financial institutions, enhancing the overall accountholder experience and safeguarding consumer rights in the dynamic landscape of instant payment transactions.

Privacy and Use of Data

In an increasingly data-driven financial landscape, maintaining robust privacy measures and transparent data practices is imperative for ensuring consumer trust and compliance with regulatory requirements. Financial institutions engaging in partnerships must provide clear and comprehensive information to accountholders regarding the sharing and utilization of their data within the collaborative framework. Transparency is key, and accountholder data privacy policies should be explicitly stated, with any updates or modifications to these policies clearly communicated to accountholders.

When accountholder data is shared with third-party service providers as part of a partnership arrangement, it is essential for financial institutions to disclose the types of data being shared and the intended purposes for which it will be used. Often, this data sharing is conducted for functions such as screening and authentication of bank accounts or identities, underscoring the importance of informed consent and awareness among accountholders.

Moreover, financial institutions must proactively address data security risks to mitigate potential threats to accountholder information. Clear and concise risk disclosures should be provided to inform accountholders of the possible vulnerabilities and challenges associated with data security in the partnership context. It is critical to explain to accountholders how these risks are being actively managed and mitigated through robust cybersecurity measures, encryption protocols, access controls, and ongoing monitoring processes.

Rules and Laws

Financial institutions must comply with various rules, laws and regulations and ensure their disclosures are accurate and compliant. Adherence to rules and laws governing the financial sector is essential for ensuring ethical conduct, consumer protection, and operational integrity within financial institutions. To maintain compliance with relevant financial regulations, institutions must proactively assess, monitor, and disclose how regulatory requirements are being upheld throughout their operations. Areas of relevance include Regulation J, Regulation CC, USS 4A, Federal Reserve Operating Circulars, FedNow Service Operating Procedures, USA Patriot Act, BSA, OFAC, UDAAP, Regulation E. This commitment to compliance not only safeguards the institution but also fosters trust and confidence among accountholders and stakeholders.

- **Regulation J[22]:** Established by the Federal Reserve, it governs how financial institutions collect checks and other items through the Federal Reserve System, including how they settle balances with the Fed, the terms, and conditions for receiving and delivering funds transfers over the Fedwire system and the FedNow service. Regulation J, Subpart C specifically governs the rules and procedures for funds transfers made through the FedNow service, essentially outlining the terms and conditions under which Reserve Banks will process instant payments via this system; it acts as a set of guidelines for facilitating quick, real-time transactions through FedNow. essentially outlining the legal framework. Regulation J, Subpart C applies UCC 4A to all FedNow transfers. FedNow transfers that are subject to the EFTA are governed by UCC 4A except if there is an inconsistency between the provisions. If there is an inconsistency between EFTA and UCC 4A, EFTA would prevail to the extent of the inconsistency. Subpart C of Regulation J establishes the funds availability requirements for receiving financial institutions, the obligations for sending financial institutions, and the use of ISO 20022 standards for messaging. This allows the Federal Reserve Banks to rely on account and identification numbers for the transfers, unless they are aware of an inconsistency.

- **Regulation CC**[23]**:** Regulation CC is a Federal Reserve Board regulation that establishes requirements for how funds are made available to accountholders and how checks are collected and returned. When speaking about instant payments, Reg CC comes into play with the RTP network and the FedNow service when customer credit transfers are Accepted Without Posting. It creates a fallback to immediate funds availability requirements when financial institutions need additional time to investigate a transfer prior to making funds available to the Receiver.

- **UCC 4A**[24]**:** Uniform Commercial Code (UCC) Article 4A governs funds transfers and wholesale payments. Financial institutions must adhere to UCC 4A provisions related to payment orders, security procedures, and liability for unauthorized payment orders, under FedNow the provisions of the EFTA and Regulation E will supersede UCC 4A in any transaction involving a consumer sender or receiver. The Clearing House states that UCC 4A will also apply to funds transfers through RTP that do not credit nor debit a consumer account, as defined in Regulation E. Compliance with UCC 4A ensures the legality and security of electronic funds transfers conducted by financial institutions.

- **Federal Reserve Financial Services Operating Circulars**[25]**:** Compliance with the Federal Reserve Financial Services Operating Circular is required for financial institutions participating in Federal Reserve payment systems. The circular outlines operational guidelines, risk management practices, and compliance requirements that institutions must follow to ensure the safety and efficiency of payments processed through Federal Reserve services. Operating Circular 8 (OC8) outlines the terms and conditions for using the FedNow service, essentially dictating the rules and guidelines that financial institutions must follow when participating in instant payments through the FedNow platform; it specifies details like participant expectations, service availability expectations, connection profiles, fraud mitigation and reporting, message formats and security requirements.

- **Federal Reserve Banks Operating Circular No. 5 – Electronic Access[26]:** FRB Operating Circular No. 5 establishes the terms under which an institution accesses services and applications provided by a Reserve Bank. It also outlines exchanging certain data with a Reserve Bank. The circular addresses security requirements, service providers, risks, and liabilities associated with using and maintaining an electronic connection to a Federal Reserve Bank. Operating Circular No. 5 describes the minimum self-assessment a financial institution should conduct on security procedures, operating instructions, and guidelines involved with the electronic connection and outlines the expectation of confidentiality and data security.

- **FedNow Service Operating Procedures[27]:** The FedNow service Operating Procedures are requirements, guidelines, and expectations that outline how the Federal Reserve Banks use the FedNow service. These procedures cover various aspects, including participant and service availability, message signing, participant and connection profiles, fraud mitigation, reporting, and ISO 20022 messaging. They also address compliance-related requirements, such as anti-money laundering and sanctions compliance.

- **RTP Network Operating Rules[28]:** The RTP network Operating Rules cover the use of the system, including operating obligations, the sending and receiving of messages, funds availability, and settlement. They also contain the technical specifications for using the RTP system, formatting requirements for messages, availability expectations as well as audit and testing requirements. RTP incorporates the use of additional RTP Rule Schedules to address participant obligations on specific topics such as risk management and fraud. TCH issues rules interpretations for the RTP Operating Rules.

- **RTP Network Participation Rules[29]:** The RTP Participation Rules establish the eligibility requirements and the process of becoming an RTP participant. The Participation Rules also define categories of participants, address the use of third-party service providers and the use of Funding Agents, and establish the participant's liability when using the payment system. Additionally, the Participation Rules provide The Clearing House with the right to terminate or suspend a participant.

By emphasizing the importance of regulatory compliance, financial institutions demonstrate their commitment to ethical conduct, regulatory accountability, and consumer protection. Transparent disclosure of compliance practices and adherence to relevant rules and laws promote a culture of integrity, trustworthiness, and regulatory excellence within the financial industry.

9) Fraud Mitigation

Fraud in Instant Payments

As financial institutions begin to offer their accountholders the ability to send instant payment transactions, they are exposed to a heightened risk of fraud. Unlike traditional payment methods, where processing delays allow time to identify and intercept fraudulent activities, instant payments settle in seconds, leaving little room for error or recovery. This immediacy makes them attractive targets for cybercriminals who exploit vulnerabilities in authentication processes, accountholder awareness, and system controls. Fraud schemes like account takeovers, social engineering scams, and unauthorized transfers can result in significant financial and reputational losses for both accountholders and institutions.

To effectively combat these risks, financial institutions must understand the current faster payments fraud environment, understand industry classification methods for frauds and scams, implement fraud mitigation techniques and controls, learn applicable fraud reporting requirements for the instant payments networks with which they chose to participate, and embrace the role of Third-Party Partnerships in implementing an effective faster payments solution for their accountholders.

Faster Payments Fraud Environment

2024 AFP Payments Fraud and Control Survey Report

The Association for Financial Professionals (AFP) published its annual 2024 AFP Payments Fraud and Control Survey, which noted that check fraud continues to account for much of the payments fraud landscape and that ACH credit transactions have surpassed wires as one of the significant contributors to business email compromise (BEC) credit-push fraud schemes. Credit-push fraud is a concern with the instant payment rails (such as the RTP Network and the FedNow service). A trend toward additional fraud in this space is a concern as the industry sees more adoption and usage of credit-push instant payments.

An interesting note from the survey centers around the percentage of faster payments subject to overall attempted and actual payment fraud reported. In 2022, 8% of this fraud was reported as attributed to faster payments. In 2023, that number had dropped to just 1%. While this trend is currently down, the number of senders using the instant payment rails is still relatively low compared to the more established payment networks.

BEC fraud continues to be a challenge in payments, with trends occurring around impersonator vendor payment change instructions, fake internal CEO emails requesting the purchase of gift cards, and false bank account remittance updates occurring. BEC trends were addressed in the report by Nacha on *New Risk Management Framework for the Era of Credit-Push Fraud*[30]. The fraud control survey results are consistent with the trends and challenges outlined in the framework. However, an interesting note in the survey is that the percentage of organizations impacted by BEC decreased from 71% in 2022 to 63% in 2023. This is an indicator that education and controls are becoming more effective.

Fraud Schemes in an Instant World

As the AFP Payments Fraud and Control Survey Report indicates, payments fraud is a continuing issue, and instant payments channels are no exception. Many of the same fraud schemes that happen on other payment channels also happen in instant payments. However, instant payment fraud schemes often exploit the speed and irrevocability of instant payments, making instant payment fraud detection and prevention even more challenging for financial institutions than traditional payment channels. Below are some examples of how fraud schemes for traditional payments have been used in an instant payment environment.

- Authorized Push Payment Scams: Fraudsters exploit the immediate settlement nature of instant payments, giving victims no time to reconsider transfers before funds become irrevocable.

- Account Takeover: Once criminals gain account access, they specifically target instant payment channels to transfer funds rapidly before detection systems can respond.

- Phishing: After obtaining credentials through deception, attackers leverage instant payments for immediate fund extraction, bypassing traditional fraud monitoring periods.

- Social Engineering: Scammers create artificial urgency scenarios specifically designed to push victims toward using instant payment methods where transactions cannot be reversed after the victim has more time to consider the reasonableness of the request.

- Business Email Compromise: Fraudsters impersonating executives deliberately direct employees to use instant payment channels, knowing these transactions settle immediately with no recall option.

- Synthetic Identity Fraud: False identities are created specifically to access instant payment capabilities, allowing fraudsters to quickly move stolen funds across multiple accounts.

- Vendor/Invoice Fraud: Fake invoices now specifically request payment via instant channels, as fraudsters know these payments cannot be stopped once initiated.

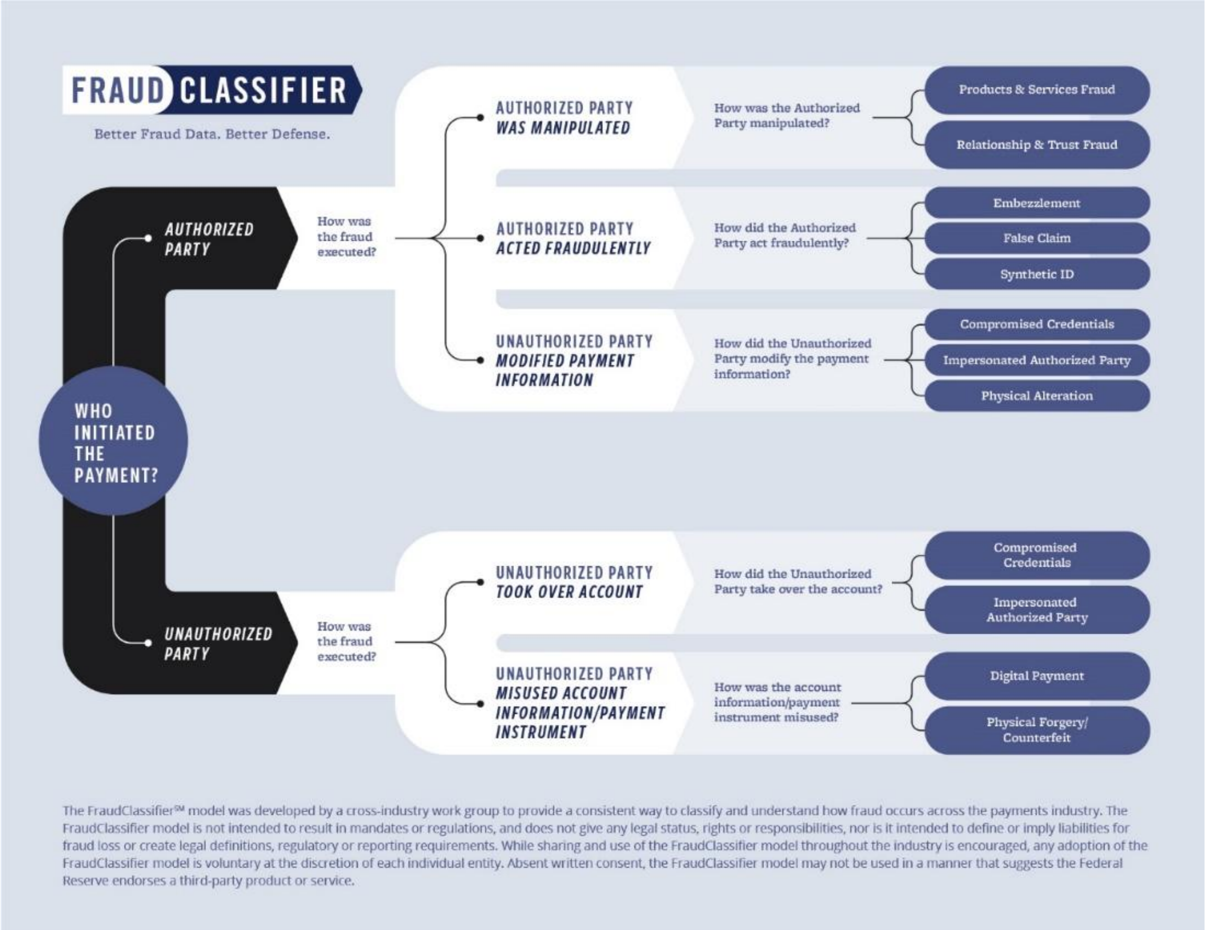
Additional information on the speed and irrevocability of instant payments can be found in reports published by the Fraud Work Group of the Faster Payments Council.[31]

Fraud vs. Scams in Instant Payments

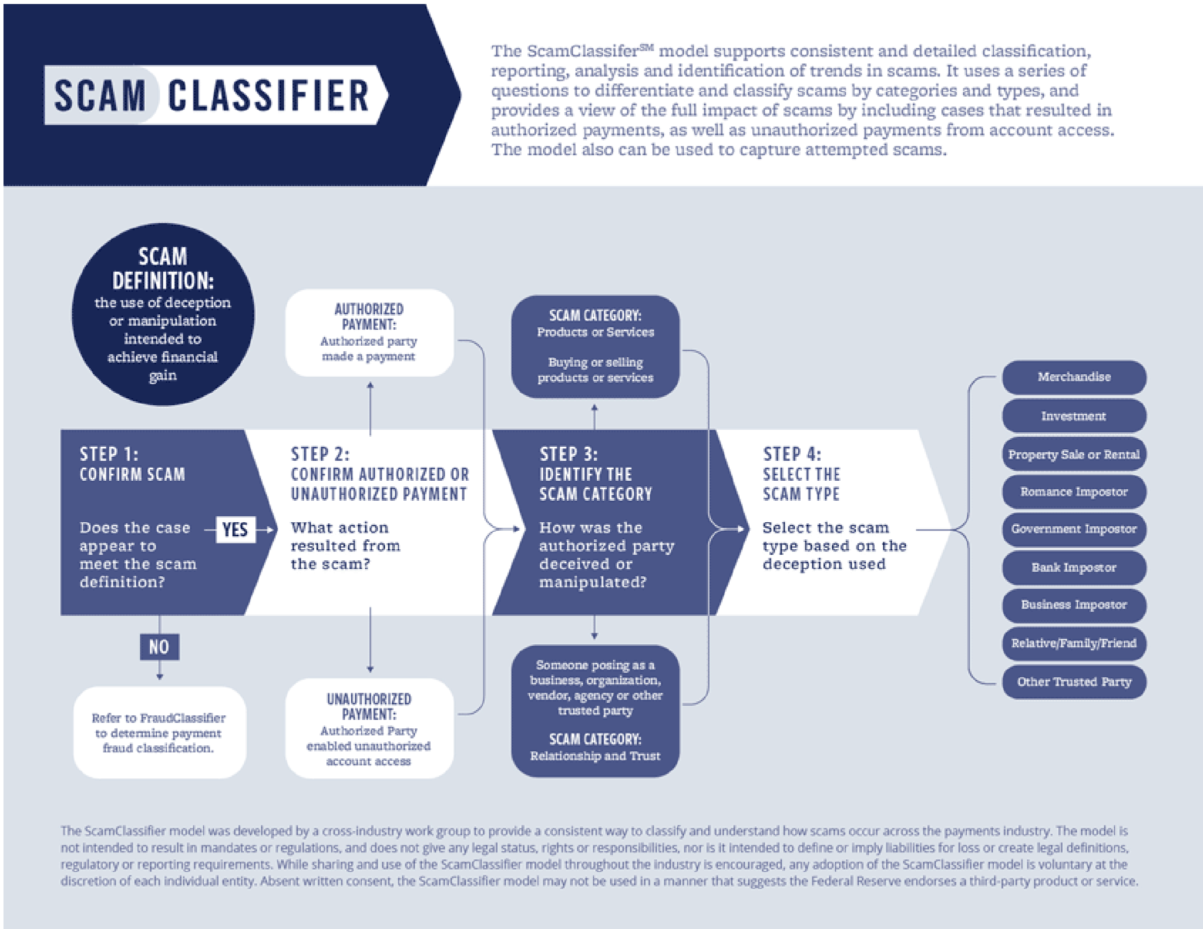
As evidenced with the tactics described above, instant payments are subject to both fraud schemes and scam schemes by criminals. The Federal Reserve distinguishes between fraud and scams, with scams being a specific type of fraud involving deception or manipulation for financial gain. To help the industry more effectively combat fraud and scams, cross-industry work groups established two models, the FraudClassifier^{SM} and the ScamClassifier^{SM}, to standardize classifications across the industry.

Fed Fraud and Scam Classifier Models[32]

The Federal Reserve Bank's Fraud and Scam Classifiers provides standardized frameworks for categorizing fraud and scam events, including those related to instant payments credit push scenarios. The Fraud model classifies fraud based on three key questions: who initiated the payment (authorized or unauthorized party), how the fraud was executed, and what tactic was used. The Scam model determines if the scam included authorized or unauthorized payments, defines the event into scam categories of buying or selling products, services, relationships, and trust, and classifies scam events as merchandise, investment, property sale or rental, romance imposter, government imposter, bank imposter, business imposter, relative/family/friend, or other trusted party. Both models drive consistency in fraud and scam identification and reporting, enabling financial institutions to analyze trends and share insights more effectively. For instant payments, this tool is particularly valuable, as the speed and finality if transactions leave little room for error.[33]


FRAUD CLASSIFIER
Better Fraud Data. Better Defense.
WHO INITIATED THE PAYMENT?
AUTHORIZED PARTY
How was the fraud executed?
AUTHORIZED PARTY WAS MANIPULATED
How was the Authorized Party manipulated?
Products & Services Fraud
Relationship & Trust Fraud
AUTHORIZED PARTY ACTED FRAUDULENTLY
How did the Authorized Party act fraudulently?
Embezzlement
False Claim
Synthetic ID
UNAUTHORIZED PARTY MODIFIED PAYMENT INFORMATION
How did the Unauthorized Party modify the payment information?
Compromised Credentials
Impersonated Authorized Party
Physical Alteration
UNAUTHORIZED PARTY
How was the fraud executed?
UNAUTHORIZED PARTY TOOK OVER ACCOUNT
How did the Unauthorized Party take over the account?
Compromised Credentials
Impersonated Authorized Party
UNAUTHORIZED PARTY MISUSED ACCOUNT INFORMATION/PAYMENT INSTRUMENT
How was the account information/payment instrument misused?
Digital Payment
Physical Forgery/ Counterfeit

The FraudClassifier^{SM} model was developed by a cross-industry work group to provide a consistent way to classify and understand how fraud occurs across the payments industry. The FraudClassifier model is not intended to result in mandates or regulations, and does not give any legal status, rights or responsibilities, nor is it intended to define or imply liabilities for fraud loss or create legal definitions, regulatory or reporting requirements. While sharing and use of the FraudClassifier model throughout the industry is encouraged, any adoption of the FraudClassifier model is voluntary at the discretion of each individual entity. Absent written consent, the FraudClassifier model may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.


SCAM CLASSIFIER
SCAM DEFINITION: the use of deception or manipulation intended to achieve financial gain
STEP 1: CONFIRM SCAM
Does the case appear to meet the scam definition?
YES
NO
Refer to FraudClassifier to determine payment fraud classification.
STEP 2: CONFIRM AUTHORIZED OR UNAUTHORIZED PAYMENT
What action resulted from the scam?
AUTHORIZED PAYMENT: Authorized party made a payment
UNAUTHORIZED PAYMENT: Authorized Party enabled unauthorized account access
STEP 3: IDENTIFY THE SCAM CATEGORY
How was the authorized party deceived or manipulated?
SCAM CATEGORY: Products or Services
Buying or selling products or services
Someone posing as a business, organization, vendor, agency or other trusted party
SCAM CATEGORY: Relationship and Trust
STEP 4: SELECT THE SCAM TYPE
Select the scam type based on the deception used
Merchandise
Investment
Property Sale or Rental
Romance Impostor
Government Impostor
Bank Impostor
Business Impostor
Relative/Family/Friend
Other Trusted Party

The ScamClassifier℠ model supports consistent and detailed classification, reporting, analysis and identification of trends in scams. It uses a series of questions to differentiate and classify scams by categories and types, and provides a view of the full impact of scams by including cases that resulted in authorized payments, as well as unauthorized payments from account access. The model also can be used to capture attempted scams.

The ScamClassifier model was developed by a cross-industry work group to provide a consistent way to classify and understand how scams occur across the payments industry. The model is not intended to result in mandates or regulations, and does not give any legal status, rights or responsibilities, nor is it intended to define or imply liabilities for loss or create legal definitions, regulatory or reporting requirements. While sharing and use of the ScamClassifier model throughout the industry is encouraged, any adoption of the ScamClassifier model is voluntary at the discretion of each individual entity. Absent written consent, the ScamClassifier model may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.

Examples of Fraud Mitigation Techniques and Considerations

Digital Profiling

Digital profiling is a critical component in fraud mitigation techniques for instant payments. It involves analyzing various data points to identify and verify legitimate accountholders, thereby distinguishing them from potential fraudsters.

For example, instant payment activities that are outside the accountholder's typical behavior can trigger alerts. If an accountholder’s usual transaction limit is $500, but suddenly, they initiate a $5,000 transfer, digital profiling can flag this as suspicious, triggering additional authentication steps or blocking the transaction. Similarly, if an accountholder typically transacts from the same state within the U.S., but an instant payment is attempted from another country without prior travel history or notification, an effective digital profiling framework can halt the payment for verification.

Key data points used in digital profiling could include identity verification methods (e.g., multi-factor authentication), device fingerprints (e.g., browser settings, screen resolution, IP addresses), and behavioral patterns (e.g., login times, transaction history). These data points can be analyzed to identify typical behaviors of legitimate accountholders and detect unusual activities that may indicate an account has been compromised.

Real-Time Fraud Screening

Often working in conjunction with digital profiling is a real-time fraud detection system to identify patterns and outliers, flagging suspicious activities for further review. For instance, sudden high-value transactions or a spike in transaction frequency can trigger alerts, prompting immediate action to prevent fraud. These systems are especially critical for instant payment networks because they can drive immediate action to prevent fraud before it is too late.

Real-time fraud screening should demonstrate a high degree of detection accuracy to effectively stop fraudulent transactions while minimizing false positives that impact accountholders. To achieve this, systems often leverage artificial intelligence and machine learning models to detect complex and emerging fraud patterns and adapt quickly to evolving threats. The application used for real-time fraud screening should be capable of processing large transactions volumes in real-time to manage the high velocity of instant payments, particularly as send volumes are expected to continue increasing.

Category and Transaction Limits

Category limits restrict transactions by type, while daily and weekly aggregated limits cap the total transaction value within specified periods. By setting category and transaction limits as it relates to a send transaction, a financial institution can accomplish the following goals: cap the amount of potential losses, deter fraudsters from executing large-scale fraud and allow time for fraud detection.

There are a variety of way effective limits could be set. One such way is to establish per-transaction limits that apply to all accountholders in the same manner. Similarly, a daily transaction limit can be set separately or in conjunction with the per-transaction limit. Limits could also be applied differently based on accountholder type or characteristic (e.g., personal vs. business accounts, new accountholder vs. existing accountholder). Varying limits by initiation channel is another type of limit that could be established (e.g., via mobile app, online banking, request for payment).

Payee Validation

Payee validation refers to verification processes and systems to ensure the transfer is going to the intended recipient. Payee validation is not currently imbedded into the faster payment networks and would likely require a directory to be created and utilized.

One type of payee validation aims to ensure that the sender knows the recipient and that funds are not being sent for fraudulent reasons. For example, this could be a pop-up message to catch the sender’s attention as one last attempt to ask, “Are you sure you want to send these funds?” before the transaction is initiated and then irrevocable. Additionally, education and training to identify and question unusual transactions by frontline staff may also be beneficial, particularly when working with accountholders who are at elevated risk for scam attempts.

Another type of payee validation is also used to confirm that the account name and number match. This validation service checks whether the account name matches the intended recipient, reducing the risk of misdirected payments and fraud.

Account Validation

Account validation processes verify the legitimacy of the account details before transactions are processed, adding another layer of security. Account validation is incorporated into faster payment systems to the degree that a transaction sent to a non-participating financial institution will be rejected. However, once ubiquity is achieved among financial institutions, additional measures will be required to meet this goal.

Policy Review & Enhancement

To effectively prevent fraud when enabling instant payments, financial institutions must update and enhance their policies and procedures to address the unique risks associated with instant payment transactions. For example, existing fraud reporting mechanisms and investigation procedures should be updated to cover scenarios that are unique to instant payments, such as high-speed account takeovers or rapid fund dispersion.

Importance of KYC Programs

Know Your Customer (KYC) programs are crucial in combating fraud in instant payments by establishing a robust foundation for accountholder identity verification. These programs help financial institutions verify the legitimacy of accountholders, assess their risk profiles, and monitor their transaction patterns. By thoroughly vetting accountholders during onboarding and continuously monitoring their activities, KYC processes can detect suspicious behavior, and potential fraud attempts in real-time. This proactive approach allows FIs to implement targeted fraud prevention measures, such as transaction limits or additional authentication steps, for high-risk accountholders. Ultimately, KYC programs create a more secure instant payment ecosystem by reducing the likelihood of fraudulent transactions and protecting both financial institutions and legitimate accountholders.

Advanced Analytics Volume, Value, & Velocity

Advanced analytics related to volume, value, and velocity are crucial in combating fraud in instant payments and are often used as a component of a robust digital profiling program as mentioned above. These analytics enable real-time monitoring of transaction patterns, allowing FIs to detect anomalies quickly. Volume analytics identify unusual spikes in transaction frequency, while value analytics flag atypical transaction amounts. Velocity checks detect rapid-fire transactions that may indicate fraudulent activity. By analyzing these factors in real-time, financial institutions can swiftly identify and block potentially fraudulent transactions before they are completed. This multi-faceted approach helps FIs mitigate risks associated with the speed of instant payments, reducing fraud losses, and maintaining accountholder trust.

Artificial intelligence and Machine Learning

Artificial intelligence (AI) plays a critical role in fraud monitoring for instant payments by enabling real-time detection and preventing fraudulent activities in a high-speed transaction environment. AI-powered systems analyze vast amounts of transactional data, identifying patterns and anomalies that may indicate fraud, such as unusual transaction amounts, geographic discrepancies, or deviations from normal accountholder behavior. Machine learning algorithms continuously adapt to emerging threats, improving their accuracy in detecting sophisticated fraud schemes. These systems can also facilitate predictive analytics, allowing financial institutions to identify vulnerabilities and mitigate risks proactively before fraudulent activity occurs. By leveraging AI, institutions can ensure that the immediacy of instant payments does not come at the expense of security, safeguarding accountholder trust and maintaining compliance with regulatory standards.

Instant Payment Network Rules

FedNow Service

The FedNow Operating Procedures, a companion document to OC8, addressed some key network aspects of risk management and fraud mitigation once such area is the Participant Negative List. The negative list enables FedNow participating FIs to upload account and routing number pairs that can only receive, send, or not send and receive at all. This is a self-managed process by the FIs designed to enable participants to control potential service abuse. The FedNow Operating Procedures also address fraud reporting, but this information is not public and is only available once a FedNow participant signs up for the service.

FedNow is a credit-push network with transaction settlement resulting in irrevocability. However, the service is enabled for the Return Request (camt.056) message, which can be used to request a return of funds for a previous Customer Credit Transfer (pacs.008) or Liquidity Management Transfer (pacs.009). A Return Request message may also include the return reason code FRAD if fraud is confirmed or suspected.

The Return Request should be sent within 60 days of the credit transfer settlement. Responses to these requests include accepting the message and returning funds, rejecting the request, return pending investigation, and partial return of funds. Final responses must be sent by no later than midnight (ET) of the next standard business day after receipt of the request. To return the funds the Payment Return (pacs.004) or a new Liquidity Management Transfer (pacs.009) would be used.

FedNow supports the pacs.002 ACWP (Accept Without Posting) message to enable an institution more time to review an incoming credit before posting the credit. Receiving FIs are expected to make the funds available to the receiver or return the funds to the sender by midnight ET of the next standard business day after the ACWP response. Additional investigation time is permitted as allowed by law.

FedNow has also provided a FedNow *Readiness Guide*[34] that specifically addresses managing fraud risk. Highlights on the key considerations are reflected in these guidelines, but it is recommended that those seeking more information refer to the *Readiness Guide*.

- Risk Management Capabilities
  - Network-level transaction limits: Maximum per transaction set at the network level by the Federal Reserve (currently $1M).

  - Participant-level transaction limit: The FI may set a maximum per transaction limit for sending which can be lower than the FedNow maximum transaction limit.

  - Participant-defined negative lists: FI-specific lists that enable the institution to instruct FedNow to reject transactions to or from an account on a Participant negative list.

- Participant Reporting and Notification of Fraud: It is mandatory to notify the FedNow operator of confirmed or suspected fraud occurring on the network. The fraud indicator may be used in the Request for Return of Funds message.

- Error Resolution: FedNow Participants may use the request for information, accept without posting, and return request messages to aid them with risk management and possible error resolution scenarios.

- Information Security: FedNow Participants must use digital signatures (transaction-level encryption), data encryption and authorization, and authentication and authorization to secure and protect transactions, access, and data.

- Organizations are the First Line of Defense: FedNow Participants can leverage a combination of the following tactics for addressing fraud management:
    - Understand the basics of instant payments and fraud.
    - Activate your fraud management team.
    - Review and upgrade your systems as needed.
    - Enlist your accountholders in prevention.
    - Talk with your vendors about tools to improve detection.
    - Classify fraud to strengthen mitigation efforts.
    - Understand the fraud reporting requirements for the FedNow service.

The RTP Network Operating Rules

The RTP network shares many of the same capabilities and requirements as the FedNow service. However, there are differences. In this section, we explore fraud mechanisms and requirements as defined in the RTP network Operating Rules, such as accounts without posting, reports of fraud, and requests for the return of funds.

Participating FIs are formally required to act on alerts from The Clearing House related to suspected fraud events. In addition, participants must report fraudulent activity to The Clearing House. Such a report may be accomplished by using the fraud indicator to request a return of funds.

A key aspect of this network is with respect to the nature of the credit transfer requests (pac.008.001.08) being irrevocable. While there are mechanisms to attempt to recoup funds, which we will cover below, there is no right to cancel or amend a payment message once it has been sent to the RTP system. In addition, receiving participants are allowed to rely solely on the account number contained within the payment message for posting purposes. Similar to FedNow, name matches are not required.

As with the FedNow service, the RTP network enables participants to accept without posting. When responding to this message, the participant is granted additional time to research the transaction before making the funds available to the receiver or returning the transaction to the sender. Such a decision must be made by 11:59 p.m. local time on the next business day following the acceptance without posting a message. In either case, a response must be sent to the sending participant to make them aware. It should be noted that a receiving participant must also be a sending participant to return these funds via the RTP network. If not a sending participant, they must send the funds through another payment mechanism.

A request for the return of funds (camt.056.001.08) is considered a non-value message that a sending participant may use to request the return of a previous credit transfer message. The normal response time for a request for the return of funds (camt.029.001.09) by the receiving participant is ten banking days. However, this period may be extended for requests received with the "FRAD" indicator, which indicates potential fraud. In those cases, the receiving participant may need additional time to research the issue and there is no defined period for final response.

The RTP network Operating Rules define what happens with respect to erroneous and unauthorized RTP payments. Commercial payments are subject to the requirements of the rules in conjunction with UCC 4A. Consumer payments are subject to the requirements of the rules in conjunction with the Electronic Funds Transfer Act (EFTA or Reg E). The request for return of funds message is used to aid participants in recovering funds that may have been sent erroneously. However, the receiving participant has no obligation to return these funds if they are no longer available but is expected to cooperate to the extent it can with other participants regarding the recovery of erroneous payments.

A unique aspect of the RTP network designed to help prevent potential fraud is the use of Tokens. Token participants can pass token information instead of account details for credit transfer requests. Token use is optional, and participants are responsible for applicable compliance related to service use.

Third-Party Partnership

Third-party reliance for supporting instant payment services, including sending functionality, is a critical aspect of payment services in the financial sector today. It is of the utmost importance that a financial institution that leverages third parties has a solid third-party management program in place.

The Interagency Guidance on Third-Party Relationships for Risk Management[35] is a great resource to help an institution frame out how it should effectively manage its reliance on third parties. In this section, we provide an overview of the key considerations related to this framework.

Understanding which activities are critical within an organization is an important aspect of third-party management. When evaluating instant payment services, it is up the financial institution to identify if its reliance for supporting sending functionality falls under the umbrella of critical activities or not. Some things to consider when deciding on this include deciding if there is significant risk to the organization if the third party fails to meet its expectations and what impact there would be on the FI's accountholders if such failure occurs.

In today's payment ecosystem, third parties are far more than traditional vendors. They include a wide range of technology support firms, fintech companies, and other service providers. Given the evolving nature of these third parties, it is essential that financial institutions engaging with them for instant payment support clearly understand the nature of the relationship and the extent of their reliance on it. Is the third-party providing back-end technology support? Does it interface directly with end users? How is it integrated into the institution's overall business model for instant payments? Answering questions like these enables the financial institution to better categorize the third-party and assign an appropriate risk rating.

Once an FI has decided to work with a third-party, the process enters the Third-Party Relationship Life Cycle. This cycle includes the following key elements:

- Planning: Strategic understanding of what the organization wishes to accomplish and how a third-party fits into its business goals, objectives, and risk appetite. At this stage, the FI needs to determine an approach for instant payment, connection, and support.

- Due Diligence and Third-Party Selection: Vetting through a third-party is essential to the life cycle. Due diligence includes understanding how a third-party operates, its financial position, and insights into business continuity practices.

- Contract Negotiation: It is critical that the allocation of responsibility, liability, and SLA requirements are all appropriately defined during the contract negotiations.

- Ongoing Monitoring: Third-party management requires institutions to be proactive in managing these relationships. Critical elements include ongoing due diligence, performance against SLA, and BCP testing.

- Termination: When the relationship no longer serves the institution, it may become necessary to offboard a third-party. The framework defines these critical phases, with the need to verify contractual requirements, costs, and impact (such as data ownership).

In closing, it is important that organizations implement appropriate oversight of third-party risk management. This includes involvement at the board or board designee level with formalized reporting and program oversight. Organizations should also consider the appropriate use of independent program reviews, well-defined program documentation, and cooperation with supervisory agencies.

10) Compliance Programs Encompassing KYC/KYB & AML Obligations

Compliance with Operating Circular 8

Participants in the FedNow service are required to implement screening procedures to ensure that neither originators nor beneficiaries appear on current sanctions lists.[36] Additionally, they must develop and maintain a compliance program that aligns with sanctions laws and the terms of the FedNow service. This includes establishing a comprehensive framework in accordance with FinCEN regulations and the mandates of federal functional regulators.[37]

Adherence to RTP Network Rules

Institutions participating in the RTP network must clearly define and communicate OFAC compliance responsibilities to both senders and receivers, ensuring these obligations are incorporated into the legal agreements governing RTP usage. When addressing domestic payments, OFAC expects that US financial institutions are already screening their accountholders, both at onboarding and at regular intervals throughout the life of the account. With this exception, there is no requirement to screen incoming faster payments from either the FedNow service or the RTP network. However, it is essential that the financial institutions have a written OFAC compliance program in place, which is mandated by both the FedNow service's Operating Procedures and the RTP network's Operating Rules and Participation Rules.[38]

Domestic Transaction Focus

Currently, the FedNow service and the RTP network are restricted to domestic payments and do not support cross-border transactions. Compliance programs must address this limitation to maintain operational integrity.

Developing a Risk-Based Compliance Framework

To effectively manage the complexities associated with instant payment platforms, financial institutions should adopt a risk-based compliance framework. Factors to consider include geographic locations, the level of international exposure, the nature and history of accountholders' transactions, and the specific products and financial services offered. Institutional size and operational sophistication should also be evaluated.

Key components of this framework include:

- Establishing board and senior management accountability to promote a culture of compliance, provide necessary resources, and ensure proper oversight.

- Conducting ongoing risk identification and assessments to address fraud, misuse, and regulatory non-compliance risks, as well as monitoring transaction trends and emerging threats.

- Leveraging risk mitigation tools for real-time monitoring, fraud detection, and compliance validation, in addition to defining escalation procedures and alert triggers for suspicious activities.

- Performing regular validation and testing of risk controls through independent reviews and stress testing to identify vulnerabilities and enhance defenses.

- Implementing employee training programs to raise awareness of compliance responsibilities and improve the ability to detect fraud and sanctions risks. Training materials should be updated regularly to reflect changes in regulations and industry standards.

Bank Secrecy Act / Anti-Money Laundering Considerations

Both the FedNow service and the RTP network require financial institutions to implement compliance programs aligned with the Bank Secrecy Act (BSA), Anti-Money Laundering (AML), and sanctions laws to effectively manage risks associated with payments activities. Monitoring systems should include FedNow and RTP transactions in the same manner as other payment methods to detect suspicious or anomalous activity.

User Agreements

Institutions should establish a robust Customer Identification Program that uses commercially reasonable methods to verify user identities. User agreements should bind senders to the rules and guidelines of the instant payment rail. These agreements must be reviewed at least annually and should outline exposure limits and provide mechanisms for adjusting these limits as needed. Whether drafted internally or by a vendor, agreements should undergo legal review and be approved by the Board of Directors.

Federal Reserve Banks Operating Circular No. 5

Electronic Access Operating Circular No. 5 outlines the terms under which an institution accesses services and applications provided by a Reserve Bank, including the exchange of certain data. It addresses security requirements, service providers, and the risks and liabilities associated with maintaining an electronic connection to a Federal Reserve Bank. The circular also specifies the minimum self-assessment a financial institution should conduct regarding security procedures, operating instructions, and guidelines related to the electronic connection, as well as expectations for confidentiality and data security.[39]

Operating Circular No. 5 describes the minimum self-assessment a financial institution should conduct on security procedures, operating instructions, and guidelines involved with the electronic connection and outlines the expectation of confidentiality and data security.

UCC4A Considerations

Sending instant payments must adhere to UCC4A. If sending instant payments, the payment-related information is secure especially with health care and within the HIPPA standards (Health Insurance Portability and Accountability Act of 1996). UCC4A also addresses security procedures when sending instant payments. How often are these procedures reviewed and are organizations ensuring they are adhered to based on their agreements? Lastly, if these security procedures are not followed, is the deviation documented and who has the approval for allowing this deviation?[40]

11) Exception Processing

Managing Exceptions in Instant Payments

When processing instant payments, sending FIs should consider implementing various checks on accountholder-initiated transactions before transmitting them into the instant payment network. One of the most common exceptions encountered is insufficient funds. These transactions should be promptly rejected at the user interface level, with clear messaging indicating that the Sender's account lacks sufficient funds. Institutions must also evaluate whether to allow transactions to proceed into overdraft tolerances or whether instant payment initiation should be restricted for accounts with uncollected balances.

In addition to account balance checks, sending FIs should enforce limitations on the dollar amount accountholders are permitted to send. Institutions must decide how to manage transactions exceeding these limits and whether to apply consistent processes across consumer and business accounts. For example, hard limits may be applied to consumer accounts, automatically rejecting transactions exceeding the threshold. Conversely, business accounts might operate under soft limits, enabling over-limit transactions to be submitted for manual review before being released into the instant payment network.

Fraud Screening and Operational Oversight

Beyond funds availability and transaction limits, institutions should also consider implementing fraud screening measures. While specific fraud mitigation strategies are detailed in the Fraud Mitigation section of these guidelines, operational considerations around exception handling are critical. For example, when a transaction is flagged for review during fraud screening, it is essential to ensure that the sender has visibility into the transaction's status. This requirement is unique to instant payments, where accountholders expect near-immediate processing.

If a transaction enters a review queue, senders should be notified promptly, with real-time updates as the payment status changes. The immediacy of instant payments means accountholders may need to complete their transactions quickly and could opt to cancel flagged transactions in favor of alternative payment methods. Institutions should establish service-level agreements for completing fraud reviews to set clear expectations for accountholders. These SLAs must account for escalations to specialized teams, such as BSA/AML departments, and should include efficient communication and resolution processes. Throughout this process, senders must be provided with tools to monitor the status of their payment in real time.

OFAC Screening

Financial Institutions may also choose an Office of Foreign Assets Control (OFAC) compliance program which may necessitate screening on all transactions before processing. Depending on the program's design, exception handling may need to be analyzed. As with fraud screening, it is critical to develop mechanisms to keep senders informed about payment statuses and establish an escalation process for flagged transactions. Instant payments and their corresponding SLAs, combined with their irrevocable nature, may necessitate changes to an institution's approach to OFAC screening. Many institutions are transitioning from batch screening to real-time screening to better align with the immediacy of instant payments.

In scenarios requiring additional adjudication, institutions must implement proper controls and procedures to manage potential sanctions risks. These exceptions should be accounted for in exception handling and operational planning, ensuring compliance while maintaining seamless accountholder experience.

Reporting Fraud

Robust fraud controls must be established regardless of whether the transaction is facilitated by a financial institution or a fintech. Key components of these controls include fraud identification, escalation, remediation, internal reporting, and network reporting. Institutions should ensure these elements meet network compliance standards and support broader business requirements. Proper reporting mechanisms enable institutions to address fraudulent activities effectively while maintaining transparency and trust within the payment network.

Request for Return of Funds

Although instant payments are irrevocable by design, the Request for Return of Funds (RfRF) functionality provides a messaging mechanism for institutions to collaborate in retrieving funds sent erroneously or in cases of fraud. Common scenarios requiring RfRF handling include unauthorized payments, accountholder errors, and potential fraudulent transactions. Institutions must implement systems and processes to manage these requests efficiently while adhering to compliance and operational standards.

Inbound RfRFs also require careful exception handling. Recipients are generally allotted ten business days to research and respond to RfRF messages, although additional time may be required for complex scenarios, such as fraud or warranty claims. Institutions must ensure they have robust research and response processes in place to address these exceptions comprehensively.

To facilitate cooperation, participants are expected to work together and with The Clearing House and the Federal Reserve to address unauthorized and erroneous payments, as outlined under Article 4-A of the New York Uniform Commercial Code and the Electronic Funds Transfer Act (EFTA). By fostering collaboration and accountability, institutions can uphold the integrity of the instant payment network while ensuring efficient resolution of exception cases.

Staffing Considerations

The nature of instant payments lends itself to and requires a higher level of automation and will result in a significant reduction in the number of payments that are typically encountered in traditional exception processing. However, unlike traditional payment rails, users of instant payments will expect a higher level of responsiveness and shorter delays when payments encounter an exception scenario. While the number of staff required to manage exception processing may be drastically reduced, the availability of staff to address payment exceptions will likely need to increase, particularly to cover after-hours, weekends, and holidays. Institutions will need to consider how this need will impact staffing in departments that support instant payments.

12) Mechanisms for Achieving Performance Requirements

In the fast-paced landscape of instant payments, ensuring high performance for the initiation of transactions on the sending-side is essential. From a business and user perspective, send-side performance is defined by the ease and speed with which users can initiate payments, while technically, it entails the infrastructure needed to meet these demands efficiently.

For send-side transactions, the RTP network and the FedNow service set ambitious SLAs of completing payments within 15-20 seconds end-to-end. This demands not only high-speed processing but also systems that enable users to initiate transactions seamlessly 24x7x365. This section focuses on the various considerations for supporting the send-side capabilities for the RTP network and the FedNow service.

While both sending and receiving transactions necessitate high availability, performance, and infrastructure reliability, the following components are specifically critical for the send-side:

1. High Performance and Availability of Systems: Send-side systems must always be available and responsive to support 24x7x365 payment initiation. Additional features like real-time fraud prevention and sender verification introduce complexity that requires low-latency, high-performance infrastructure. Additional monitoring of server storage and system capacity is vital for proactively addressing storage limitations and maintaining system performance.

2. Modernized Cloud Architecture: Send-side demands for cloud solutions and microservices are often higher due to the need for scalability, particularly to manage high-frequency transaction initiation. Send-side instant payments require cloud environments designed for real-time initiation, including sender verification, fraud checks, and compliance screening. Systems must operate in active-active, multi-region setups with auto-scaling to support outbound volume surges. Observability tools should monitor latency, throughput, and failure rates to maintain SLA compliance. Microservices and containerization enable rapid updates to payment workflows, while infrastructure-as-code ensures reliable, repeatable deployments. Unlike passive receive-side systems, send-side cloud infrastructure must sustain constant outbound activity, requiring real-time elasticity, fault tolerance, and low-latency responsiveness.

3. Optimized Workflow Design: On the send side, workflows must be structured to manage payment initiation swiftly, routing transactions to necessary fraud and compliance checks in parallel. This differs from receive-side flows, which are typically simpler.

4. Straight Through Processing (STP) for Outbound Payments: STP is crucial on the send side to minimize manual interventions. Payment instructions should be processed automatically through systems that ensure compliance, verification, and fraud checks are passed seamlessly.

5. Scalable Solution: Scalability is especially important for the send side due to higher volumes of outbound payments during peak times. Systems should be prepared to manage increased demand in real-time without delays that could affect user experience.

6. API Performance Requirements: Send-side APIs must support high-volume, low-latency transaction initiation with consistent uptime and fast failover. They must include idempotency, timeout handling, and structured error responses to prevent duplicate or failed sends. APIs should execute balance checks, fraud screening, and compliance validations in parallel and support asynchronous callbacks for real-time status updates. Unlike receive-side APIs, send-side endpoints often face external users and must meet stricter authentication, observability, and SLA tracking standards. Real-time monitoring and detailed logging are essential to detect issues and maintain network performance commitments.

7. Enhanced Security Protocols: On the send side, there is a higher emphasis on security and authentication measures since it involves initiating payments and releasing funds. The send-side process requires additional layers of identity verification, such as multi-factor authentication (MFA), biometric verification, and enhanced accountholder authentication protocols to prevent unauthorized access. This is critical to protect against fraud and to comply with regulatory requirements related to outbound transactions.

8. Fraud Detection and Prevention Systems: Unlike the receive side, which primarily involves accepting incoming funds, the send side is more vulnerable to fraudulent activity due to the risk of unauthorized payments. Therefore, real-time fraud detection mechanisms, such as anomaly detection algorithms, transaction pattern analysis, and velocity checks, are essential to detect suspicious behaviors before funds are transferred. Fraud prevention must operate without compromising speed, necessitating advanced AI-driven solutions that can flag and stop fraudulent transactions instantly.

9. Payment Velocity and Limit Controls: The send side must implement controls to manage payment velocity and enforce transaction limits, as high volumes of outbound payments can increase exposure to potential fraud and overdrafts. These controls allow financial institutions to limit the frequency and amount of transaction throughput based on user behavior, reducing risk while maintaining regulatory compliance.

10. Sender Verification and Validation: On the send side, verifying the sender's account status, available balance, and transaction history is crucial to ensure that funds are available before the transaction is initiated. Systems must check the availability of funds in real-time and perform account validations to avoid overdrafts and failed transactions, which are typically less stringent on the receive side.

11. Real-Time Outbound Routing Optimization: The send side requires optimized routing mechanisms to determine the most efficient and reliable pathway for transmitting payments. Unlike the receive side, where the transaction routing path is fixed, the send side must dynamically assess various pathways to meet SLAs. Outbound routing systems that consider factors such as network congestion, transaction fees, and latency are necessary to ensure timely and cost-effective payments.

12. Compliance with Outbound Payment Regulations: Sending payments involves more complex compliance requirements, including KYC, AML, and transaction monitoring standards. Institutions must implement compliance checks for each outbound payment to ensure regulatory adherence, which may not be as stringent on the receive side. Automated compliance processes, integrated directly within the payment initiation workflow, are essential for reducing regulatory risk.

13. Automated Reconciliation for Outbound Transactions: Send-side transactions benefit from real-time reconciliation processes that ensure account balances are updated instantly after a transaction is initiated. This prevents issues like overdrafts and allows for accurate, up-to-the-moment balance reporting. Automated reconciliation processes also help in managing exceptions and resolving issues before they affect downstream systems, which is generally less critical on the receive side.

14. Payment Status and Exception Management: The send side requires systems to track the status of initiated payments closely and manage exceptions, such as failed or delayed transactions. Implementing real-time monitoring and alert systems is crucial to ensure that send-side transactions meet SLA targets. This may include generating automated responses to Payment Status Requests (PSRs) and triggering resolution processes for any exceptions that arise, which is often less demanding on the receive side.

15. Cost and Fee Management: Send-side payments often incur transaction fees, especially in cross-border or instant payments, where different networks, partners or correspondent banks may be involved. Systems must account for fees and manage cost allocation accurately. Additionally, some institutions may pass transaction costs on to accountholders, necessitating clear fee visibility within the payment initiation interface.

16. Intra-Network Performance Monitoring Communication: Communication within the payment network is another critical component of performance monitoring. Institutions using vendor connections to facilitate network connectivity must maintain open lines of communication with vendors, network overseers, and other participants. This collaboration ensures transparency regarding payment statuses and network availability. For network participants, intra-network communication is expected and essential. Participants should be prepared to engage with other participants to address payment statuses and system availability. Similarly, timely responses to communications from network operators about negative scenarios, network statuses, and other critical updates are crucial for maintaining operational integrity. A proactive approach to intra-network communication helps mitigate disruptions and reinforces trust across the payment ecosystem.

This highlights the extra layers and considerations essential for effective send-side processing of the FedNow service and the RTP network transactions, ensuring secure, compliant, and efficient outbound payment handling. These additional requirements reflect the more complex nature of initiating transactions as opposed to simply receiving them.

Conclusion

In conclusion, these guidelines provide a comprehensive overview of the operational considerations for financial institutions implementing instant payments "send" capabilities, focusing on the FedNow service and the RTP network. It emphasizes the importance of understanding instant payment send flows, navigating the complexities of interoperability and routing, and optimizing the user experience for both accountholders and FI staff. Furthermore, the document stresses the necessity of robust liquidity management, real-time reconciliation practices, and business continuity planning to ensure seamless and resilient operations in the 24x7x365 instant payment environment.

A key takeaway is the critical role of robust fraud mitigation and compliance programs in safeguarding against the heightened risks associated with the speed and irrevocability of instant payments. The document highlights the need for proactive measures such as digital profiling, real-time fraud screening, and adherence to KYC/KYB (Know Your Business) and AML obligations, alongside continuous employee training and accountholder education. It also emphasizes the value of third-party partnerships and leveraging advanced technologies such as AI and machine learning to enhance fraud detection and prevention capabilities.

Ultimately, successfully implementing instant payment send capabilities requires a comprehensive approach that balances innovation, efficiency, and risk management. Financial institutions must carefully consider their staffing needs, accountholder disclosures, and exception processing mechanisms to deliver a secure, dependable, and user-friendly payment experience. By adhering to the best practices and considerations outlined in this document, FIs can unlock the full potential of instant payments to drive innovation, improve accountholder satisfaction, and maintain a competitive edge in the evolving payments landscape.

Acknowledgements

Operational Considerations for Instant & Immediate Payments Work Group

Thank you to the members of the FPC Operational Considerations for Instant & Immediate Payments Work Group (OCWG), sponsored by Endava, who contributed to these guidelines.

OCWG Leadership

Form3 US Inc.	Miriam Sheril (Chair)
FirstBank	Tony Cook (Vice Chair)

OCWG Contributors

FPC Member Organization	Representative
1st Source Bank	Steve Group
1st Source Bank	Sabrina Keel
Alloya Corporate FCU	Lisa Richmond
BHMI	Donna Blum
BOK Financial	Dana Woller
Corporate One	Martha Dixie
Cross River Bank	Sai Kailash
EPCOR	Sharon Hallmark
Fintech Consulting, LLC	Marcia Klingensmith
FirstBank	Maranda Blake
JJ4Tech	Caroline Serejo Cypriano
Nacha	Mark Dixon
North American Banking Company	Ryan McNaughton
PaymentsFirst Inc.	Mary Gilmeister
PaymentsFirst Inc.	Jeanette Waye
RedCompass Labs	Stephen King
Reef Karson Consulting, LLC	Rodman Reef
Serio Payments Consulting	Anthony Serio (Editorial Review)
UMACHA	Kimberly Stachak
US Bank	Dustin Martin
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 change that instant and immediate payments have on bank operations.

References

[1] Note: “Instant” and “real-time” payments are used interchangeably throughout this document. Instant payments (also known as immediate or real-time) are an electronic payment solution available 24x7x365. They result in the immediate interbank clearing of the transaction and crediting of the payee’s account, with confirmation to the payer within seconds of payment initiation. In contrast, "RTP" is a trademark for the real-time payments network owned and operated by The Clearing House. Source: https://fasterpaymentscouncil.org/Glossary-of-Terms

[2] Faster Payments Council. (2024, September). *Operational Considerations for Receiving Instant Payments.* https://fasterpaymentscouncil.org/userfiles/2080/files/OCWG_Operational%20Considerations%20for%20Receiving%20Instant%20Payments%20Guideline_09-12-2024%20Final.pdf.

[3] The Federal Reserve. (2017, August 9). *Final Guidelines for Evaluation Joint Account Requests*. https://www.federalreserve.gov/newsevents/pressreleases/files/other20170809a1.pdf.

[4][8][15] The Clearing House. (2025, July 21). *RTP® Operating Rules*. https://www.theclearinghouse.org/-/media/New/TCH/Documents/Payment-Systems/RTP/RTP_Operating_Rules_Effective_07-21-2025.pdf?rev=ee80c7bbc8df4a869f5046f0f5baaae1&hash=A975411FB4F361D22663822DF5DB48B8.

[5] Marek, L. (2025, February 27). FedNow boosts send option to $1M. *Payments Dive*. https://www.paymentsdive.com/news/federal-reserve-fednow-instant-payments-increased-send-option/741077/

[6] The Clearing House. (2025, June 26). *Breaking Barriers: RTP® Network $10 Million Transaction Limit Spurs High-Value Payment Surge* https://www.theclearinghouse.org/payment-systems/Articles/2025/06/RTP-10m-Limit#:~:text=RTP%20Network%20%2410%20Million%20Transaction,Payment%20Surge%20%7C%20The%20Clearing%20House.

[7] FedNow. (2024, November 4). *FedNow® Service adds net send limit feature to help correspondents manage liquidity.* https://explore.fednow.org/explore-the-city?id=3&postId=73&postTitle=fednow%C2%AE-service-adds-net-send-limit-feature-to-help-correspondents-manage-liquidity

[9] Faster Payments Council. (2025, January). *Guideline.02: Operational Considerations for Instant Payments Send-Side Primer.* https://fasterpaymentscouncil.org/userfiles/2080/files/OCWG_Guideline_02_Operational%20Considerations%20for%20Instant%20Payments%20Send%20Side%20Primer2_01-13-2025%20Final.pdf.

[10] J.P. Morgan. (n.d.). *The Second Payments Services Directive: A Catalyst for Innovation*. Retrieved September 15, 2025, from https://www.jpmorgan.com/insights/payments/payments-optimization/psd2.

[11] The Clearing House. (n.d.). *RTP®: Frequently Asked Questions.* Retrieved September 15, 2025, from https://www.theclearinghouse.org/payment-systems/rtp/institution; and FedNow. (n.d.). *Resources*. https://explore.fednow.org/resources.

[12] The Clearing House. (n.d.). *RTP®: Real-Time Payments for All Financial Institutions.* Retrieved September 15, 2025, from https://www.theclearinghouse.org/payment-systems/rtp.

[13] The Federal Reserve Financial Services. (2025, April). *FedNow® Service Operating Procedures.* https://www.frbservices.org/binaries/content/assets/crsocms/resources/rules-regulations/0429-fednow-service-operating-procedures.pdf.

[14] [27] FedNow. (n.d.). *Operating Procedures.* Retrieved September 15, 2025, from https://explore.fednow.org/explore-the-city?id=5&building=operating-center&resource=95&role=fi_spe&resourceTitle=operating-procedures.

[16] Office of the Comptroller of the Currency. (2023, June 6). *Third-Party Relationships: Interagency Guidance on Risk Management.* https://www.occ.gov/news-issuances/bulletins/2023/bulletin-2023-17.html.

[17] Nacha. (2023, October). *Enhancing Operational Resilience for ACH Network Participants.* https://www.nacha.org/sites/default/files/2023-10/Enhancing_Operational_Resilience_for_ACH_Network_Participants_FINAL.pdf.

[18] Faster Payments Council. (n.d.). *Use Case Repository.* Retrieved September 15, 2025, from https://fasterpaymentscouncil.org/use-cases.

[19] The Clearing House. (n.d.). *RTP® Participating Financial Institutions.* Retrieved September 15, 2025, https://www.theclearinghouse.org/payment-systems/rtp/rtp-participating-financial-institutions.

[20] The Federal Reserve Financial Services. (n.d.). *FedNow® Service Participants and Service Providers*. Retrieved September 15, 2025, from https://frbservices.org/financial-services/fednow/organizations.

[21] Nacha. (n.d.). *How to Become an AFPP*. Retrieved September 15, 2025, from https://www.nacha.org/accredited-faster-payments-professional.

[22] National Archives. (2025, September 15). *Part 210—Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through the FedWire Funds Service and the FedNow Service (Regulation J)*. https://www.ecfr.gov/current/title-12/chapter-II/subchapter-A/part-210.

[23] National Archives. (2025, September 15). *Part 229— Availability of Funds and Collection of Checks (Regulation CC).* https://www.ecfr.gov/current/title-12/chapter-II/subchapter-A/part-229.

[24] Uniform Law Commission. (n.d.). *Uniform Commercial Code*. Retrieved September 15, 2025, from https://www.uniformlaws.org/acts/ucc.

[25][26][39] The Federal Reserve Financial Services. (n.d.). *Operating Circulars*. Retrieved September 15, 2025, from https://www.frbservices.org/resources/rules-regulations/operating-circulars.html.

[28][29][38] The Clearing House. (n.d.). *RTP®: Document Library*. Retrieved September 15, 2025, from https://www.theclearinghouse.org/payment-systems/rtp/document-library.

[30] Nacha. (2022, September). *A New Risk Management Framework for the Era of Credit-Push Fraud*. https://www.nacha.org/sites/default/files/2022-09/9.22%20Risk%20Management%20Framework.pdf?.

[31] Faster Payments Council. (n.d.). *Faster Payments Resources*. Retrieved September 15, 2025, from https://fasterpaymentscouncil.org/Guides-Research.

[32][33] The Federal Reserve. (n.d.). *FraudClassifier℠ Model.* Retrieved September 15, 2025, from https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/fraudclassifier-model/; and *ScamClassifier℠ Model.* Retrieved September 15, 2025, from https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/scams/scamclassifier-model/.

[34] FedNow. (n.d.). *Managing Fraud Risk*. Retrieved September 15, 2025, from https://explore.fednow.org/resources/fraud-at-a-glance.pdf.

[35] National Archives. (n.d.). *Federal Register Documents*. Retrieved September 15, 2025, from https://www.federalregister.gov/.

[36] OFAC. (2022, September). *Sanctions Compliance Guidelines for Instant Payment Systems.* https://ofac.treasury.gov/system/files/126/instant_payment_systems_compliance_guidance_brochure.pdf.

[37] The Federal Reserve Financial Services. (2024, April 22*). Federal Reserve Banks Operating Circular No. 8: Funds Transfers Through the FedNow® Service*. https://www.frbservices.org/binaries/content/assets/crsocms/resources/rules-regulations/042224-operating-circular-8.pdf.

[40] OFAC. (2022, September). *Sanctions Compliance Guidelines for Instant Payment Systems.* https://ofac.treasury.gov/media/928316/download?inline; and Financial Crimes Enforcement Network. (n.d.). *FinCEN's Mission*. https://www.fincen.gov/.