Operational Considerations for Receiving Instant Payments

Fasterpaymentscouncil.org

September 2024

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.

The Clearing House Payments company did not write this document and is not responsible for any inaccuracies about the RTP®[1] Network, the laws and regulations relevant to instant payments, or payment systems generally.

The advent of instant payments has revolutionized the financial landscape, offering unparalleled speed, convenience, and efficiency. As financial institutions embark on their journey to adopt instant payment capabilities, they must navigate a complex array of operational considerations to ensure a smooth and successful implementation.

Following the "Operational Considerations for Instant Payments Receive-Side Primer,"[2] these guidelines explore the critical aspects of enabling instant payment receipt. Adapting existing payment flows, managing liquidity, mitigating fraud risks, and handling exceptions are key priorities for financial institutions. Additionally, the implications of instant payments on staffing needs and training requirements are examined, ensuring organizations are well-equipped to embrace this transformative technology. These guidelines cover the intricacies of instant payments and provide a framework for successful adoption.

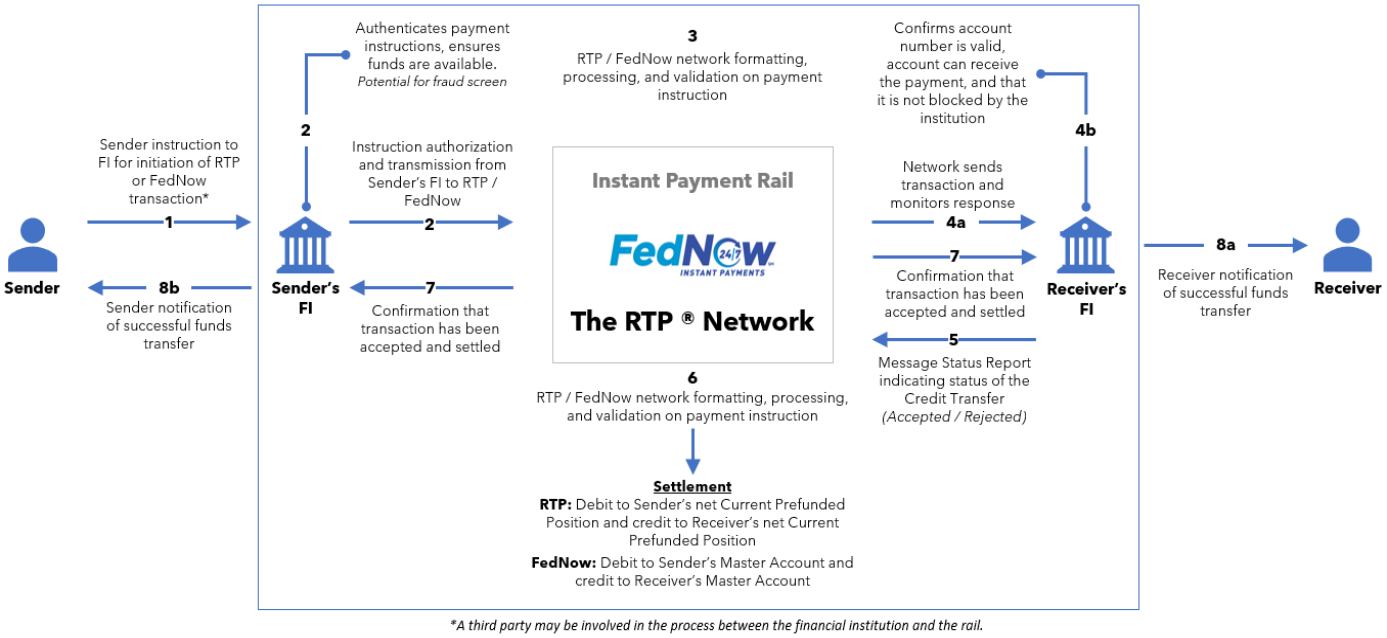
New Flows/Processes in Relation to Existing Payment Flows

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 receiving institution receives an ACH file or accepts a wire payment.

While both the RTP® Network and the FedNow® Service require an immediate confirmation of receipt and acceptance 24x7x365, neither ACH nor wires require a response. 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 receiving institution to return the payment for various reasons. However, the instant payment rail supports an automated, immediate rejection, whereas ACH and wires can accommodate a manual review and can result in a later return through a manual process.

RTP® and FedNow® Message Flows



A third party may be involved in the process between the financial institution and the rail.

This section will point out considerations for sending institutions throughout the process flows but will not provide the level of detail that will be covered in the receive processes. Future publications will focus in greater detail on considerations for sending institutions.

1. The sender (an individual or business) initiates a payment with their financial institution (FI), who is a participant in the instant payment network, through an interface provided by the financial institution such as an online or mobile banking application.

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. Another consideration for sending financial institutions must be fraud controls. System limitations should be set based on the financial institution's risk appetite and "knowing your customer." Additional fraud screening of transactions may be performed including sender's behavioral patterns, device recognition, or login history. Financial institutions will need to consider how to implement such fraud screening systems and the staffing to support them.

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:
    a. the message is properly formatted and not future-dated.
    b. the routing number belongs to a network participant.

4. The network sends the transaction to the receiver's financial institution and monitors for a response. The receiver's financial institution then receives the 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 in five seconds or less, including processing time, any OFAC/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 alerted. The financial institution may choose to respond to the incoming message with the "accept without posting"[3] response which would instruct the network to settle the payment but also allow the financial institution additional time to review the alert and make a final determination to return the payment or make funds available to the receiver. Operational considerations for managing these exceptions including systems and staffing will be discussed in more detail in the Exception 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 settlement account and credit the receiver's financial institution settlement account. For the RTP network, this will be the shared prefund balance account 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 the FedNow Service. In both networks settlement could occur through funding agents/ correspondent bank 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 and settled.

8. 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. When confirmation of acceptance or rejection of the message is received from the network, the sender's financial institution notifies the sender of the status of the payment.

Liquidity Management

Cash management and liquidity management are interconnected yet distinct concepts within the realm of finance. Cash management primarily concerns itself with the day-to-day oversight of cash flows and balances, ensuring that an entity possesses sufficient liquid funds to meet immediate financial obligations. On the other hand, liquidity management adopts a broader perspective, encompassing both short-term and long-term considerations related to cash and other liquid assets, as well as various financial instruments. Its overarching goal is to maintain financial stability while optimizing the utilization of financial resources across different time horizons.

Traditionally, financial institutions have relied on legacy batch systems for payment processing, enabling them to forecast cash flows and guide cash management effectively. However, the advent of real-time payments and continuous 24x7x365 payment processing has introduced a new dynamic to managing cash flows.

In today's fast-paced financial landscape, both cash and liquidity management have become critical components of modern financial systems. An organization's capital requirements strategy is intricately linked to its ability to provide accurate reporting of available liquidity, which can be challenging. The introduction of real-time gross settlement instant payment schemes, such as in the United States, has added new dimensions to this task, with multiple cash positions to manage simultaneously, including RTP prefunded positions, CHIPS® prefunded positions, and Federal Reserve Master Account.

Real-time recognition of funds necessitates real-time account reconciliation to maintain up-to-date, timely, and accurate account positions. Even for institutions primarily receiving value from other network participants, monitoring, and managing these pools is essential for projecting future account needs. Automated reconciliation tools in real-time play a pivotal role, enabling continuous transaction matching and swift identification of discrepancies, allowing for prompt corrective action when necessary. In this rapidly evolving financial landscape, robust cash and liquidity management practices are indispensable for financial institutions to thrive and adapt to the changing dynamics of the industry.

As payment systems become faster and more real-time, effective cash management becomes paramount as it provides greater opportunities for cash earnings and investments. Financial institutions should adapt their cash management strategies to ensure they have the necessary funds to facilitate transactions and manage their cash flow effectively. Here are some key considerations:

- Real-Time Settlement
    - In a real-time payments environment, individual transactions settle instantly or within seconds. This means that liquidity needs to be readily available to ensure outbound payments across all payment rails can be processed. Without sufficient funding, some payments may not be processed.

- Intraday Liquidity Monitoring
    - Continuous monitoring of intraday liquidity positions is crucial in a real-time settlement payment system. This involves tracking incoming and outgoing payments throughout the day.

    - Financial institutions should ensure they maintain positive balances to prevent overdrafts and payment failures. For example, it should be noted that financial institutions cannot overdraw their position on the RTP Network. Additionally, financial institutions maintaining a settlement account under the FedNow Service are required to maintain actually and collected funds in that account to settle FedNow transactions, consistent with Federal Reserve policies, including but not limited to the Federal Reserve Policy on Payment System Risk.

    - Consideration should be given to always monitoring and managing all the existing liquidity positions.

    - System downtime may be predictable, system outages and gateway outages are not and introduce the need for stand-in processes, dual site systems, and redundant processing during these periods. When leveraging stand-in processing solutions, the receiving institution is still obligated to post the payment to the recipient in accordance with network rules. For the RTP Network this means ensuring proper pre-funding as well as the ability to redirect/invest excess funds.

- Access to Central Bank Facilities
    - Liquidity Management Transfers (LMT) in the FedNow Service are used to support liquidity needs related to payment activity in the FedNow Service or another instant payment system backed by a joint account at a Reserve Bank. LMT is currently available for use between the hours of 7PM – 7AM ET Monday – Friday (excluding holidays) and 24 hours on weekends and Federal Reserve holidays.

- Stress Testing & Scenario Analysis
    - Stress testing and scenario analysis help institutions assess their liquidity resilience in extreme situations. These exercises can identify vulnerabilities and help institutions prepare for unexpected liquidity shocks. This is extremely important as the FedNow Service is a new method of receipt and payment and as such there is no historical data to derive trends and patterns.

- Collateral Management
    - Some institutions may use collateralized borrowing to meet liquidity needs.

- Regulatory Compliance
    - Regulatory requirements regarding liquidity management may vary by jurisdiction. Institutions must ensure compliance with these regulations, which may include liquidity risk management standards and reporting requirements.

- Partnerships and Liquidity Pools
    - Financial institutions may form partnerships or participate in liquidity pools to collectively manage liquidity and optimize cash positions.

- Technological Infrastructure
    - Robust and scalable technology infrastructure is essential for real-time liquidity management. This includes efficient payment processing systems, real-time monitoring tools, and secure data analytics capabilities.
    - As noted above, provision for stand in processing during planned and unexpected network and application outages.

<u>Resources to Consider:</u>

- Predictive Analytics
    - To manage liquidity effectively, financial institutions can use predictive analytics and modeling to forecast payment flows, actionability and anticipate liquidity needs.
    - Artificial intelligence (AI) can improve the ability to forecast future liquidity needs, but a more important development will be the ability of AI to support confident decision-making using the output from those predictions.

- Automated Liquidity Management Tools
    - Automation is key to managing liquidity in real-time. Automated tools can help optimize cash positions and initiate fund transfers as needed.
    - Automated sweeps, transfers, and overdraft alerts can be integrated into liquidity management systems.

- New Reporting Tools
    - The Federal Reserve provides balance reports and has FedNow reports to assist with account management and reconcilement functions.
    - Real-time balance inquiry reports are available via the FedNow *S*ervice and the Account Management Information (AMI) application.
    - The RTP Network also provides end-of-day reports on the transactions that take place each day for a participant as well as for funding agents.
    - The RTP Network Volume Calculator estimates how many RTP transactions a depository institution will receive each month based on asset size.
    - The Clearing House provides functionality through APIs to request reports from the RTP Network in real-time to support liquidity management.

Liquidity management in a real-time gross settlement faster payments world requires financial institutions to be agile, technologically advanced, and proactive in monitoring and forecasting their liquidity needs. With the right tools, strategies, and regulatory compliance, they can navigate the challenges and opportunities presented by the evolving payments landscape.

Business Continuity & Resilience

Payments are critical to the efficient functioning U.S. financial system, and financial institutions can mitigate risk with a focus on business continuity and operational resiliency. Business continuity and disaster recovery practices prepare financial institutions for response to disruptions both planned and unplanned. Operational resiliency has built upon this practice to enhance proactive measures and minimize downtime during system issues, as well as document, communicate, and benefit from lessons learned during disruption to business-critical operations.

Despite the absence of prescriptive U.S. regulations on Business Continuity and Operational Resiliency, U.S. regulatory bodies including the Office of the Comptroller of the Currency (OCC), the U.S. Department of the Treasury, and the Federal Financial Institutions Examination Council (FFIEC) offer advisory and best practices for financial institutions' operations. Further, payments-oriented continuity and resiliency guidance from the Federal Reserve and Nacha on services including ACH and Fedwire® Funds Service can be leveraged as financial institutions expand their focus to real-time payments operational risk.

Financial institutions who support both instant payments (RTP Network and/or FedNow) and debit card transactions from a single core system, should be mindful about the availability of credits made during the off-line period. An in-bound instant payment credit made when the core is off-line will not be visible to the debit card system (e.g., at an ATM) and a deposit made with a debit card (e.g., at an ATM) will not be available to be sent as an instant payment while the core is off-line.

To meet the instant network rules, FIs with cores that go off-line for nightly batch processing should determine how they can make funds received through the instant payment network immediately available to other payment channels including the card system. There are several options including memo posting on a server outside the core and updating the core when it is back on-line.

Business-critical operations specific to instant payments systems RTP Network and FedNow come from the introduction of 24x7x365 operations, automated reconciliation, and what is for many an increased dependency on third-party service providers (TPSPs). Financial institutions are encouraged to take such factors into consideration as they conduct their periodic review of documented policies, procedures, and Business Continuity & Disaster Recovery (BCDR) plans for business continuity and operational resilience.

Uptime Requirements

The RTP and FedNow networks operate 24x7x365 and as such, expect their participants to operate in that manner as well. However, they understand that downtime may be needed and have thus provided expectations/requirements to ensure minimal disruption to the network and end users. It is important that financial institutions understand the uptime requirements for the network(s) to which they are connecting. The timing of planned downtime as well as how many consecutive hours an institution can be offline will vary by network. For instance, FedNow currently expects that planned downtime will not exceed two consecutive hours, or twenty-four hours total per quarter.

The Federal Reserve does not have specific downtime windows but expects participants to plan their downtime when expected transaction volume is minimal. FedNow and RTP also provide sign on/off and connect/disconnect functionality, including broadcasts, to help participants manage downtime. The RTP network expects participants to have at least 99.5% continuous connectivity, with the goal of requiring a 99.9% connectivity standard in the future. The Clearing House allows participants to utilize a maintenance window for scheduled maintenance and will not count the first eight hours per calendar month towards their continuous connectivity requirement. The maintenance window is over a period of four hours every Sunday between 2:00AM and 6:00AM ET.

Understanding the requirements as well as how the financial institution performs maintenance will be imperative. Conversations should occur early in the process to understand potential points of failure, identify mitigation or remediation steps, and assign owners to ensure internal processes or maintenance procedures can meet network requirements. Financial institutions may consider implementing "stand-in processing" to minimize the impact of downtime.

Additionally, there will be times when a financial institution must utilize unplanned downtime and sign off the network. In these situations, it is important to have a plan in place to ensure the networks are notified and can collaborate and provide guidance on next steps. Particular consideration should be given to managing accountholder and end user reactions to downtime amidst expectations of 100% availability. Regardless of the type of downtime being utilized, there are operational considerations which are important to think through. For instance, identifying individuals to serve as the point of contact and notify the network(s) of downtime, understanding the process, as well as who will be responsible for signing off and on the network, and any escalation procedures that should be considered. These considerations, especially processes for signing off during downtime, are critical to preserving the health of the instant payment networks.

If an accountholder's experience is going to be impacted due to downtime, the best practice is to communicate directly with accountholders and provide any applicable information or expected timing. Financial institutions should consider if, when, and how best to communicate this information to accountholders.

Financial institutions should also consider how they will stay appraised of other participants' downtime, to ensure rejected messaging is minimized.

Lastly, understanding how a financial institution ensures it meets the network(s) requirements is critical. A few questions to consider: Is this something a Third-Party Service Provider (if applicable) will provide, or will the financial institution need to build out a method to monitor this in a different manner? Will the financial institution be alerted—or does it have alerts built out—to notify applicable teams when unexpectedly signed off the network? Having a plan and ways to monitor this will ensure the financial institution is not only meeting the requirements, but also provides the opportunity to identify a potential issue as quickly as possible.

Weekend & Evening Support

Adoption of real-time payment schemes drives the necessity to reevaluate operational resiliency and adapt to providing services 24x7x365, including provision of weekend and evening support. An expansion of critical payments operations to weekends, evenings, and holidays introduces material operational risk as compared to the existing support structure built around batch processing windows and traditional business hours.

Financial institutions must establish documented processes for handling off-hour operations. Mapping exercises and scenario testing can expose operational interdependencies and weekend/evening processes underlying critical operations delivery unique to the organization.

Automated reconciliation during non-standard working hours is an example of operational activity linked to instant payments, which offers benefits of decreasing variations and increasing consistencies. However, automatic reconciliation can also have a compounding effect and drive automated errors. Much of the automated reconciliation process happens out of sight, particularly on weekends and overnight, and it may become difficult for employees to flag errors and remediate.

Financial institutions must place an emphasis on 24x7x365 transaction monitoring and clearly define who is responsible for this and the actions they should take when fraud is suspected, or outages occur. Transaction monitoring is especially important in times of unplanned downtimes, where FIs hold the responsibility to respond to and reconcile instant payment network messages that accumulate, as well as those messages dropped from the queue due to expiration or exceeding queue depth.

Escalation Procedures

Proactive definition of escalation procedures ensures procedural guidance is in place for when system issue instances arise. Financial institutions should establish clear decision points with trigger criteria, including the severity and impact of the issue. During business hours, FIs participating in the payment network are often the first to identify network system issues, and their timely reporting and notification to necessary parties drives expedient escalation and remediation.

A financial institution may want to plan for and define escalation procedures as it relates to various processes within the instant payment lifecycle such as excessive errors or timeouts, posting errors, out of balance reconciliations, or getting signed off the network unexpectedly, to provide a few examples.

One critical aspect of effective escalation procedures is defining who has the authority to make escalation decisions when system issues occur. This may involve senior executives or designated incident response teams within financial institutions or service providers. Implement communication protocols and outline escalation chains for communications that ensure prompt contact and reporting to decision-makers, even during off-hours.

Parties in the Escalation Chain:

1. **Network Operators**, such as the Federal Reserve and The Clearing House, should be immediately informed when issues impact the entire network's functionality.

2. **Participant/Customer call centers** are often the first line of defense in the event of fraud and suspicious activity.

3. In cases where **third-party service providers (TPSPs)** are responsible for facilitating transactions, they must play an active role in escalation and information exchange.

4. **Regulatory bodies** should also be part of the escalation chain to ensure transparency and adherence to regulatory requirements.

For the RTP network, operating rules outline that in times of emergency leading to disruptions of RTP operations, the Chief Executive Officer of The Clearing House may exercise the authority to instruct participants to refrain from sending payment messages, payment message responses, or non-financial messages until issue resolution.[4] The CEO may also temporarily alter RTP operating rules or technical specifications. Any actions taken in response to system disruption will be promptly communicated to the business committee and RTP Network participants.

Similarly, in the event of an emergency or failure of the Reserve Bank's hardware, software, data transmission, or operations facilities, messages via the FedNow Service may be delayed until resolution. For the FedNow Service, operating rules dictate that participants and service providers experiencing unplanned downtime establish monitoring and alerting systems to address availability issues promptly, to contact the Federal Reserve Support Center for guidance in the case of unplanned downtime for instruction on actions to take, and if necessary, sign off from the service so FedNow can inform other participants.[5]

Contingency Plan

A comprehensive contingency plan is critical for financial institutions participating in instant payment network(s), enabling them to maintain resilience and continuity in the face of unexpected disruptions. A well-crafted contingency plan should involve continuous monitoring for anomalies, especially anomalies in message counts, using alert systems to detect unusual patterns. It should also incorporate robust measures to manage transaction duplicates efficiently and prevent inaccuracies.

Important to the contingency plan is the action plan, which requires a comprehensive risk assessment to identify potential points of failure and mitigation strategies for various scenarios. Service level agreements (SLAs) for communications in tandem with clear documentation and well-defined process flows can ensure a smooth escalation process, even during traditional off-hours.

Performance Monitoring

Performance monitoring is a critical piece of consideration to ensure a financial institution's system is working as intended and that any potential accountholder impact is addressed as quickly as possible. This includes having alerts set up to quickly identify and monitor any unusual activity. Below are a few areas to consider adding monitoring around (although this is not all encompassing):

- Rejects – Understanding the volume of rejects as well as monitoring any sudden increase in rejection rates. It is important to ensure accurate reject codes are being utilized and to use rejects as an opportunity to talk to accountholders about how to effectively utilize the system if applicable.

- Posting Failures – Ensure there is visibility into posting failures as well as a process or way to be notified if one occurs.

- Response Times – Monitoring or trending response times can provide visibility into system performance as well as any SLA requirements.

- Sign-On Status – Visibility into the current connection status with the network through internal reporting or through applicable network portals.

Third-Party Risk Management

Third-Party Service Providers' (TPSP) involvement in business-critical operations indicates a degree of reliance for the FI, necessitating a revisit of policies and procedures on the entire vendor lifecycle, from onboarding, to continued vendor management, to offboarding. New "aspects" which a third party would benefit from for real time payments include 24x7 support incident management, run time, and high resiliency availability. Risk management procedures should be adjusted to account for these new aspects.

Representation from the relevant business workstream lead, as well as procurement, risk, and legal teams is essential to gaining a comprehensive input on vendor search and selection. The vendor evaluation process should include predefined assessment criteria, a formal document request, and interviews with key vendor representatives and existing accountholders as inputs to a rationalized final decision on vendor choice.

TPSP/vendor attributes that are key to a due diligence include existing policies & procedures, compliance training, strategy & reputation, information security practices, service delivery capability, financial condition, executive qualifications, Know Your Customer (KYC) and Anti-Money Laundering (AML) check results, insurance coverage, and company history. Further, impact to customer, business operations, reputation, and cost of contract should comprise an operational risk assessment.

After completion of the necessary due diligences, the selection of a TPSP partner, completion of contract negotiations, and implementation, the financial institution should monitor the TPSP, with regular reviews on an annual basis (at minimum), to confirm continued compliance with contractual obligations and to confirm assessments in risk, security, operational, and controls remain within thresholds of comfort as well as understanding the TSTP's future product roadmap to identify additional assessment needs or new intervals for reviews.

When a relationship with a TPSP ends or is terminated, procurement and risk teams at the FI should maintain procedures by which documentation is adequately transitioned to appropriate parties and sensitive data is destroyed from vendor systems, as well as document lessons learned from the vendor relationship.

Staffing Needs & Training Requirements

As a financial institution prepares to enable the receipt of instant payments, employee needs will need to be evaluated. Due to the instant nature of these payments, many FIs have been able to support their instant payment operations without having to increase staffing. Depending on how each organization is structured, there may be an opportunity for existing departments to absorb any operational needs to support instant payments and/or explore opportunities to increase automation and alerting capabilities. Key areas to consider within the evaluation include:

- Application and Customer Support - to support 24x7x365 processing
- Operations - processing return requests, reporting, and monitoring
- Fraud - fraud alerts and fraudulent related return requests
- Accounting/Treasury - reconciliation and funding
- Compliance/BSA - audits, disclosures, OFAC

Once live, it will be important to continually keep a pulse on network activity and different use cases that may require additional resources or support. The more familiar the organization becomes with how the network works, the easier it will be to assess potential staffing impacts associated with enabling send/request for payment capabilities.

Training for All Employees (Fundamentals)

Ensuring all employees understand what instant payments are and how they work will be vital to successful implementation. The depth of training needed may depend on the financial institution's adoption of other faster payment products and how familiar employees are with those options. For instance, if Zelle® is a product offering that the financial institution supports, the employees would be familiar with the concept of immediate funds availability but would need training around the immediate settlement and irrevocability of the funds. A key differentiator when discussing Zelle versus the RTP Network and FedNow, is that Zelle is a product, whereas RTP and FedNow are payment rails that a product could settle over. Regardless of the financial institution's faster payments journey, awareness training will be needed to ensure all employees understand the benefits and how it is being implemented at their organization.

Education around use cases will be beneficial for employees to understand how these rails are being utilized as well as how accountholders can take advantage once the financial institution is live on the network(s). The U.S. Faster Payments Council Use Case Repository offers an opportunity to learn more about use cases[6] that may benefit the financial institution's accountholder customer base. In a receive-only capacity, use cases will depend on who the accountholders work with and whether they are enabled to send instant payments.

Lastly, it is important for employees to understand that organizations must sign up and enable the ability to receive and/or send instant payments, it is not something currently offered by all FIs. A list of financial institutions lives on each network,[7] is available to and can be a resource for both employees and accountholders.

Training for Frontline Employees

From a customer service perspective, training documents and materials, along with a standard script with escalation triggers, can be utilized to provide service to accountholders. It is important to ensure that there is factually correct information being given out to accountholders and a system to ensure follow-up in case escalation is needed and a resolution cannot be provided instantly. All these workflows and escalation triggers need to be well documented and easily accessible to frontline employees to provide 24x7x365 support to accountholders. As a receive only financial institution, it may be infrequent that frontline employees receive questions on instant payments, making it imperative that resources are both easily accessible and understandable. Consider the best way for employees to easily obtain this information, such as a manual, list of FAQs, video education, or a combination of several different, readily available resources.

Training for Sales Employees

Sales employees play a critical role in the proliferation of knowledge to accountholders and in creating interest in new products and services. Most financial institutions begin their journey into instant payments in the receive-only mode, and it will be critical for sales employees to begin to sell the benefits of that connectivity to accountholders. Creating a buzz around instant payments will set the stage for the financial institution's progression into send capabilities and the institution's ability to monetize the products built on the new rails. There are two distinct sales groups that will need to be trained in discussing the benefits of instant payments and how to sell them.

Branch and call center employees are often the first employees that come into contact with accountholders, and nearly all sales conversations begin with these employees. These employees need to understand how to leverage the financial institution's ability to receive instant payments to differentiate the financial institution from others that have yet to adopt instant payments. Selling the benefit of instant payments should enable sales employees to increase the conversion of non-accountholders to accountholders as well as deepen existing accountholder relationships. While consumer adoption of instant payments may not be a source of revenue for the FI, the ancillary products and services that can be sold to new accountholders can be a way to drive revenue.

Treasury Management (TM) teams will need to be able to explain the benefits of being able to receive instant payments to their commercial accountholders and set the stage to eventually sell those same customers on the ability to send instant payments. Sales employees should focus on the benefits of instant payments, including the immediacy and irrevocability of the payments as well as the increased ability to receive information related to the payment as part of the message. For example, the ability of a building supply company to receive an instant payment could enable it to ship products faster or collect on delivery rather than waiting for payment in slower traditional payment channels. The benefits of instant payments will enable TM employees to differentiate the financial institutions offering from others. The ability to articulate and sell accountholders the benefits of receiving instant payments will lay the groundwork for selling send capabilities and help TM employees identify future pilots and sales opportunities when send capabilities are available.

Specialized Training for Back-Office

Specialized training will be needed for certain departments to understand their role and responsibilities related to instant payments. The RTP and FedNow networks have nuances, where training may require callouts on key differences between the rails. Below are a few areas to consider when building out a training plan for employees:

Accounting: One of the fundamental differences between existing payment rails and instant payments is the immediacy of the settlement of the transactions and the 24x7x365 operational environment. Accounting employees will need to be trained in the reconciliation of settlement accounts, which will require changes to the existing reconciliation of the Master Account for FedNow and a new reconciliation of the pre-funded balance account for RTP. When the financial institution begins offering send capabilities, accounting employees will need to develop and be trained in forecasting and funding methods for both FedNow and the RTP Network.

Operations: Operations employees will need to be trained in handling issues related to requests for the return of funds and instances where the financial institution accepts a payment without posting. Training will also need to include troubleshooting issues or reconciliation issues related to the posting of transactions to customer accounts.

Compliance: Compliance employees are responsible for ensuring that they update customer-facing disclosures, policies, and procedures as instant payment rules and regulations change. They will also need to collaborate with other internal stakeholders to ensure that regular risk assessments are performed on instant payment products to ensure that the organization's risk stance is appropriate and commensurate with the level of risk instant payment products present. To perform these functions, it will be critical that compliance employees are provided with training on the rules and regulations that govern instant payments and that they receive ongoing training as those rules and regulations change.

Fraud: On top of understanding the nature of instant payments, a financial institution's fraud employees will need to understand the reporting requirements related to fraudulent transactions and how to submit the information to the respective network(s). Employees will need to understand the type of fraud monitoring in place for instant payments and have procedures to follow when alerts are received. Training will also need to be completed for investigating return requests related to fraud. It will be critical that investigative employees are familiar with the irrevocable nature of instant payments and the responsibilities of both the sender and the receiver.

IT: Technology teams will need to understand the message flows and the different network specifications to support the processing of payments 24x7x365. Documenting procedures and the teams that need to be involved when an issue is identified will be important in ensuring issues get resolved as quickly as possible. If utilizing a third-party service provider, staff should understand when and to whom any issues should be escalated.

Accountholder Support, Education & Disclosures

Accountholder Support & Education

Supporting accountholders with instant payments is not significantly different from supporting them for any of their other products and services. For example, staff will be helping accountholders during branch transactions, on the phone at the call center, on the website, with their online banking solution, etc. Below are some key factors to consider as a financial institution develops accountholder support and education and establishes internal processes to fully support them with receiving instant payments.

Benefits: Help accountholders see the various benefits of receiving instant payments. Consider using testimonials, stories, or examples of use cases to drive home the message that instant payments can help them get paid more quickly, have access to the funds right away, and feel secure knowing that the funds received will not be rescinded. Notable benefits for the consumer receiving an instant payment include immediate funds availability and confirmation for the originator that funds were received.

Educational Content & Resources: Provide educational content and resources to help users understand how to use instant payments securely. Provide clear instructions and customer support channels for any questions or issues. This could include FAQs, video tutorials, and blog articles. It is important to remember when educating customers that they are not familiar nor aware of network specific names like FedNow or RTP and therefore education should be regardless of network.

Managing Accountholder Expectations: Managing accountholders' expectations from the get-go is another key consideration. For example, provide communications that demonstrate the types of messages or transaction descriptions they will see on their accounts when they receive an instant payment. Also, help them understand that while the funds will be made available to them within seconds, on occasion the institution may need more time to review the transaction more closely as an additional security precaution. Finally, if the institution anticipates charging their accountholders to receive instant payment transactions, be sure to communicate that with them early so they are aware prior to their first receipt.

Transaction Messaging: Although it happens quickly, instant payment transactions include multiple messages that are exchanged throughout the process flow. The financial institution should help accountholders understand how they will know if they receive an instant payment and how they will be informed (i.e., via SMS, online banking, etc.). Given accountholders do not speak in ISO 20022, the institution may need to convert the data-rich message into a human-readable format.

Frequently Asked Questions (FAQ): A financial institution may also consider creating an FAQs document to share with accountholders to assist them in understanding some of the most frequently asked about topics such as:

- When can I start to receive instant payments?
- Is authorization required to receive transactions?
- How can I receive money?
- When will I get access to the funds?
- What account number do I provide to receive instant payments?
- Is it safe to share my account information with a trusted party?
- What is this money deposited to my account? I do not think it belongs to me.

Disputes: Even on the receiver's side, there may be times when an accountholder receives funds they did not anticipate or do not belong to them. Financial institutions should establish a clear process for handling disputes related to instant payments and provide a mechanism for users to report issues or errors and the process to return the funds.

Enhanced Security Measures: Again, even receiving instant payments transactions could pose some degree of immediate or future risk for accountholders. For example, the receipt of an instant payment could be used against an accountholder, or the accountholder may unknowingly be a money mule for a fraudster. Accountholder education on these scenarios is an important aspect of fraud mitigation. Also, the information provided to another party today for a legitimate instant payment may be used for fraudulent transactions in the future. Implement robust security measures to protect the account holders' funds and data. Best practices include utilizing multi-factor authentication (MFA), encryption, fraud detection systems, and real-time monitoring to mitigate risks.

User-Friendly Mobile Apps and Websites: The financial institution should enhance its mobile banking apps and website to support instant payments and ensure the user interface is intuitive and easy to navigate. The institution should update the transaction history and notification features to accommodate these new types of transactions.

Consistency and Clarity of Information: No matter how financial institutions support their accountholders; they expect that the information they receive is consistent. Additionally, the information should be clear and concise so that accountholders understand the institution’s policies and practices regarding instant payments, regardless of their financial literacy or technological aptitude.

Customer Feedback: The financial institution should encourage feedback and suggestions from accountholders, make necessary adjustments, and ensure it is continuously improving its instant payment services.

While there are many similarities in how a financial institution supports its accountholders with instant payments as compared to other payment channels, the unique features of instant payments do require some special considerations.[8]

24x7x365 Support Model: Because instant payments are available around-the-clock, be prepared to provide support at all hours, or communicate when they can reach the financial institution with any questions or issues they have. This could include a dedicated hotline, online chat, email support, etc. Options include outsourcing customer support function during hours staff is not available or relying on a third-party service provider who manages the processing of instant payments on the institution's behalf, the service provider may be able to support accountholder questions and issues when the employees are not available. Alternatively, the institution could provide messaging to accountholders during closed hours so that they are aware of when they can reach support or when they should expect a response.

Regular Monitoring to Convey Up-to-Date Information: Especially while instant payments are still in their infancy as a payments rail, information about rules, regulations, issues, processes, etc. will continue to evolve. Keep abreast of technological advancements and changes in the instant payment landscape. Be prepared to adapt its services and product documentation to meet changing accountholder needs and regulatory requirements.

Fintech & TPSP Relationship Education for Customers

Fintechs and financial institutions should provide the following:

Clear Communication: Maintain clear and consistent communication with their customers about the partnership. This includes informing customers about the benefits and potential changes resulting from the collaboration.

Product Information: Provide detailed information about any new products or services resulting from the partnership. Explain how they work, their features, and how they will impact customers.

Customer Support: Ensure that customers have access to support channels where they can get their questions answered and issues resolved. Both parties should provide responsive customer service.

Disclosures

Financial institutions are currently subject to a range of regulations, guidance, and best practices on disclosures to accountholders on 'legacy' payment rails. General buckets of information for disclosure include, if applicable, transaction details, consumer/accountholder rights, error resolution procedures, fees and charges, protections over consumer privacy and data security, and confirmation of terms with opt-out optionality.

Description of Service: Financial institutions are encouraged to disclose a description of instant payment services being provided to the accountholder, enumerating the key aspects of the service and the accountholder's role in the payment process.

Error Resolution: With the adoption of instant payments account disclosures should be reviewed to include error resolution. Reg E on Error Resolution requires reporting/ notification to consumer on resolution status and remediation activity within defined timelines. Errors in scope on the receive-side of payments include an incorrect electronic fund transfer to or from the consumer's account; the omission of an electronic fund transfer from a periodic statement; and a computational or bookkeeping error made by the financial institution relating to an electronic fund transfer.[9]

Privacy and Use of Data[10,11]**:** Financial institutions should be transparent about how accountholder data will be shared and used within the partnership. Clearly state data privacy policies and any changes to them. If applicable, disclose accountholder data shared with third party service providers, and its use – oftentimes for screening and authentication of bank account or identity. In the case of data security risks, provide clear and concise risk disclosures. Explain how these risks are being managed.

Fees & Charges: Financial institutions should clearly disclose any fees, charges, or pricing changes associated with the new payment instant payment rail. Ensure that accountholders understand the cost implications and funds availability and fees associated with this new service. 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.

Rules and Laws: Financial institutions should ensure the financial institution is compliant with relevant financial regulations and disclose how regulatory compliance is being maintained at the institution. Areas of relevance include Regulation E[12], UCC 4A, UDAAP, Federal Reserve Financial Services Operating Circular, and The Clearing House.

Making Funds Available – Instant Payments: A beneficiary's financial institution (other than a Federal Reserve Bank) that accepts a payment order over the FedNow Service and the RTP network is obligated to pay the amount of the order to the beneficiary of the order immediately after its acceptance of the payment order, by crediting the account of the beneficiary in accordance with §4A-405(a) – Payment by Beneficiary's Bank to Beneficiary of UCC 4A.

UCC 4A applies to the FedNow Service for both commercial and consumer transfers. §210.40(b)(4) of Part 210 Subpart C - Fund Transfers Through the FedNow Service provides: "This subpart governs a funds transfer that is sent through the FedNow Service, even if a portion of the funds transfer is governed by the Electronic Fund Transfer Act, but in the event of an inconsistency between the provisions this subpart and the Electronic Fund Transfer Act, the Electronic Fund Transfer Act shall prevail to the extent of the inconsistency."[13]

Fraud Mitigation

Fraud is Not New but Evolving[14]

Fraud involving a payment is classified into two main types: "unauthorized" and "authorized" – in terms of whether the payer authorized the payment. An "unauthorized" payment describes an erroneous or fraudulent payment where the payer did not authorize the payment instruction. In contrast, an "authorized" fraudulent payment is used to describe payment instruction in a scenario where the payer was duped into making the payment.[15]

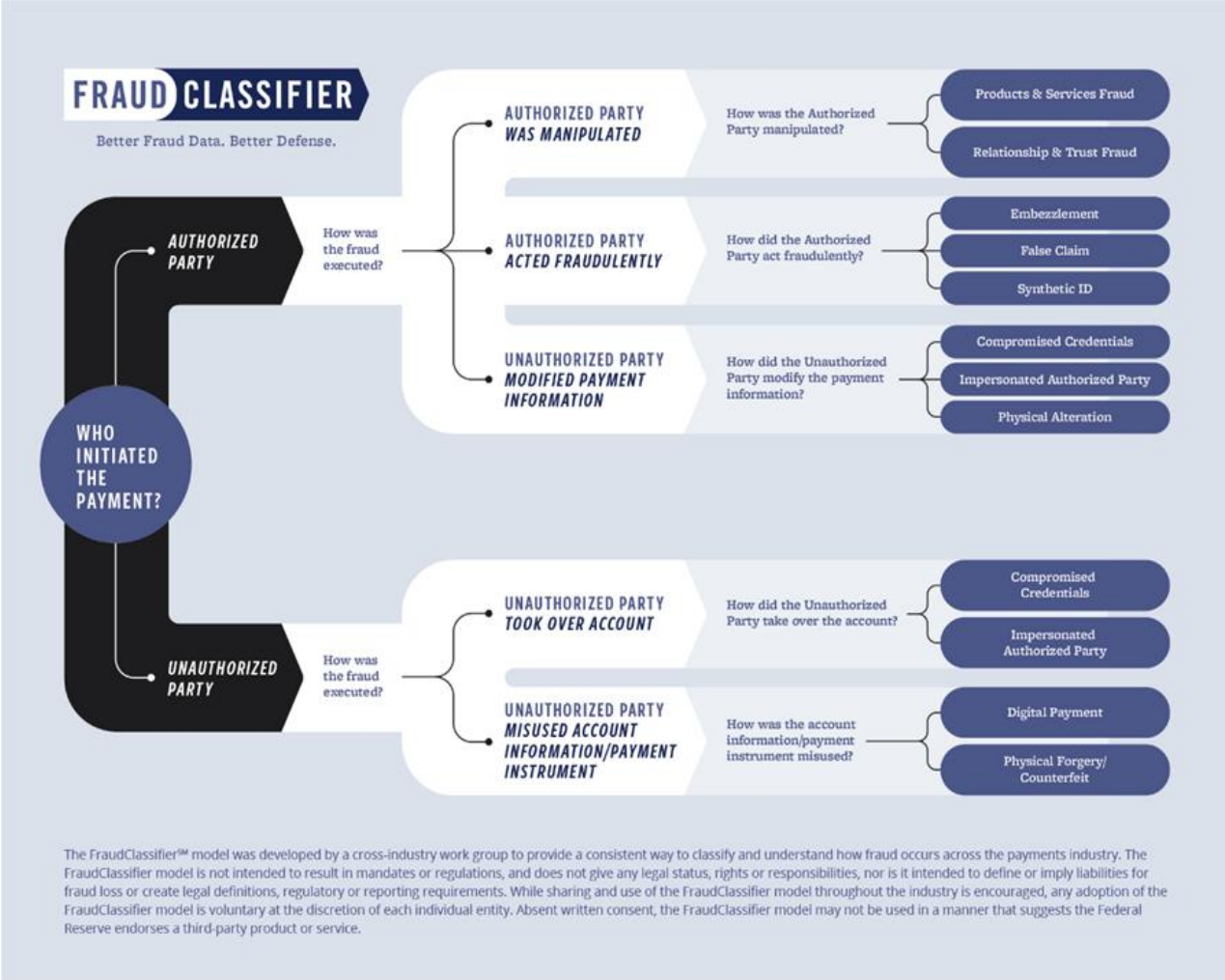
In short, fraud is not new, and it is not unique to financial services. Fraud will continue to evolve if there is something to be gained and innovation results in changing the way activities are conducted and/or performed. While sending participants must ensure robust controls are in place prior to participation in this sort of ecosystem, an equally large burden of responsibility falls on receiving institutions to combat authorized payment fraud (i.e., scams). Crucial monitoring, reporting, and customer education in combination present a unique challenge specifically for community and regional financial institutions looking to implement RTP and/or FedNow as a way of differentiating themselves in the marketplace.

Fraud in Faster Payments

Fraud Types

In a credit push, around-the-clock, environment where payments are instant and irrevocable, the primary concern vis-à-vis fraud is unauthorized fraud in the form of account takeover.

As such, controls, and governance frameworks around KYC for onboarding accountholders and behavioral analytics after the fact are paramount in combating bad actors for participants. For receiving participants, scammers have an easier task needing only to convince a payer to submit an authorized payment (see FraudClassifier[16] model below). As a result, receiving participants in a payment ecosystem designed for non-stop and immediate activity must be vigilant in their controls and procedures in place to onboard new clients and support inbound activity with robust monitoring and reporting (both internal and external) mechanisms in place. Flags for payment value and/or volume are insufficient; in this new ecosystem payment velocity is equally important, if not of greater concern. Receiving participants will need to consider the regulatory and legal implications of supporting this new payment activity as well as the risks inherent and decide if the organization's risk appetite is one that supports participation.[17]



Authorized Party Fraud:

- Scams: the use of deception or manipulation intended to achieve financial gain.[18]
- Account owner is bad actor (i.e., False Claim / Mule Account / Synthetic ID).
- Payment modification (i.e., Credential Compromise).
- Spoofing bad actors disguise their communication, making it appear as if it is from a trusted source, such as a financial institution or payment processor, to mislead account owners into initiating transactions to the fraudster.

Unauthorized Party Fraud:

- Account Takeover: The bad actor gains access to a victim's bank account or digital payment platform, often through phishing or malware, and makes unauthorized transactions. This constitutes impersonation of an account owner by the bad actor.
- Man-in-the-Middle Attacks: The attacker intercepts communication between two parties in a transaction to secretly alter or steal data.

Fraudulent Account Types:

- Identity Theft: Identity theft in financial environments is characterized by the unauthorized acquisition and use of an individual's personal data, such as Social Security numbers, bank account information, or credit card details. Bad actors exploit this stolen identity to conduct illicit transactions, obtain loans, or open accounts, which can result in substantial financial loss for both the accountholder whose identity has been compromised as well as both financial loss and reputational damage for the financial institution.

- Synthetic Fraud: Synthetic fraud involves the creation of fictitious identities by combining real and fabricated information to establish bank accounts with a legitimate credit history. These accounts are typically used to acquire credit, goods, or services with no intent to repay, leading to account abandonment resulting in potential significant losses for the financial institution. Financial institutions should use advanced analytical tools, strong KYC protocols and cross-reference data extensively during the accountholder onboarding process to uncover inconsistencies indicative of synthetic identities.

- Money Mule: Money mule fraud is the misuse of a bank account, either with their knowledge as a knowing participant or as an unknowing conduit to transfer and launder illicit funds. This type of fraud is commonly conducted by criminal organizations seeking to move money while obscuring its illegal origin. The individuals involved, or "mules," receive and redistribute the funds, creating layers of transactions that evade monitoring efforts of financial institutions and regulatory agencies.

Fraud Mitigation Considerations

Policy Review & Enhancement

In the face of an ever-evolving threat landscape, it is important for organizations across the financial sector to establish and maintain a robust policy review and enhancement protocol, particularly in the domain of instant payments. Core to this framework is the continuous and thorough evaluation of internal controls, alongside the systematic refinement of policies and procedures. This proactive approach is critical in preserving a resilient fraud mitigation infrastructure that adapts swiftly to new threats. Integral to these efforts are comprehensive audits—internal and coordinated with independent external entities—that serve as vital checkpoints to measure the effectiveness of current fraud mitigation strategies. A well-conceived audit plan stands as a multifaceted line of defense, providing clarity and direction in pinpointing and shoring up potential vulnerabilities within our complex systems and operational processes.

Furthermore, segregation of duties must be central to any organization's strategy to combat fraud effectively. Constructing in-depth policies and layered audit protocols ensures that no single individual exercises unilateral control over sensitive financial transactions, thereby creating an environment of focused internal checks and balances. Additionally, the implementation of advanced and tailored monitoring systems is crucial across various tiers of operation. These systems play a pivotal role in elevating fraud mitigation efforts, enhancing comprehensive vigilance and facilitating prompt intervention when irregularities are detected. By adopting a holistic, layered defensive strategy, institutions can foster an organizational culture deeply rooted in fraud deterrence, equipped with the agility to confront, and proactively manage potential fraud risks within the electronic payment's spectrum. This collective commitment to rigorous fraud mitigation is essential in safeguarding transactional integrity.

Importance of KYC programs

Investing in stringent KYC measures is not just about protection; it is a strategic imperative in today's electronic payments environment. KYC policies are vital in mitigating fraud within electronic payments. KYC involves verifying the identity of clients, understanding their financial behaviors, and continually assessing the risks they may pose. With electronic payments, transactions can be instantaneous and robust KYC procedures enable institutions to detect unusual patterns that may indicate fraudulent activity. By ensuring each customer is who they claim to be, financial institutions can significantly reduce the risk of becoming conduits for money laundering, identity theft, scams, and other forms of financial crime which are costly to remediate and cause significant reputational damage. A proactive stance on KYC can serve as both a shield against attempted fraud and as a competitive advantage by enhancing the financial institution's reputation with clients.

Furthermore, with the regulatory landscape around electronic payments tightening globally, thorough KYC practices ensure compliance with Bank Secrecy Act (BSA), AML and counter-terrorism financing (CTF) regulations. Investing in stringent KYC measures is not just about protection; it is a strategic imperative in today's digital banking ecosystem.

Advanced Analytics Volume, Value, & Velocity

In the realm of instant payment fraud mitigation, financial institutions are increasingly leveraging advanced analytics to scrutinize transactional data across three critical dimensions: volume, value, and velocity. By analyzing high volumes of transaction data, institutions can identify patterns that deviate from established norms, flagging potentially fraudulent activity. Simultaneously, tracking the value of transactions enables the detection of anomalous high-value movements that may signal unauthorized transfers or the exploitation of system vulnerabilities. Lastly, assessing the velocity of transactions—the speed at which funds move—allows for the identification of rapid, sequential transactions that could indicate money laundering or account takeover attempts. The integration of these analytical parameters into real-time surveillance systems equips financial institutions with a powerful toolset to proactively detect and prevent fraudulent activities, ensuring the security of instant payment platforms and maintaining accountholder trust in the digital financial ecosystem.

Operational Irrevocability & Request for Return of Funds (RFRF)

A sending participant may send a Request for Return of Funds (RFRF) for any reason, including to request a return of funds related to an erroneous payment or a payment made in response to a fraudulent Request for Payment. The sending financial institution through RTP has 60 calendar days from the date of the original credit transfer to submit a request. The 60-day timeline does not apply to claims related to fraud. The Receiving financial institution through RTP has ten banking days to respond except for Fraud (FRAD) or Breach of Warranty (UPAY). For FedNow, breach of warranty (WNTB) claims must be sent within 95 calendar days of the date of settlement of the credit transfer. The response to the claim is required within 20 business days of receipt of the RFRF. Instant payments are final and irrevocable, a participant that receives a Request for Return of Funds is not required to return the funds but should respond immediately with a response and then a final response after the RFRF investigation. However, it is important to note that the sending participant may still need to reimburse the consumer's account per Regulation E (12 CFR 1005.6) if the participant determined that an error occurred regardless of the success of a return-of-funds request to the receiving participant.[19]

Moreover, when addressing erroneous or unauthorized transactions not covered under the Electronic Fund Transfer Act (EFTA), Commercial Code (UCC) comes into play.[20] This statute delineates the liabilities between the involved entities in a funds transfer, particularly focusing on errors. In cases of unauthorized transactions, the liability between the sender and the sending financial institution will be determined by the security procedures established and mutually agreed upon, as outlined in Article 4-A. It is crucial for financial institutions to understand that the act of returning funds following a request does not absolve a sending participant's obligations under Article 4-A in the event of an unauthorized payment. Ensuring adherence to these legal frameworks while implementing robust security measures and diligent operational practices is essential for maintaining trust in the real-time payment systems and protecting all stakeholders from potential fraud.

FedNow Service

An FI must investigate each unusual payment order it sent or received to ascertain whether it is a reportable transfer.

- Unusual Payment Order: any payment order that was authorized when sent but that a FedNow participant learns otherwise may have resulted from fraudulent activity.
- Reportable Transfer: a funds transfer based on an unusual payment order and that the FedNow participant believes in good faith was the result of fraudulent activity.

If so, the participant must then report the transfer to the FedNow Service and the other FedNow participant. A determination by an FI that an unusual payment order is a Reportable Transfer is not necessarily a final determination. An FI may update the report made with new information received including response to additional facts provided by other FedNow participants or their accountholders. The FRB will provide reporting capabilities for non-value messages and procedures for FedNow participants to meet reporting requirements. Participants are also required to provide a list of authorized contacts to receive reports of reportable transactions that may be provided to other FedNow participants.

The RTP Network

Sending participants are required to report unauthorized payments to the network using the Request for Return of Funds (RFRF) message using the "FRAD" code.[21]

This immediately goes to the involved receiving participant, who is obligated to "reasonably cooperate" with efforts to recover erroneous or unauthorized payments, though there is no obligation to return funds.

Report material findings regarding (i) unauthorized payments or (ii) authorized payments that were sent in response to a Request for Payments that the sender claims was deceptive or misleading via email to: RTPEnforcement@theclearinghouse.org.[22]

Third-Party Partnership

The real-time payments ecosystem thrives on the seamless interconnectivity and collaboration between various stakeholders, including service providers, financial institutions, fintech companies, and fraud mitigation vendors. The symbiosis among these entities is pivotal for fostering a secure and efficient payment environment. Financial institutions and fintechs are at the forefront of offering innovative payment solutions that cater to the instantaneous expectations of modern consumers and businesses. However, with the rapid execution of transactions, the window for detecting and responding to fraudulent activities narrows considerably. It is here that the relationship with adept service providers and specialized fraud vendors becomes crucial. These partners provide the necessary technological infrastructure and advanced analytics to monitor transactions in real time, identify suspicious patterns, and flag potential fraud with minimal impact on the user experience.

Moreover, as cyber threats evolve in sophistication, the collective intelligence garnered from this diverse network of players becomes an invaluable resource for staying ahead of fraudsters. Service providers and fraud vendors are continuously developing and refining their tools, using machine learning and artificial intelligence to not only keep up with but also anticipate new fraud tactics. Financial institutions and fintechs benefit immensely from these advancements, ensuring they can offer cutting-edge services without compromising security. This collaborative dynamic fosters a proactive approach to fraud mitigation, where continuous information sharing and joint efforts in developing best practices for fraud mitigation are central. By maintaining strong partnerships and fluid communication channels, the consortium of payment processors, financial institutions, fintechs, and fraud experts can work in unison to safeguard the integrity of real-time payments, instilling consumer confidence and ensuring the longevity and reliability of these modern financial services.[23]

Regulations & Compliance

In the rapidly evolving landscape of faster payments, one must take pause to fully appreciate the crucial role that compliance with laws, regulations and network rules takes in ensuring the success of faster payment initiatives and safeguarding the integrity of the broader financial system. Such laws and regulations are designed to safeguard consumers, facilitate seamless transactions, and foster a robust and dynamic financial ecosystem. Below is a description of various laws, regulations and network rules that impact faster payments; such a complex web is one that should also be guided by legal counsel.

Regulation J Subpart C[25]

Regulation J, Subpart C, lays the groundwork for the operational and legal aspects of the FedNow Service. The subpart begins with definitions, clarifying key terms such as "payment order" and "sender," which are fundamental for understanding the roles and responsibilities within the FedNow framework. These definitions ensure a common understanding and set the stage for the more detailed provisions that follow.

Section 210.42 addresses the reliance on identifying numbers, highlighting that a Federal Reserve Bank may depend on these numbers to process transactions, even if there are discrepancies with the associated names. This section is critical for streamlining operations and reducing errors. The agreements addressed in 210.43-210.44 emphasize the obligations of a sender and a receiver, including a senders obligation to fund payments, and a receivers obligation to make funds available immediately.

In 210.45, the regulation covers execution of payment orders by the Federal Reserve Bank. This includes the details related to rejecting payments, processing through other Federal Reserve Banks, and parameters around execution and payment date. The Federal Reserve Banks' role in this process is further detailed in 210.46, which describes their responsibilities in accepting and settling payment orders. These provisions ensure that the FedNow Service operates efficiently, maintaining the speed and reliability required for instant payments.

Overall, Regulation J, Subpart C, provides a comprehensive framework that supports the secure, efficient, and reliable processing of instant payments through the FedNow Service.

Operating Circular 8

In September of 2022, The Federal Reserve Banks issued Operating Circular 8, which sets the terms and conditions governing FedNow in conformity with section 210.40(c) of Regulation J.[25] Operating Circular 8 is specific to FedNow and does not apply to RTP transactions or other faster payment systems. While the entirety of Operating Circular 8 is considered necessary reading for all FedNow participants and service providers, some of the key points addressed in this circular related to the receipt of FedNow transactions have been summarized below.

- General Obligations: All participants and service providers are required to follow the FedNow operating procedures and technical specifications, and the Reserve Banks are not liable for any loss if a participant or service provider does not comply. Additionally, participant profiles and processing options for the FedNow Service are described in this section. Finally, expectations and requirements to maintain the confidentiality of information, whether it be transactional or about the FedNow Service in general, are also addressed.

- General Obligations: All participants and service providers are required to follow the FedNow operating procedures and technical specifications, and the Reserve Banks are not liable for any loss if a participant or service provider does not comply. Additionally, participant profiles and processing options for the FedNow Service are described in this section. Finally, expectations and requirements to maintain the confidentiality of information, whether it be transactional or about the FedNow Service in general, are also addressed.

- Message Format, Routing Numbers and Accounts: Participants must follow message formats prescribed by the FedNow Service. The Reserve Banks are not liable for any loss related to the accuracy of routing numbers or other information contained in a message.

- Settlement: Each participant must designate a settlement account, which may be their own master account or maintained by a correspondent. Settlement is final at the earlier of the time the debits and credits of a payment order is recorded, and an Advice of Credit is sent to the receiver.

- Security Procedures: By using the FedNow Service, participants agree to and must comply with the Reserve Bank's Operating Circular 5, Electronic Access. Messages must be sent via one of The Reserve Bank's Electronic Connections.

- Receipt, Acceptance and Delivery of Messages: Any messages can be rejected or deleted by a Reserve Bank for any reason. Participants must retrieve messages made available to it as soon as possible. The Reserve Banks do not assume any responsibility for completion of a funds transfer on the day requested. Upon receipt of a Request for Confirmation, the participant should ascertain whether it maintains an account for the beneficiary and is required to respond to the Request for Confirmation.

    - If the message is accepted, a pacs.002 ISO message should be sent back to the sending participant with the status code of ACTC, and funds should be made available to the receiver immediately following the receipt of the Advice of Credit from the Reserve Bank.

    - If the message is rejected, a pacs.002 ISO message should be sent back to the sending participant with the status code of RJCT.

    - If the response to the message is Accept Without Post (ACWP), the receiver must investigate and resolve the concerns and use the pacs.002 ISO message to accept (ACTC) or reject (RJCT) the message by the ACWP Target Deadline (midnight Eastern Time the next business day, as of the February 2024 FedNow Operating Procedures). If the message is rejected, the receiver must issue a refund payment.

- **Operating Hours & Extensions:** The FedNow Service operates 24 hours/day, 7 days/week. Business days begin and end at the times published at FRBservices.org; cutoff times are also established for the service.

- **Required Reporting and Reconcilement:** Each participant must keep records sufficient to perform its obligations, including to reconcile its activities and resolve exceptions. As indicated in the February 2024 FedNow Operating Procedures, cutoff times for FedNow cycle days are approximately 7:01 PM ET.

- **Availability, Recovery, Resiliency, and Testing:** Each participant must maintain the ability to send and receive Messages as appropriate for their profile, communicate with their accountholders regarding activity, and make funds immediately available. Reasonable maintenance windows are allowed. Contingency and recovery plans must be established and tested.

- **Service Providers:** A participant may authorize another entity to act on its behalf, subject to an agreement and requirements listed in the circular.

- **Compliance Related Requirements:** All participants must maintain procedures to screen their customer base against sanction lists, establish a compliance program that is designed to comply with sanctions laws and this circular, and maintain a BSA/AML compliance program consistent with FINCEN and their regulator.

It is critical that all FedNow participants become familiar with all requirements set forth in Operating Circular 8, including those listed above as well as requirements not addressed here. To that end, stakeholders from a variety of areas within the financial institution or service provider (i.e., Legal, Operations, Audit, Compliance, Information Security, Finance, etc.) should be involved with faster payments implementation to ensure controls are in place to comply with the requirements.

The Clearing House RTP Operating Rules

The Clearing House RTP Operating Rules[26] create the framework for the RTP network and define the rights and roles of all participants and The Clearing House. They define and establish requirements for participants with respect to sending and receiving RTP payments and other RTP messages, including request for payment. Sending institutions are required to act as the gatekeeper to ensure that all payments introduced into the network are valid and adhere to the network rules.

The rules require receiving institutions to accept payments that conform to RTP technical specifications into valid accounts unless the owner of the account does not wish to accept RTP payments or the payment cannot be accepted due to legal or regulatory compliance requirements. The rules also establish requirements for fraud detection, reporting, and reasonable cooperation in resolving errors and returning funds. Finally, the rules establish the mechanisms for participants to ensure that they maintain funding for transactions that enable settlement in the network to take place in real time.

The RTP rules require that an annual audit of the institution's compliance with the rules be performed by an internal auditor or external audit firm on an annual basis. If the institution chooses to have an internal department perform its audit it must ensure that the auditor has sufficient independence as well as knowledge of the rules. Lastly, The Clearing House establishes in its rules, a rules enforcement mechanism to maintain the quality and reliability of the RTP network.

Key points of Receiving Participant Obligations under the RTP Operating Rules include:

- *General Responsibilities:* All participants are required to follow the RTP Operating Rules, the RTP Technical Specifications, the RTP Risk Management and Fraud Control Requirements, and the RTP Information Security Standards and Requirements. Defines eligible payments and system limits as well as prohibited activity such as correspondent transactions, foreign payments, fee netting, and use of the system to search for accounts. Covers the requirements of participants to report fraudulent activity, to act on fraud alerts received from TCH and maintain an OFAC compliance program. Finally, provision of payment status to both senders and receivers as well as provision of message information is addressed.

- *Receiving Participant Obligations:* Receiving participants must respond to payment messages within established timeframes and cannot establish cut-off times that would delay receipt of funds beyond the RTP day in which the payment message was received. Receiving participants must accept all payments other than those meeting specific exception criteria, and the participant can rely on the account number identified in the payment message. Finally, participants must respond to all payment messages with either Accept, Accept without Posting, or Reject and make funds available immediately to the receiver of any accepted payments.

- *Funding and Settlement:* All participants must provide funding directly or through an agent in the RTP prefunded balance account and maintain their position consistent with expected RTP activity. Settlement of payment messages will be complete when the RTP system records both the decrease in the sending participant's net position and the increase in the receiving participant's net position and is final.

- *Non-Payment Messages:* Participants may send, and receivers must respond to requests for return of funds.

- *Risk Controls Established by TCH:* TCH maintains the right to audit, monitor, inspect, and investigate participants compliance with the rules and requires that all participants conduct a self-audit annually.

UCC4A

Under UCC4A,[27] financial institutions have specific obligations when it comes to handling funds transfers. At a high level these pertain to verification of payment orders, execution accuracy, prompt notification of payments, security measures, and error resolution. These requirements are intended to maintain the integrity, security, and efficiency of funds transfers within the framework of UCC4A.

When it comes to receiving instant payments, there are not specific UCC4A requirements that differ from other payment rails, and instant payment can be handled like other payment types but will be necessary to ensure the new payments are integrated into existing applications, processes, and polices related to the UCC4A requirements.

A prime example of how UCC4A requirements apply to payments is UCC4A-207 where it stipulates that when executing payment orders, financial institutions may post transactions based solely on the account number provided, even in instances where the beneficiary's name differs from that specified in the order. The guiding principle here is the primacy of the unique identifier—the account number—over ancillary details such as the accountholder's name.

Funds Availability

Funds availability requirements outlined in section 210.44(b); financial institutions must adhere to a specific timeline once a payment order has been accepted by the beneficiary's financial institution. This requirement mandates that the recipient institution must immediately credit the beneficiary's account following acceptance, conforming to the guidance in section 4A-405(a) of Article 4A. The prompt crediting of funds is not merely a procedural step but a regulatory requirement to ensure the prompt availability of funds for the accountholder, thereby reducing friction in the posting of electronic transactions.

Funds availability for RTP payments is set forth in the RTP Operating Rules.

The implication for financial institutions is clear: upon the acceptance of incoming payment orders, the procedures they have in place must immediately and accurately credit the payment to the receiving party.

By adhering to the funds availability requirements of 210.44(b) financial institutions will meet the expectations of accountholders and remain in regulatory compliance. It is incumbent upon financial institutions to devise and maintain systems, policies, and procedures to comply with funds availability regulations. Failure to comply can result in regulatory scrutiny and erode accountholder confidence in electronic payments.

Unauthorized Transfers

Like most electronic payment mechanisms, financial institutions must prepare for the inevitability of unauthorized payments and how to investigate and support accountholder claims and inquiries accordingly. While many aspects of handling unauthorized instant payments will be like other electronic payments it is also important to note some considerations. From a receive only perspective financial institutions need to ensure they are clear on how they will receive any requests for returns claiming the credit transfer was unauthorized and have clear policies and procedures on how to document, investigate, and respond to such requests. In some instances, this may feed into existing applications, processes, and procedures, or may warrant separate processes to be created. Certainly, the implications of unauthorized payments are greater for financial institutions that support sending instant payments, which will be covered in a subsequent bulletin.

Funds Availability Exceptions 210.44(b)(3)

Regulation J 210.44(b)(3)[28] provides the regulatory framework for the receiving institution to delay posting of the transaction when it has reasonable cause to doubt that the beneficiary is not entitled or permitted to receive the payment. Receiving institutions can delay posting if they notify their Federal Reserve Bank that additional time is needed to determine if the beneficiary is entitled to the funds. When the beneficiary financial institution takes this action, it does not accept the payment order when it receives payment from the Federal Reserve.

This is a critical provision to enable receiving institutions to implement real time fraud monitoring and OFAC sanction screening for payments received through the instant payment networks. Both instant payment networks enable institutions that run real time fraud and OFAC monitoring to detect potential fraud or OFAC matches and use the response accept without post to allow time for a manual review of the transaction prior to posting. Efforts to detect and deter fraud and sanctioned parties from leveraging instant payment networks is critical to maintaining accountholder confidence in the security and reliability and would not be possible without this provision. Receiving institutions should develop appropriate policies and procedures that document the steps necessary for staff to perform expeditious evaluation of potential fraud or OFAC sanctions and either post or return the payments.

Electronic Fund Transfer Act (EFTA)[29]

The Electronic Fund Transfer Act (EFTA) establishes the foundational framework for electronic payments, including instant payments, ensuring consumer protection and transparency. Under EFTA, financial institutions are required to provide consumers with clear disclosures regarding their rights and responsibilities when receiving electronic payments. This includes requirements related to disclosure of fees and limits, cancellation and error correction resolution procedures, liability, preauthorized transfers, and receipts. Additionally, any unauthorized transactions must be promptly investigated and resolved by the financial institution. In the context of instant payments, these provisions are critical to building and maintaining consumer trust, especially as instant payments continue to emerge.

As instant payments function inherently different from other payment rails, especially when it comes to the irrevocability and the request for return of funds process, it will be important for financial institutions to appropriately educate their accountholders and build processes and policies that ensure the adequate transparency and protections are provided as intended under EFTA.

Mechanisms for Achieving Performance Requirements

In the dynamic sector of instant payments, especially with the integration of The Clearing House's RTP network and the Federal Reserve's FedNow Service, adhering to exacting performance standards is pivotal. Performance in this context is two-pronged: from a business and user perspective, it encompasses rapid transaction completion; technically, it involves the requisite infrastructure to efficiently meet these standards.

The RTP network and FedNow set ambitious SLAs — 15 and 20 seconds, respectively, for end-to-end transaction completion. Meeting these SLAs bolsters accountholder trust and involves strategic measures such as using transaction status (pacs.028) and confirmation messages (pacs.002) for efficient exception handling and operational strategies that ensure conclusive payments. Reducing reliance on manual processes is critical for maintaining the networks' real-time capabilities.

- **Technological Imperatives:** To leverage instant payment networks, financial institutions must revamp their technology infrastructure. Key technologies include cloud computing for scalability, APIs for seamless integration, and in-memory processing for high-speed data handling. These technologies ensure the rapid processing of payments, aligning with the expediency expected in modern payment systems.

- **Financial Landscape:** The integration of cutting-edge technologies like cloud computing APIs is now a necessity for financial institutions to facilitate real-time payments. Traditional banking systems, bogged down by legacy processes, fall short of today's digital demands. Cloud computing APIs provide the needed scalability, flexibility, and velocity, enhancing accountholder experiences and improving operational efficiencies.

- **Real-World Application:** Consider a financial institution that leverages cloud computing to dynamically scale its infrastructure during high transaction periods, like holiday shopping seasons, ensuring uninterrupted service. Similarly, APIs facilitate the integration of banking systems with e-commerce platforms, enabling real-time transactions for consumers and businesses alike. For FedNow and RTP compliance, financial institutions should adopt a blend of technologies including cloud computing for scalable infrastructure, APIs for system integration, and AI for fraud detection. Mobile and digital banking applications should feature advanced security measures like biometric authentication for accountholder convenience and security.

- **Decision Points for Financial Institutions:** Financial institutions must decide between in-house development or outsourcing to third-party vendors for instant payment solutions. In-house systems offer customization and control but require significant investment. Third-party vendors provide expertise and infrastructure, potentially speeding up market entry.

- **Infrastructure Choices:** Choosing between on-premises and cloud-based (off-premises) solutions is crucial. On-prem offers control and data security, while cloud-based solutions offer flexibility and scalability. Each choice has implications for data security, operational continuity, and cost.

- **Effective Operating Models:** For optimal instant payment processing, integrating automated reporting, real-time status updates, and efficient Payment Status Requests (PSR) is essential. A robust status response mechanism, especially through ISO 20022 standards like pacs.002, is crucial for ensuring transaction reliability and prompt error resolution.

- **Governance and Risk Management:** Robust control mechanisms, effective data management, and integrated systems for automatic reconciliation and ERP integrations are indispensable. These ensure secure, accurate, and efficient payment processing, meeting the high demands of modern financial transactions. Incorporating these insights and use cases provides a comprehensive understanding of the mechanisms and strategies necessary to meet the performance requirements in the realm of real-time payments.

Exception Processing[30]

The acceptance of instant payments brings with it a complex challenge: managing exceptions in an environment where immediacy leaves little room for traditional processing delays. Meeting the requirements of the payment rail and the ever-increasing demands of accountholders, while still maintaining due diligence and limiting liability brings with it many challenges that financial institutions need to navigate.

Conversely, the instant nature of these payments eliminates many of the manual exceptions experienced in other payment rails, such as non-sufficient funds (NSF), account not found, over limit, etc. In these situations, the payment would be systematically rejected with no intervention needed. This section delves into the intricacies of exception handling within financial institutions while navigating the instant payment framework. Financial institutions should be prepared to manage the following types of exceptions when receiving instant payments:

- **Funds Return Request:**[31] Financial institutions may occasionally receive a Request for Return of Funds (RTP Network) or a Return Request (FedNow) message camt.056 from the sending institution. This message is sent by the sending financial institution when a sender identifies an erroneous or fraudulently induced payment to recover the funds. The receiving institution must investigate and respond to the request using the camt.029 message. In the case where the financial institution determines that funds will be returned, the funds should be sent back using the pacs.008 for the RTP network and the pacs.004 message for FedNow. For financial institutions on the RTP or FedNow network that do not have send capabilities enabled, funds may be returned through other payment rails such as ACH or wire transfers. Some vendors may support the ability for receive-only RTP participants to send return of funds payments. Both networks place no liability on the receiving financial institution to return the funds but do require that the receiving financial institution uses reasonable efforts to aid in the investigation and recovery of the funds. Both networks require that a final determination and response be made within ten business days in most cases but do allow for longer investigations when needed. Financial institutions should consider the following:

    - Develop processes and procedures for receiving, investigating, and responding to requests for return.
    - Designate a department or staff that will be responsible and have appropriate authority to make decisions on returning funds.
    - Document clear criteria for return decisions.
    - Ensure that records of requests, investigations, and determinations are retained as evidence of compliance with network rules.
    - Ensure that the system maintains an audit and history file with linkage to the original transaction and all subsequent actions.

- **Accept without Posting:** A receiving participant may send an "Accept without Posting" message when it has not yet determined whether to send an "Accept" or "Reject" message in response to the payment message and will not provide immediate funds availability to the receiver due to the need to further review the transaction. An Accept without Posting message should not be used for any other reason outside the need to review for legal or compliance purposes, such as AML or sanctions compliance, suspected fraud, or if the account is subject to certain court-ordered restrictions. Once researched, the receiving participant must, as applicable, either make funds available and send a follow up acknowledgement message to the sending participant or refund the amount of the payment to the sending participant. Financial institutions should consider the following:

    - Designate a department or staff that will be responsible and have appropriate authority to make decisions on these alerts. Typically, these decisions would require review by BSA/AML staff for potential OFAC reviews and fraud analysts for fraud alerts.

    - Develop processes and procedures for receiving, investigating, and responding to alerts. Institutions may be able to leverage existing processes used for other payment channels such as ACH and Wires.

    - Ensure that records of alerts, investigations, and determinations are retained as evidence of compliance with AML/BSA and network rules.

- **Report of Abuse (Fraud Reporting):** Financial institutions have the obligation to decisively act upon and report fraudulent activity, including notification of fraudulent activity or transactions from FedNow or RTP providers. It is important that institutions have well-documented procedures in place for the review of any suspected fraudulent activity or fraud notification and actions required, if any. The integration of these processes into the institution's operational framework is a major component of a strong fraud mitigation plan and the ability of institutions to meet FedNow and RTP fraud reporting requirements. Furthermore, as fraud activity increases in sophistication and complexity it is important that participants stay abreast of emerging trends in the industry and potential enhancements to fraud reporting requirements in instant payments. In summary, a proactive posture and appropriate review and update of internal controls in response should be a key component of institutions processing instant payments and meeting minimum FedNow and RTP fraud reporting requirements. Financial institutions should consider the following:

- Designate a department or staff that will be responsible and have appropriate authority to review and make decisions on these reports.
- Develop processes and procedures for receiving, investigating, and responding to reports of abuse.
- Define criteria and steps to take in suspending or terminating users when abusive activity is confirmed.
- Ensure that records of reports, investigations, and determinations are retained as evidence of compliance with network rules.

- Request for Information (RFI), Request for Payment Cancellation, & Other Administrative Messages: The instant payment networks allow for nonvalue messages for the exchange of information and requests. Although payments are final and irrevocable, and therefore money is not required to be returned, participants should respond to nonvalue messages to cooperate with other participants seeking to address and recover from errors or erroneous payments.

- Payment Status Request (Pacs.028): The payment status request message is available from both the RTP network and FedNow to be used to automate some exception handling on the processing of a payment. The RTP system allows for the payment status request to be used on both the sending and receiving side. On the receiving side specifically, the payment status request can be used if a final 5th leg pacs.002 message is not received to trigger the final status to be sent from the RTP network so that the financial institution can put the payment in final status. FedNow allows for the same behavior on the receiving side. Both schemes allow the use of pacs.028 to assist on the sending side as well, which will be covered when send capabilities are reviewed in depth.

- Payment Status Research: Although the instant nature of these payments will inherently reduce questions related to the status of payments, there will still be some accountholder questions. Training materials centered on troubleshooting instant payments questions, along with clear communication protocols will be crucial in empowering staff to address accountholder concerns promptly and efficiently, thereby maintaining trust and satisfaction.

In addition to these considerations for receiving instant payments, upon deciding to send instant payments, financial institutions will need to prepare for processing exceptions such as outgoing OFAC/fraud queues, setting and maintaining accountholder limits for sending transactions and requests for payments, and additional fraud monitoring including velocity checks for potential account takeover.

Mechanisms and Processes for Reconciling Incoming Funds in Real-Time

It is imperative for financial institutions to build out and/or adapt existing processes to reconcile the instant payments they receive. Given the 24x7x365 nature of these payments, having well-defined, reconciliation processes will ensure any out of balance situation can be addressed and corrected as soon as possible, minimizing any impact to the financial institution or accountholder. This section will cover key considerations related to automation, end-of-day reconciliations, and reconciling internal and/or customer accounts.

Automation is Key

Having an automated reconciliation process is crucial to managing an instant payments rail. Automation improves reconciliation efficiency and minimizes the risk of errors associated with manual data entry. At a minimum, financial institutions should have an automated end-of-day reconciliation process. Best practice, and a goal to work towards for those financial institutions on batch processing, would be implementing real time reconciliation. This means a financial institution can reconcile every payment that comes in throughout the day at the time it is received.

Reconciliations can be built in-house or can be automated using a single, seamless vendor software solution designed to manage large volumes of data from multiple data sources at speed. Though few vendors tout reconciliation of FedNow and RTP payments today, there are several real-time reconciliation solutions available on the market that are well positioned to reconcile instant payments data. Both end-of-day reconciliation with the network and internal reconciliation methods will be discussed further within this section.

Real-Time Reconciliation

As the instant payment networks both send a message to the receiving institution to confirm the settlement of the payment, these messages can also be relied upon to reconcile or validate the payment is in a final status. This should subsequently trigger funds to be made available to the recipient in real-time if not done so already within the payment process. This approach minimizes the risk of there being an issue with the payment reconciling to the network but should still be used in conjunction with applicable end of day reporting and reconciliation tools. In no circumstances should the availability of the payment to the recipient be delayed until end of day reconciliation has been completed.

For financial institutions with the capability to hard post payments in real-time, this method can be utilized to validate both against the networks and internally in real-time, but again, should still be used in conjunction with end of day reconciliation procedures.

End-of-Day Reconciliation

Both the RTP Network and the FedNow Service provide reports which allow financial institutions to perform automated reconciliations at the end of each "day." It is important to note that these reconciliations are not based on calendar days, rather they are based on any payment received within the respective Cycle Date (FedNow) or RTP Day. The RTP Day ends at 11:59:59 PM ET, whereas the FedNow Cycle Day ends at approximately 7 PM ET.

- **RTP Reconciliation**: Participants of the RTP Network can utilize the System Notification Message (SNM) 999 or the Participant Reconciliation Report to automatically reconcile against the financial institutions' internal logs. Financial institutions should utilize the interbank settlement date when reconciling against their internal logs. Based on this reconciliation, all records would either match or a discrepancy would be identified. If a discrepancy is identified, escalation procedures must be documented to notify an individual to investigate and fix the situation if needed. If the reconciliation is out of balance, the Detailed Payment Reconciliation Report can be utilized to complete a detailed analysis to understand and locate the missing or out-of-balance transaction(s).

- **FedNow Reconciliation**[32]**:** Participants of FedNow can utilize the Account Activity Totals Report and Account Activity Details Report to automatically reconcile against the financial institution's internal logs; these reports are also available for Correspondents settling payments on behalf of their Respondents. This report can be scheduled at the end of Cycle Day via ISO Message and can be used to kick off the automated reconciliation process; the totals report is also available intraday. These reports can also be generated through the FedNow interface. The FedNow Service Cycle Day aligns with the close of the Fedwire Funds Service, which is approximately 7 PM ET. If Fedwire Funds Service extends, FedNow's Cycle Day will extend accordingly. The FedNow Service assigns the applicable Cycle Day to the transaction and includes it within the advice of credit message. Based on this reconciliation, all records would either match or a discrepancy would be identified. If a discrepancy is identified, escalation procedures must be documented to notify an individual to investigate and fix the situation if needed. If the reconciliation is out of balance, the Activity Details Report can be utilized to complete a detailed analysis to understand and locate the missing or out-of-balance transaction(s). Additionally, Correspondents can use the Account Debit/Credit Notification camt.054 message to assist in reconciliation of payments settled for Respondents' FedNow activity.

It is important to build a process that is flexible to allow for potential delays in receiving reports or System Notification Messages. With the RTP Network, there is also the potential of multiple reconciliation windows per day, which must be built into the automated reconciliation process. Additionally, financial institutions should build this automated process to reconcile every day of the week and have appropriate procedures in place to manage and address any out-of-balance reconciliations.

Reconciling with Accountholders and Internal General Ledger Accounts

In addition to "end of day" reconciliations, financial institutions should build a process to reconcile internally with its accountholders and/or general ledger accounts. The best practice is to complete this reconciliation in real-time utilizing the pacs.002 message (camt.054 message for Correspondents on the FedNow Service). This reconciliation is an internal reconciliation that ensures that accountholders' accounts were credited appropriately as soon as the credit transfer is accepted. Automated real-time reconciliation provides more accurate data for funds availability calculations than slower and more manual efforts.

However, many financial institutions are still utilizing batch processing and may not be able to complete this type of reconciliation in real-time. It is important to note that although hard posting may not occur until batch processing is complete, the funds still need to be memo credited and available to accountholders in real-time. In this situation, financial institutions will need to complete an internal reconciliation of their general ledger accounts once funds have been posted to ensure accountholders' accounts were credited appropriately. If out of balance, they should first validate all transactions are complete and have a final status.

Conclusion

These guidelines highlight the transformative impact of instant payment systems like the RTP network and the FedNow service on financial institutions, underscoring the significant operational changes required to adapt to this new era of payment processing. Unlike traditional legacy rails, instant payments demand immediate transaction confirmations, 24x7x365 operational readiness, and automated processes for handling errors and rejections.

This shift necessitates a more dynamic approach to liquidity management, real-time settlement, and continuous monitoring of financial positions. Financial institutions must also enhance their technological infrastructure, fraud detection mechanisms, and compliance strategies, including rigorous KYC protocols and advanced analytics, to manage the increased risks associated with instant transactions. Reconciliations for receiving banks will be one of the more challenging hurdles to solution.

The critical importance of robust business continuity plans, effective exception handling, and comprehensive staff training is also evident in ensuring seamless adaptation to these real-time payment systems.

Overall, these developments mark a significant evolution in the financial landscape, requiring proactive adaptation and a keen focus on operational efficiency, security, and regulatory compliance that may require material investments in governance, talent, operating model design, policy and procedure updates, vendor partnerships, business intelligence reporting and communications, and risk management. While this paper does not solve for all issues and/or provide all the various solutions that exist, it does hope to provide the deeper level information on the challenges that arise and how others have already solved for these that financial institutions can leverage and explore as they move towards their instant payment journey.

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 this guideline.

OCWG Leadership

Miriam Sheril (Chair), Form3 US Inc.
Tony Cook (Vice Chair), FirstBank
Kevin Michels (FPC WG Facilitator), Guidehouse

OCWG Contributors

Lisa Richmond, Alloya Corporate FCU
Bret Henderson, BOK Financial
Dana Woller, BOK Financial
Martha Dixie, Corporate One
Nicole Payne, EPCOR
Marcia Klingensmith, Fintech Consulting, LLC
Kerri Rachal, First National Bankers Bank
Maranda Blake, FirstBank
Mary Gilmeister, Macha
Jeanette Waye, PaymentsFirst Inc.
Stephen King, RedCompass Labs
Sudeep Manchanda, RedCompass Labs
Rodman Reef, Reef Karson Consulting, LLC
Susan Currey, Sionic Mobile Corporation
Barry Tooker, TransactionBanker.com
Nathan Carman, Wespay

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] RTP is a registered service mark of The Clearing House Payments Company L.L.C.

[2] Faster Payments Council. (2023, October). *Guideline.01: Operational Considerations for Instant Payments Receive-Side Primer.* https://fasterpaymentscouncil.org/userfiles/2080/files/Operational%20Considerations%20for%20Instant%20Payments%20Guideline_10-2023_Final.pdf.

[3] The RTP Network Operating Rules only permit accept without posting responses under certain circumstances.

[4] The Clearing House. (2023, March 19). *RTP® System Operating Rules.* https://media.theclearinghouse.org/-/media/New/TCH/Documents/Payment-Systems/rtp_operating_rules_effective_03-19-2023.pdf?rev=a26f0c495a1145adb79e7ec9be8cf034&hash=502D59B5AB389397960EC42F14A47BC4.

[5] The Federal Reserve Financial Services. (2023, March 3). *FedNow℠ Service Operating Procedures.* https://www.frbservices.org/binaries/content/assets/crsocms/resources/rules-regulations/030323-fednow-operating-procedures.pdf.

[6] Faster Payments Council. (n.d.). *Use Case Repository.* Retrieved September 9, 2024 from https://fasterpaymentscouncil.org/use-cases.

[7] The Clearing House. (n.d.). *RTP: RTP® Participating Financial Institutions.* Retrieved September 9, 2024 from https://www.theclearinghouse.org/payment-systems/rtp/RTP-Participating-Financial-Institutions. The Federal Reserve. (n.d.). *FedNow® Service Participants and Service Providers*. Retrieved September 9, 2024 from, https://frbservices.org/financial-services/fednow/organizations.

[8] The Clearing House. (2021, November). *RTP® Customer Inquiry Management (CIM) Playbook.* https://media.theclearinghouse.org/-/media/New/TCH/Documents/Payment-Systems/05_RTP_Customer_Inquiry_Management_Playbook_v1_2021019.pdf?rev=2ba69398ca394469b20b9092170d1ebe&hash=811E9941212914AEA9B2829C2B62AA24.

[9] Consumer Financial Protection Bureau. (n.d.). *§ 1005.11 Procedures for resolving errors.* Retrieved September 9, 2024 from https://www.consumerfinance.gov/rules-policy/regulations/1005/11/.

[10] The Clearing House. (2019, January 7). *RTP Operator - Customer Information Security Standards.* https://media.theclearinghouse.org/-/media/New/TCH/Documents/Payment-Systems/RTP_Operator_Customer_Information_Security_Standards_Schedule.pdf?rev=25391652ad5f4742a12c570b2b77de92&hash=AFF90D3B93CA68EA67FE623455F6FFAE.

[11] FedNow. (n.d.). *General Reserve Bank Data Privacy Notice.* Retrieved September 9, 2024 from https://explore.fednow.org/data-privacy.

[12] Consumer Financial Protection Bureau. (n.d.). *§ 1005.6 Liability of consumer for unauthorized transfers.* Retrieved September 9, 2024 from https://www.consumerfinance.gov/rules-policy/regulations/1005/6/.

[13] eCFR. (n.d.). *12 CFR Part 210 Subpart C -- Funds Transfers Through the FedNow® Service.* Retrieved September 9, 2024 from https://www.ecfr.gov/current/title-12/chapter-II/subchapter-A/part-210/subpart-C.

[14] **Additional Resources:**

- FedNow. (n.d.). *Resources.* Retrieved September 9, 2024, from https://www.frbservices.org/binaries/content/assets/crsocms/resources/rules-regulations/120423-fednow-operating-procedures.pdf.
- The Clearing House. (n.d.). *RTP®*. Retrieved September 9, 2024, from https://www.theclearinghouse.org/payment-systems/rtp; https://www.theclearinghouse.org/payment-systems/rtp/document-library.
- Faster Payments Council. (2022, July). *Examining Faster Payments Fraud Trends.* https://fasterpaymentscouncil.org/userfiles/2080/FraudInfoSharingWP.pdf.
- Faster Payments Council. (2022, March). 2021 *Faster Payments Fraud Survey and Report.* https://fasterpaymentscouncil.org/blog/8621/2021-Faster-Payments-Fraud-Survey-and-Report.
- Faster Payments Council. (2022, July). *Faster Payments and Financial Inclusion.* https://fasterpaymentscouncil.org/userfiles/2080/files/Financial%20Inclusion%20White%20Paper_7-29-2022_Final.pdf.
- The Federal Reserve. (n.d.). *FraudClassifierSM Model.* Retrieved September 9, 2024, from https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/fraudclassifier-model/.
- The Federal Reserve. (2023, September 15). *Federal Reserve System announces industry-recommended scams definition.* https://www.frbservices.org/news/fed360/issues/091523/industry-perspective-scams-definition-announcement.
- Faster Payments Council. (2024, January). *Faster Payments Fraud Trends and Mitigation Opportunities (Bulletin .01).* https://fasterpaymentscouncil.org/userfiles/2080/files/FPC%20Fraud%20Bulletin_01_01-24-2024_Final.pdf.

[15] P2. (2023, October). *Public-Private Data Exchange for Fraud Prevention: Best Practice Recommendations.* https://static1.squarespace.com/static/5efcc6dae323db37b4d01d19/t/652838a429e8a3542649bbe1/1697134757431/P20+ Report+-+Public-Private+Data+Exchange+for+Fraud+Prevention.pdf.

[16][17] The Federal Reserve. (n.d.). *FraudClassifier℠ Model.* Retrieved September 9, 2024, from https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/fraudclassifier-model/.

[18] The Federal Reserve. (n.d.) *Scams.* Retrieved September 9, 2024, from https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/scams/#:~:text=In%202023%2C%20the%20Federal%20Reserve,intended%20to%20achieve%20financial%20gain.

[19] Consumer Financial Protection Bureau. (2020, July 21). *12 CFR Part 1005 - Electronic Fund Transfers (Regulation E).* https://www.consumerfinance.gov/rules-policy/regulations/1005/.

[20] Uniform Law Commission. (n.d.). *Uniform Commercial Code.* Retrieved September 9, 2024, from https://www.uniformlaws.org/acts/ucc.

[21] The Clearing House. (2023, March 19). *RTP® System Operating Rules.* https://media.theclearinghouse.org/-/media/New/TCH/Documents/Payment-Systems/rtp_operating_rules_effective_03-19-2023.pdf?rev=a26f0c495a1145adb79e7ec9be8cf034&hash=502D59B5AB389397960EC42F14A47BC4.

[22] [26] The Clearing House. (n.d.). *RTP®.* Retrieved September 9, 2024, from https://www.theclearinghouse.org/payment-systems/rtp; https://www.theclearinghouse.org/payment-systems/rtp/document-library.

[23] Faster Payments Council. (2024, January). *Faster Payments Fraud Trends and Mitigation Opportunities (Bulletin .01).* https://fasterpaymentscouncil.org/userfiles/2080/files/FPC%20Fraud%20Bulletin_01_01-24-2024_Final.pdf.

[24] Cornell Law School. (n.d.). *12 CFR Subpart C - Subpart C—Funds Transfers Through the FedNow Service.* Retrieved September 9, 2024, from https://www.law.cornell.edu/cfr/text/12/part-210/subpart-C.

[25] The Federal Reserve. (2022, September 21). *Funds Transfers Through the FedNow℠ Service.* https://www.frbservices.org/binaries/content/assets/crsocms/resources/rules-regulations/operating-circular-8.pdf.

[27] YouTube. (2023, December 18). *Payments Professor: Does UCC 4A apply to FedNow? FedNow Rules and Regulations.* https://www.youtube.com/watch?v=COJBGOVnlyQ.

[28] Cornell Law School. (n.d.). *12 CFR § 210.44 - Agreement of receiving bank.* Retrieved September 9, 2024, from https://www.law.cornell.edu/cfr/text/12/210.44#:~:text=(3)%20In%20circumstances%20where%20the,determine%20whether%20to%20accept%20the.

[29] Federal Trade Commission. (n.d.). *Electronic Fund Transfer Act.* Retrieved September 9, 2024, from https://www.ftc.gov/legal-library/browse/statutes/electronic-fund-transfer-act.

[30] FedNow Service. (2024, June). *FedNow® Service Operating Procedures.* https://www.frbservices.org/binaries/content/assets/crsocms/resources/rules-regulations/0624-fednow-service-operating-procedures.pdf; The Clearing House. (2021, May 21). *RTP Rules and Legal Framework (Part 2).* https://media.theclearinghouse.org/-/media/New/TCH/Documents/Payment-Systems/RTP_Rules_Video_Part_2.pdf?rev=3dc6ab4d114547c4babb8c4b4761b420&hash=B5AFA57765821A9DD6CD12F6BAA41847 and (2019, September 9). *RTP Rules: Interpretation Fraud Reporting and Acting on Alerts.* https://media.theclearinghouse.org/-/media/New/TCH/Documents/Payment-Systems/Fraud_Alerts_and_Reporting_09-09-2019.pdf?rev=511c74ae37d44c52ab9603b244aa10d2&hash=93F3A43FEB383A316E0AC3A939A73E1F.

[31] The Clearing House. (2023, March 19). *RTP® System Operating Rules.* https://media.theclearinghouse.org/-/media/New/TCH/Documents/Payment-Systems/rtp_operating_rules_effective_03-19-2023.pdf?rev=a26f0c495a1145adb79e7ec9be8cf034&hash=502D59B5AB389397960EC42F14A47BC4. FedNow Service. (2024, June). *FedNow® Service Operating Procedures.* https://www.frbservices.org/binaries/content/assets/crsocms/resources/rules-regulations/0624-fednow-service-operating-procedures.pdf; The Federal Reserve. (2022, September 21). *Funds Transfers Through the FedNow℠ Service.* https://www.frbservices.org/binaries/content/assets/crsocms/resources/rules-regulations/operating-circular-8.pdf.

[32] It is important to note the FedNow Service debits and credits the designated master accounts of the sender's and receiver's FI, and therefore all FedNow transactions are included as part of the master accounts' end of cycle day reconciliation.