The Clearing House®

U.S. Real-Time Payments Technology Playbook

Version 1.0
November 2016

Proposed features, functionality, implementation details, requirements and timetables are in development and subject to change at any time.

Real-Time Payments Playbooks

Real Time Payments (RTP) provide consumers and businesses with the ability to immediately send and receive funds directly from their accounts at financial institutions anytime 24/7/365. RTP represents a new phase of evolution within the United States (U.S.) payments industry, with several key features that differentiate them from current payment methods, specifically speed, value-added messaging capabilities, and immediate availability of transaction status. RTP will provide FIs with the functionality and features to innovate for the future.

Outside the U.S., many countries are developing "faster payments" systems to expedite the movement of money and increase the speed with which transferred funds are made available to recipients. Within the U.S., The Clearing House (TCH) is leading a multi-year effort to build a real-time payments system (RTP) that addresses the needs for safer and faster payments in an increasingly digital economy.

Your institution has expressed interest in finding out more about the RTP system and what it would take to implement. TCH has developed three targeted playbooks highlighting considerations for business, operations and technology audiences. As each FI is different, these playbooks should be considered guidelines rather than rules to give your organization the information and insight it needs to get started. In addition, contact information for TCH experts can be found in the Contact Us section on page 47.

BUSINESS PLAYBOOK 01

The Business Playbook provides a basic understanding of the real-time payments system and the potential for using it as a platform to develop new services. This playbook includes consideration of the involvement of various business units and specific items to consider as you develop your ideas and plans.

OPERATIONS PLAYBOOK 02

The Operations Playbook provides a basic understanding of the real-time payments system and outlines the processes and procedures that may be needed across various operational areas within your organization as you implement the RTP system.

TECHNOLOGY PLAYBOOK 03

The Technology Playbook contains a technical overview of the RTP system for participating FIs in order for them to develop high-level estimates for interfacing to the RTP system.

The Clearing House owns and operates payments technology infrastructure, which clears nearly $2 trillion each day for financial institutions in the U.S. and around the world. Its business is developing and operating industry utilities focused on safer and faster payments.

Contents

Technology Playbook

01: What is the RTP Playbook?

RTP Playbook purpose and objectives

The purpose of the RTP Playbook is to provide a high-level description of the functionality of the RTP system from an FI's perspective and to identify important considerations for implementation of RTP. The Playbook offers information to support communications with an FI's internal and external stakeholders (e.g., vendors and regulators), as it moves forward with its RTP effort. The playbook can also be used to create awareness by providing a clear understanding of what RTP is, identifying key benefits, and providing a framework highlighting key action items and decision points organizations should consider as they begin planning and execution of their RTP implementation.

The following pages include key tasks and decision points, along with practical tools and tips for RTP planning and implementation. It provides guidance and recommended practices in the form of checklists, reminders, and useful exercises to assist your organization in delivering RTP.

01 How to use this document
Call out symbols and icons help you use this document to its fullest extent.

02 Overview of Real-Time Payments
Describes real-time payments and how they work. Provides examples that demonstrate the breadth and scope of RTP. Clarifies the role of RTP in the payments ecosystem.

03 How do Real-Time Payments Work?
Illustrates use case scenarios in the RTP system, including step-by-step flow of messages.

04 Business Case Considerations
Demonstrates opportunities for new products and markets. Supports analysis of operations and technology investments and associated costs.

05 Technology Considerations
Identifies key features of RTP, provides an overview of architecture and messaging requirements, highlights important considerations to take when designing an interface to RTP.

06 Checklists and Supporting Documentation
Provides useful integration and consideration checklists and overviews of supporting systems documentation.

07 Contact Us
Provides contact information for experts who will answer questions and assist you as needed.

Technology Playbook target audience

The RTP Technology Playbook is intended for FI technology teams and technology partners that will design and develop the interface to the RTP system.

How to use this document

Throughout the Playbook, icons will appear that represent important notes, tips, or resources that you can reference to help navigate the process of implementing RTP. There are specific callouts to focus attention on key decision points, action items, and checklists that FIs should consider.

IMPORTANT The "Important" icon marks the information or action item that is of utmost importance for a successful implementation. You should pay special attention to this information and ensure that these items are tracked to closure.

TIPS / FACT CHECK The "Tip / Fact Check" icon indicates helpful information about the industry. You may discover a leading practice in the field or an innovative way to implement your solution to save time or money.

CHECKLIST The "Checklist" icon highlights a list of recommended considerations for approaching a specific RTP concept or task. For example, these lists may be used as a starting point for project managers when creating a plan to complete a specific RTP-related task identified in the Playbook.

RESOURCES The "Resources" icon marks the section offering links to additional resources on a topic. Resources may include embedded file attachments, external sites, files, white papers, or press releases.

DECISION POINT The "Decision Point" icon highlights a step where your FI will need to make a decision regarding the implementation of RTP.

STAKEHOLDERS The icons displayed in the "Stakeholders" callout box indicate groups that may have an interest in RTP within your organization. Highlighted icons represent areas that should be involved in the discussion of the topic while grayed icons represent groups that may have less of an interest in that topic.

02: Overview of Real-Time Payments

What are Real-Time Payments?

Real-time payments provide consumers and businesses with the ability to conveniently send and receive immediate funds transfers directly from their accounts at FIs, anytime 24/7/365. RTP is a new national payments system that will support this functionality and provides a platform for product innovation. Financial institutions can leverage a variety of features – enhanced speed, security, and messaging capabilities – to create unique offerings for their retail and corporate customers.

Real-Time Payment Characteristics

01 **24/7/365** – The RTP system will operate on a 24/7/365 model, which means the system will be available for customers to send or receive payments at any time.

02 **Immediate Availability –** Recipients will receive the payment within seconds of the Sender initiating the transaction; the Receiving FI is required to make funds available immediately, except where necessary for risk management or legal compliance purposes.

03 **Payment Certainty** – Senders will not be able to revoke or recall a payment once it has been authorized and submitted to the RTP system. However, there will be a process to facilitate FI-to-FI communication around return of funds sent in error.

04 **Ubiquity** – The RTP system will be accessible by all financial institutions, regardless of size or charter type, and will reach the vast majority of U.S. account holders.

05 **Extensibility** – Rich, flexible messaging functionality will be included to support value-added products. For example, the RTP system provides messaging capability enabling a request for payment directly via RTP.

06 **Account Data Privacy –** FIs may use tokens to encrypt receiver account information as it is transmitted through the RTP system.

07 **Safety and Security** – To deter fraudulent activity, RTP requires participants to provide strong authentication prior to initiating payments and provides network-level fraud monitoring and reporting.

08 **Cash Flow Control** – The ability to send and receive payments immediately will give customers more control over cash flow, which is particularly important for cash-constrained small businesses and consumers

09 **Adaptability** – The RTP system will have flexible architecture to adapt to changing market needs

10 **Global Standards** – The RTP system will adhere to global standards to the extent necessary to facilitate domestic needs

How are Real-Time Payments different?

CURRENT PAYMENT METHODS		REAL-TIME PAYMENTS
DELAYED AVAILABILITY – Due to unpredictable clearing times, the sender does not know for 1-3 days whether the transfer was successful and that funds are available to the receiver for use.	01	**Immediate Availability and Notification** With TCH's RTP system, receivers have immediate funds availability. Related status notifications are sent to senders (that a transfer was successful) and recipients (that funds are available).
PAYMENT REVERSAL – Payments may be reversed under certain circumstances and within a predefined period of time.	02	**Payment Certainty** Payments cannot be revoked or recalled once authorized by a sender and submitted to the RTP system.
CREDIT PUSH AND DEBIT PULL– ACH supports credit push as well as debit pull transactions.	03	**Credit Push Only** TCH's RTP solution will only support Credit push transactions. The payee may send a Request for Payment message but will not be able to pull funds directly from the payer's account.
LIMITED MESSAGING OPTIONS – Remittance information is typically included within the payment message itself.	04	**Flexible Messaging Options** TCH's RTP solution will provide flexible, robust messaging components with multiple options for enclosing remittance information. Options include using the payment message, sending a non-payment message, or referencing an external remittance source.
DELAYED FRAUD DETECTION – The time between the sending and actual posting of a payment allows for a window during which fraud analysis may be conducted.	05	**24/7 Fraud Detection** Fraud detection and controls will need to be enhanced and automated to correspond with the ability to move funds nearly instantaneously.

Who can use RTP?

Real-time payments are intended to be used for transactions between any entity whether business, consumer, or government.

Business to Business (B2B)

A ***small business*** paying an urgent invoice in order to receive goods or services

A ***restaurateur*** who pays for farm-fresh produce from the local farmer to serve that evening's dinner specials

Business to Consumer (B2C)

A ***utility company*** requesting payment for services from a business or consumer

A ***retail bank*** distributing personal loan proceeds to a dealership on behalf of a customer who is at the showroom buying a new car

An ***insurance company*** adjustor reviewing a claim, determining a settlement amount, and immediately providing funds to the policy holder

A ***small business owner*** who is paying temporary employee salaries or tips on an ad hoc basis

A ***large corporation*** paying employees for travel expenses in time for payment of corporate credit cards

Person to Person (P2P)

College roommates splitting monthly rent and utility payments

A ***head of household*** sending emergency funds to a family member on vacation

Consumer to Business (C2B)

A ***busy working individual*** paying for general services around the house such as the gardener, cleaning services, or child care provider

A ***day trader*** sending real-time money transfers to his or her investment account to take advantage of the most recent market swing

Government to Consumer / Consumer to Government (G2C/C2G)

A ***government agency*** paying out emergency disaster relief funds to citizens impacted by a natural disaster

A ***tax payer*** making his or her tax payment in time for the April 15 deadline

Defining the RTP Ecosystem

The Clearing House hosts the RTP core infrastructure for the U.S. providing:

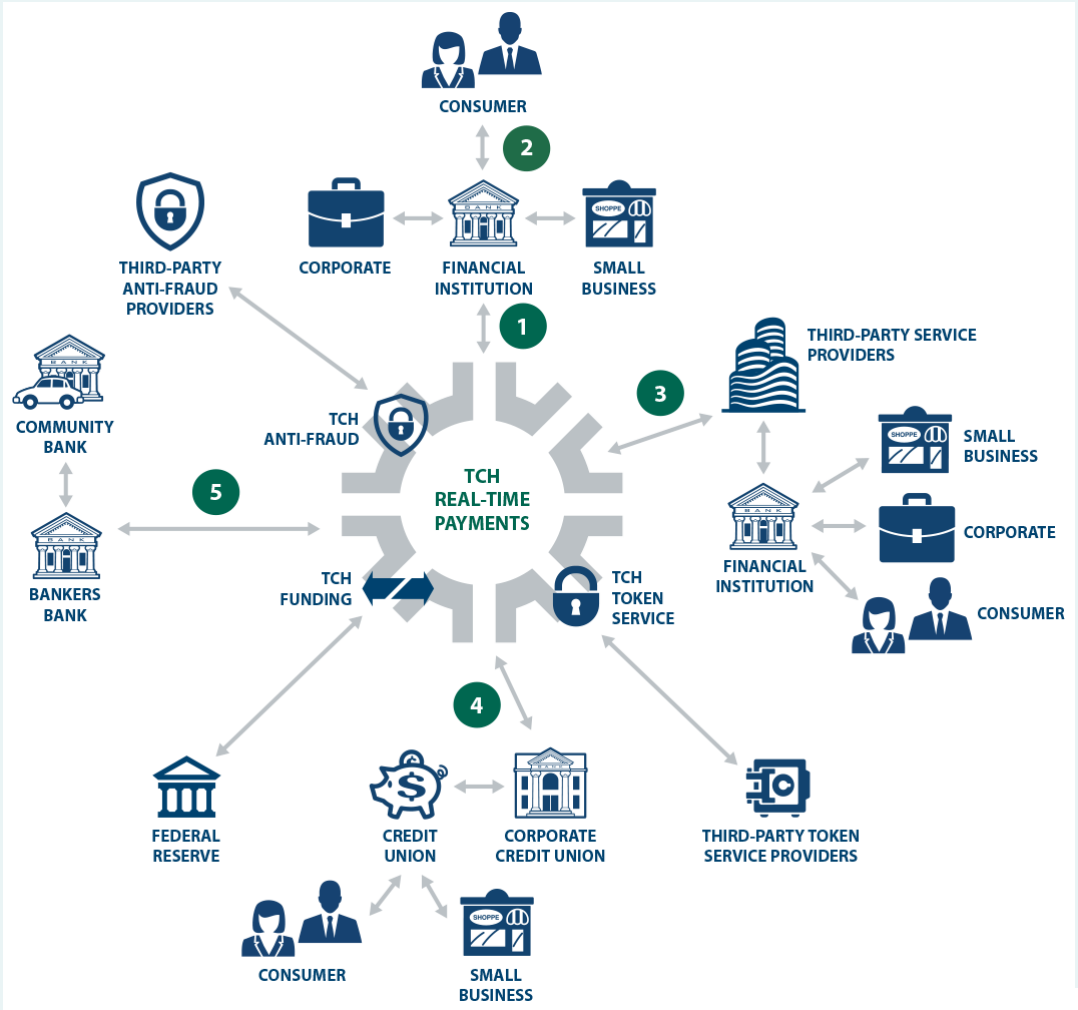
- *Payment processing services* – The RTP system orchestrates movement of payments and value-added messages to and from FI participants.
- Fraud Detection– The RTP system will offer fraud detection services to scan and report on network-level fraudulent activity. FIs will also be required to maintain their own automated real-time fraud detection capabilities to scan transactions being sent to and received from the RTP system.

Financial Institutions will have the ability to ***directly*** connect to the RTP core infrastructure to provide real-time payments capability and value-added payment related services to their customers and clients. FIs include (but are not limited to) global banks, regional banks, credit unions, community banks, etc.

Third-Party Service Providers (for example: FIS, Jack Henry and D +H) will provide connectivity into the RTP network, providing access to FIs that may not want to connect directly to the RTP system. They will also integrate RTP into their existing and new payments products for the benefit of their account holders.

Correspondent Banks*, Banker's Banks, Community Banks and Corporate Credit Unions, will provide connections to the RTP network as well as settlement services for FIs that may not want to connect directly to the RTP system.

* Note: Correspondent banks offer connectivity and liquidity services. This differs from conventional correspondent bank wire transfer services that may involve a series of bank transfers to complete a payment.



Note: There should be no difference in the user experience for customers of direct FIs and those connecting through a TPSP.

Illustrative RTP ecosystem

Drivers of real-time payments

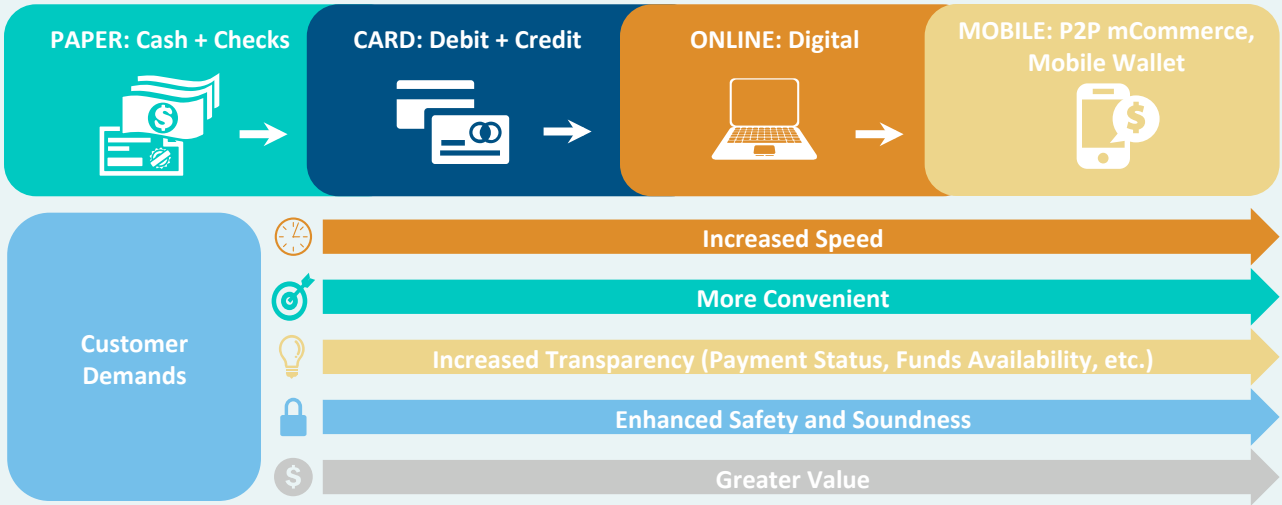
Customer demand

In today's world of sophisticated computing devices, information is moving in real-time. With high-speed data networks, and nearly universal presence of smartphones, customers expect everything – including payments – to keep up with their pace of life.

- **Increased speed:** Over the past decade, immediate delivery of electronic content and near real-time delivery of physical goods has become the norm. This along with faster, pervasive technology, has increased the expectation for faster payment solutions.
- **More convenient:** Customers are moving away from cash and checks in favor of the convenience associated with newer banking channels, like online and mobile. Growth rates of non-cash transactions in mature markets (North America, Europe, mature Asia-Pacific) have accelerated in the past few years, accounting for almost three quarters of the payments market.[1]
- **Increased transparency**: A faster pace of life means making sure payment information is transparent and readily available. Customers are looking for robust, real-time payment information, including payment status and immediate confirmation of funds availability.
- **Enhanced safety and soundness**: Despite an increase in data transparency, customers still expect their information to be kept secure and private. As data breaches have become nearly commonplace events, the demand from consumers for information privacy and security has continued to increase. FIs must work harder to implement the best and most secure systems to protect customer account data.
- **Greater value:** Banks and non-bank payment service providers are creating value-added services such as automated matching of purchase orders to invoices for businesses or geo-location based in-store promotions for consumers. These value-added services can span the entire purchasing experience beyond the payment itself. They enrich the basic payment data with a wider set of information to create added value.

The RTP system allows FIs to address consumer demands in the digital age – providing a way for consumers and businesses to make immediate payments to merchants and vendors in a safe and convenient manner.

Customer Adoption of New Payment Mechanisms



[1]World Payments Report. Capgemini and The Royal Bank of Scotland; 2015.

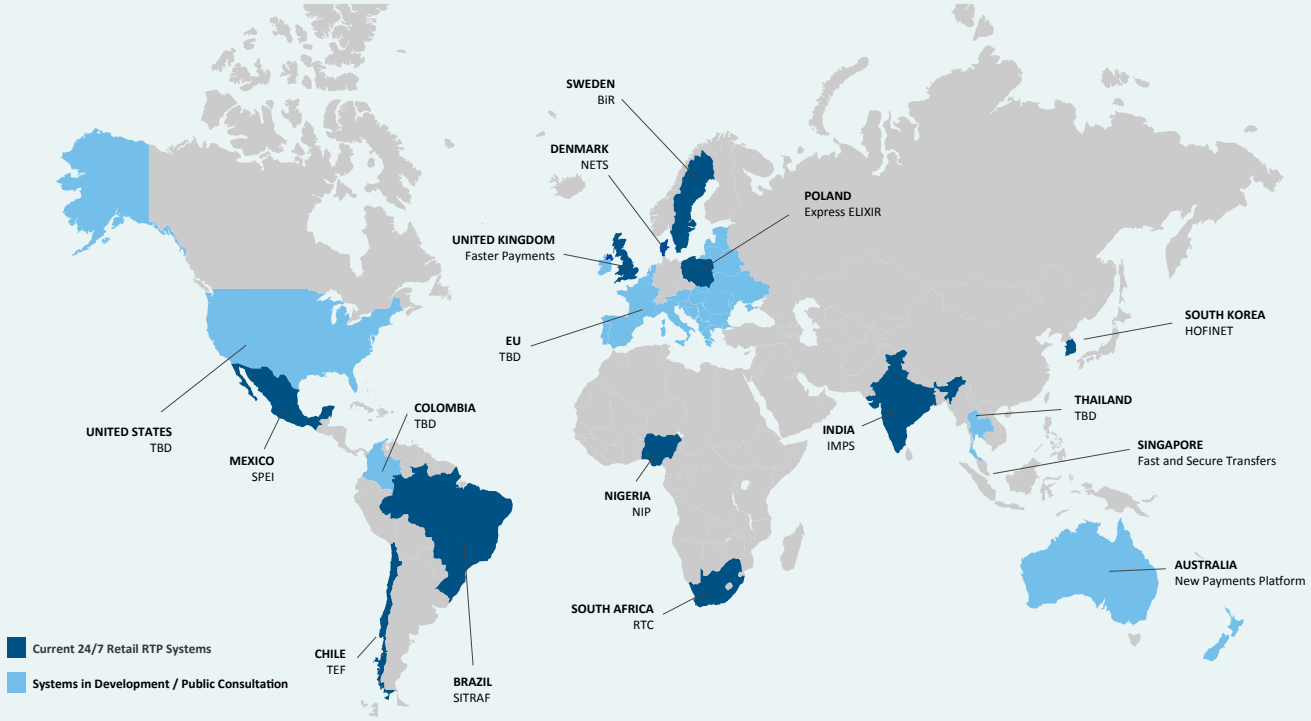
Drivers of RTP

Global competition

While TCH's RTP System is a new capability in the U.S. for FIs, at least 12 countries have implemented 24/7 retail RTP systems supporting immediate low-value account-to-account transfers,[1] and work is well underway in Australia, Europe, and the United States. The European Retail Payments Board has agreed on "the need for at least one pan-European instant payment solution."[2] In the United States, the Federal Reserve Board has called for the implementation of "a safe, ubiquitous, faster payments capability"[3] and The Clearing House has announced that it will create a national RTP system.

The diagram below illustrates the global span of 24/7 retail RTP systems to date. There is a clear trend towards more and more countries either having the ability to conduct faster payment transactions or starting the process of developing a system that allows them to do so.

Countries with 24/7 retail RTP systems that are live or in development



Countries with 24/7 retail RTP systems that are live or in development	
• Mexico – SPEI (2004) • Chile – TEF (2008) • Brazil – SITRAF (2002) • Sweden – BiR (2012) • Denmark – Nets (2014) • U.K. – Faster Payments (2008) • Poland – Express ELIXIR (2012) • Nigeria – NIP (2011) • South Africa – RTC (2006)	• India – IMPS (2010) • South Korea – HOFINET(2001) • Singapore – FAST (2014) • Australia – NPP (2016) • United States – TBD • Colombia – TBD • EU – TBD • Thailand – TBD

[1]KPMG Investigation
[2]Statement following the second meeting of the Euro Retail Payments Board European Central Bank European Retail Payments Board; December 1, 2014.
[3]Strategies for Improving the U.S. Payment System. United States Federal Reserve System; January 2015. p. 56

Drivers of RTP

Regulatory influence

The CFPB has raised several concerns regarding existing payments systems (e.g., the ability of fraudsters to initiated unauthorized debits, lack of transparency regarding when transactions will post). The CFPB believes that faster, safer payments capabilities will benefit consumers (e.g., by providing faster access to funds and greater certainty about funds availability) and sees opportunity for FIs to more effectively serve consumers with a new real-time payments functionality. As such, the CFPB is urging the financial services industry to make real-time payments an urgent priority to help mitigate many of the issues currently facing consumers.

Identified consumer risks with current payment system	RTP mitigation
Unauthorized debits from consumer accounts via ACH lead to unexpected fees to the customer and a significant effort for customers to stop payments and revoke orders	***Push transactions*** only; no auto-debit of customer accounts
Lack of transparency, particularly as it relates to ***funds availability,*** causes confusion for customers and often significant overdraft charges	***Real-time funds availability*** with payment certainty and extensive set of payment and non-payment related messages
Need for expedited payments and ***expedited funds access*** forces individuals with immediate needs or emergency situations to rely on high-cost money order services to expedite funds transfer	***RReal-time 24/7 payment ability*** for consumer to business and other payment transactions

Evolving payment technology capabilities

FIs need to offer their customers an RTP capability that provide speed, convenience, and transparency as well as the level of safety and security they expect from a traditional payments network.

Though not exhaustive, the following list represents the primary groupings of evolving technology players.

- **Closed loop cards and mobile apps**: Many non-bank companies have built closed loop card networks to promote loyalty programs and provide a convenient way for customers to pay for goods. The most successful example has been Starbucks' mobile app, which has seen a 75 percent growth in its mobile app transactions from 2013 (4 million transactions per week) to 2015 (7 million transactions per week).[1,2]
- **Digital wallets (non-banks)**: Digital wallets are beginning to gain traction among consumers as they provide an easy and flexible method to transfer money. PayPal's digital wallet continues to increase in mobile payment transactions, growing 40 percent year-over-year.[3] The industry anticipates mobile wallet usage to reach 200 million transactions by the end of 2016.[4]
- **Mobile money (non-banks):** Mobile money allows consumers to access financial services, such as money transfer or bank account access, via use of the mobile phone. In 2014 alone, mobile money services in the U.S. such as Square Cash and Venmo handled $5.2 billion in P2P payments.[5]

[1]Why Is The Starbucks Mobile Payments App So Successful? Forbes; June 13, 2014.
[2]Starbucks's Mobile App Payments Now Represent 16% of all Starbucks Transactions. Fast Company; January 23, 2015.
[3]PayPal begins piloting NFC and records 40% growth in mobile payments. NFC World; April 27, 2015.
[4]Mobile Wallets: Contactless & Remote Payments 2015-2020. Juniper Research; September 7, 2015.
[5]Mobile Payments to Explode by 2019. PYMTS.com; November 18, 2014.

Three myths about RTP

MYTH ONE RTP is only for P2P

TRUTH

- The RTP system is designed to address unmet customer needs across all customer segments (i.e., B2B, B2C, C2B, P2P, G2C, etc.).
- Consumers, businesses, and government can use RTP.
- For example RTP scenarios, refer to page 9.

MYTH TWO RTP will only be available to TCH member banks

TRUTH

- Any participating FI, irrespective of their size or charter type, will have the ability to transmit payments through the RTP system.
- FIs will have the flexibility to choose their level of participation (i.e., Receive Only, Send, Allow Request for Payment, etc.) within the RTP system.
- Technology players and third-party payment providers will have a role in the environment to provide or facilitate connectivity where necessary.
- Refer to Real-Time Payments Ecosystem on page 10.

MYTH THREE RTP is the same as Same Day ACH

TRUTH

- **Value-Added Messaging** – RTP will have the ability to enable new products and services through the use of its extensive and multifaceted messaging capabilities.
- **Availability of Funds** – The RTP system will make funds available in real-time – 24/7/365.
- **Transparency** – The RTP system will provide status updates of payment and non-payment messages in real-time.

RTP checklist

A checklist of high-level key activities which should be considered as FIs start their implementation of RTP is included below. Depending on the structure of the organization, some of these activities may be performed concurrently or in a different order. The Operations team should also coordinate with TCH, third-parties, and/or other groups within the FI to synchronize activities surrounding the implementation of RTP.

FI Operations Checklist of Key Activities for Implementing RTP			
Activity	TCH	BUS	TECH
❑ Seek direction from Business on product and customer segmentation		X	
❑ Determine operational areas that will enable a real-time product offering (i.e. Lines of Business, Information Technology, Operations, Risk Management, Regulatory Compliance, Treasury, etc.)			
❑ Develop Target Operating Model for operations teams including channels, operational processes, RTP Roadmap			
❑ Perform Current State Assessment and create RTP Roadmap			
❑ Conduct scoping and detailed planning of RTP program from an operations perspective			
❑ Assist with creation of functional requirements, design, use case scenarios, and 2D process flows			
❑ Develop testing strategy and test cases with test team	X		X
❑ Establish test window and test period for testing to be conducted	X		X
❑ Develop post-implementation and transition planning			
❑ Develop and determine training and communications plan		X	
❑ Develop and document help desk and customer service training procedures			
❑ Develop and communicate disaster recovery plan	X		
❑ Develop and document communication plans (e.g. pre go-live, go-live, and post go-live communication plan)		X	
❑ Develop implementation strategies and checklists for moving system from test environment to production environment	X		X
❑ Determine client migration and transition plan		X	X
❑ Conduct dress rehearsal and production readiness		X	X
❑ Determine detailed control procedures			
❑ Conduct go-live weekend and transition to production	X	X	X
❑ Conduct client migration / transition support		X	
❑ Document lessons learned		X	X

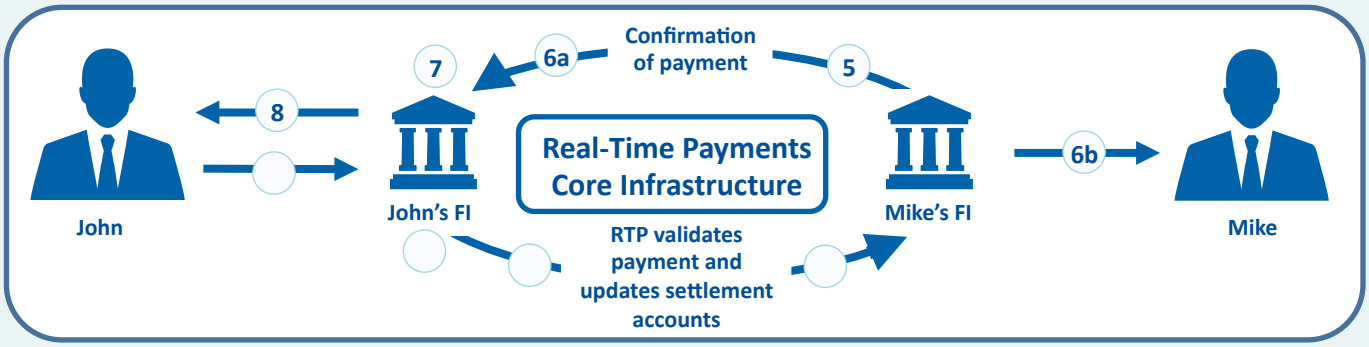
03: How do Real-Time Payments Work?

Sample P2P RTP Scenario

Real-time payments are executed through a sequence of payment messages. It starts with a payer sending a payment instruction via a channel made available by their FI (initiation). The FI ensures funds availability (approval), conducts required screening (authentication), and securely sends the payment instruction message to the RTP core infrastructure. The RTP core infrastructure validates the transaction and routes it to the receiving FI (clearing). The receiving FI acknowledges the message and immediately sends a response to the RTP core infrastructure. The RTP core infrastructure provides an acknowledgment message to the receiving FI as well as the issuing FI (receipt) and manages settlement between FIs. Upon receipt of the confirmation message, the receiving FI posts the transaction to the receiving customer's account. This provides immediate availability of funds to the recipient.

These real time payments are applicable to a variety of use case scenarios. Representative use cases are presented below.

Person-to-Person (P2P)



***Use case scenario**: Transaction from a person (John) to another person (Mike) with accounts at different FIs.*

1. John's FI carries out its normal authentication process to verify John as the account owner. John instructs his FI through Online Banking to pay Mike via RTP. He includes Mike's alias (or routing and account number) to address the payment. He may also add additional reference information so that Mike knows what the payment is for.
2. John's FI verifies the availability of funds. In certain cases, the FI may need to hold the payment to perform more extensive fraud protection checks. John's FI may also opt to perform an out of band authentication step if this payment exceeds a certain threshold.
3. John's FI resolves the alias (if used) and submits the transaction to the RTP core infrastructure. At this point, the transaction can no longer be cancelled.
4. The RTP core infrastructure validates the transaction details and provisionally updates (debits) the settlement position for the payer's FI in the amount of the transaction.
5. Once Mike's FI has received the transaction, it checks that the account number is valid and then sends a message back to the RTP core infrastructure that it has accepted (or rejected) the payment.

6a. Upon receiving the accept message from Mike's FI, the RTP core infrastructure finalizes the settlement position (debit) for the payer's FI and updates the position (credit) for the payee's FI in the amount of the transaction and sends a message to John's FI to confirm that the transaction was successful (or rejected) and sends a message to Mike's FI to confirm the transaction was successfully completed.

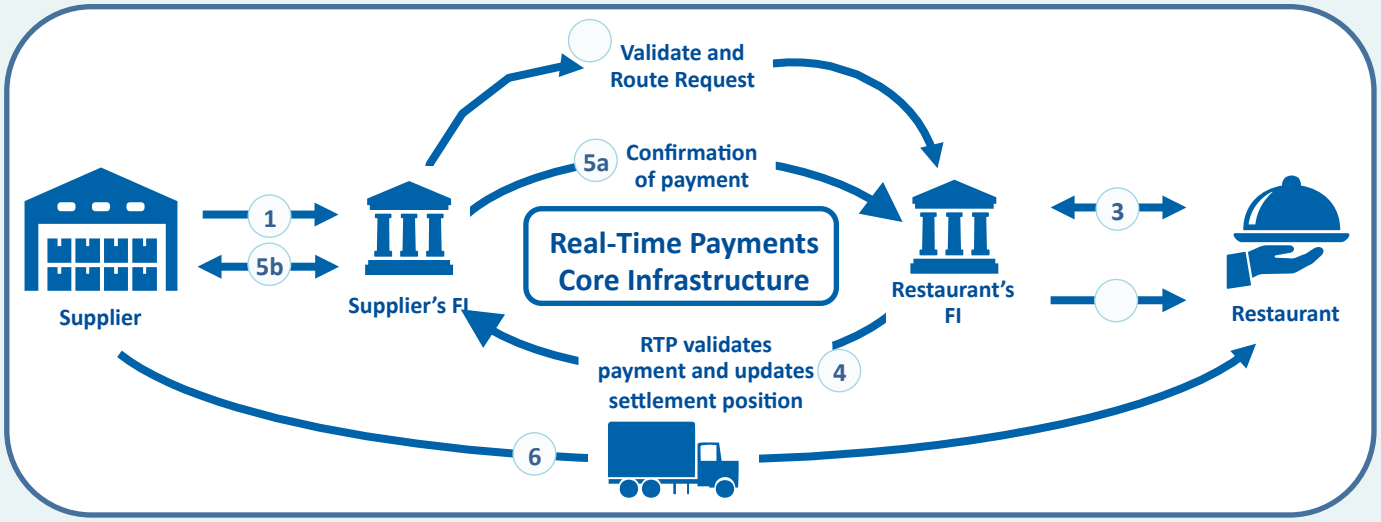
6b. Mike's FI simultaneously credits his account with the value of the transaction sent by John.

7. John's FI marks the transaction as complete.
8. FIs notify John and Mike respectively, the status of the payment. Each sending FI will decide how their customers will be notified of transaction status.

Note: Funds are accessible within seconds

Sample B2B RTP Scenario

Immediate payment systems are particularly well-suited to provide value beyond the inherent benefit of fast money movement. A fundamental feature of real-time payments is real-time communication among senders, receivers, and their FIs.



***Use case scenario**: Single business to business transaction between a restaurant and its supplier. The restaurant needs supplies immediately, and the supplier needs to be paid before shipping the goods.*

1. The supplier reviews an order received from a restaurant and sends a "Request for Payment" (RFP) through their FI. The supplier's FI sends the RFP message to the RTP core infrastructure. Sending the request through a secure, trusted channel reduces fraud risk associated with an e-mail invoice.
2. The RTP core infrastructure validates the request and routes it to the restaurant's FI, which then notifies the restaurant.
3. The restaurant receives the RFP that contains a "Pay Now" button. Upon selecting the "Pay Now" button, a pre-populated payment message that includes all pertinent payment data (e.g., remittance information, payment amount, etc.) is presented to the restaurant so they can confirm and make the payment to their supplier quickly and easily.
4. The restaurant's FI submits the transaction to the RTP core infrastructure that validates the transaction details and provisionally updates (debits) settlement position for the payer's institution in the amount of the transaction. The payment message is then sent to the supplier's FI that then confirms the account number is valid and accepts the payment.

5a. The supplier's FI sends a message to the RTP core infrastructure with acceptance of the payment and the RTP core infrastructure finalizes the settlement position (debit) for the payer and updates the position (credit) for the payee's FIs in the amount of the transaction.

5b. The supplier's FI notifies the supplier of payment. The supplier sends a payment acknowledgement message to the restaurant, confirming the goods are on the way.

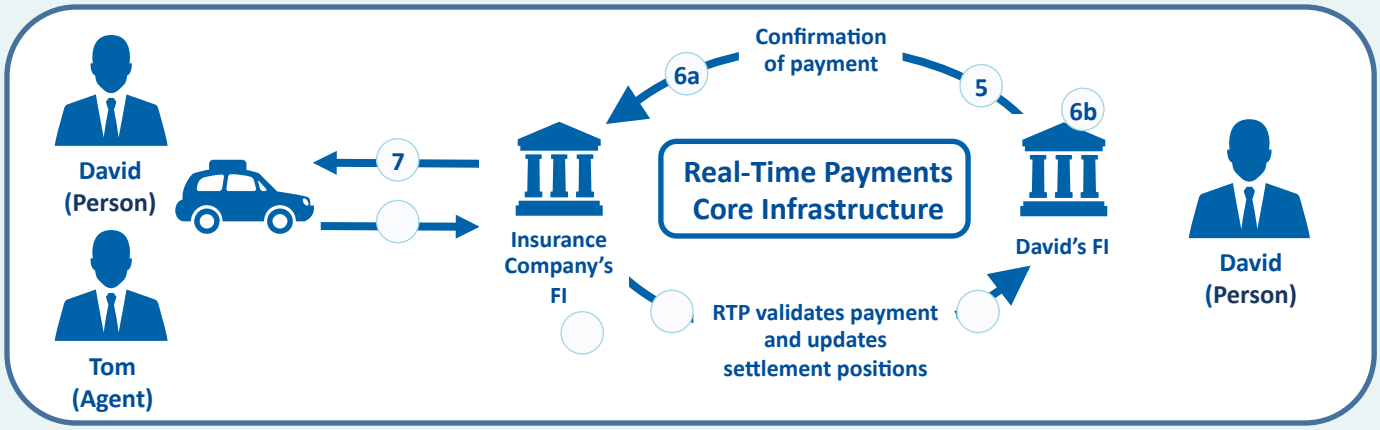
6. The supplier sends the loaded delivery truck to the restaurant, confident that payment has been made.

7. The restaurant's FI notifies the restaurant, confirming that the goods are on the way with a message arriving through a reliable, trusted channel.

Note: The exchange of information between buyer and seller goes beyond the remittance detail that typically accompanies B2B electronic payments. Remittance data is essential and enables the supplier to apply payment to the correct invoice, account for any differences, and reconcile those differences. In this immediate payment example, the payment request, notification message, and confirmation message all provide additional value for a time-sensitive transaction.

Sample B2C RTP Scenario

A business-to-consumer (B2C) transaction demonstrates that RTP offers value beyond P2P transactions. One example is the case of an insurance claims adjuster now having the ability to meet with a customer shortly after an accident or claim, assess value of damages, and provide funds immediately, thereby relieving the customer of worry in an already stressful situation.



***Use case scenario**: David has damages to his car from an accident. He calls his insurance company, which sends its local adjustor, Tom, to meet with David and view the damages. Tom inspects the claim, determines the appropriate amount for the damages, and approves it remotely. Tom's insurance company immediately sends David the settlement amount.*

- Tom instructs the insurance company's FI to pay David the approved amount of damages. The payment instruction also includes claim information that both the insurance company and David can access. (Extensive claim information could be included in a remittance advice message or through a reference to an external source).
- The insurance company's FI uses appropriate customer processes to verify Tom has authority to initiate payments from this account and that good funds are available.
- The insurance company's FI submits the payment message to the RTP core infrastructure.
- The RTP core infrastructure validates the transaction details and the payment instruction and provisionally updates (debits) the settlement position for the payer's FI. Associated claim information is then sent to David's FI as a part of the payment message.

5 Once David's FI has received the transaction, it checks that the account number is valid and then sends a message back to the RTP core infrastructure that it has accepted (or rejected) the payment.

6a The RTP core infrastructure sends a message to the insurance company's FI and David's FI to let them know that the transaction has been made successfully. The insurance company's FI marks the transaction as complete.

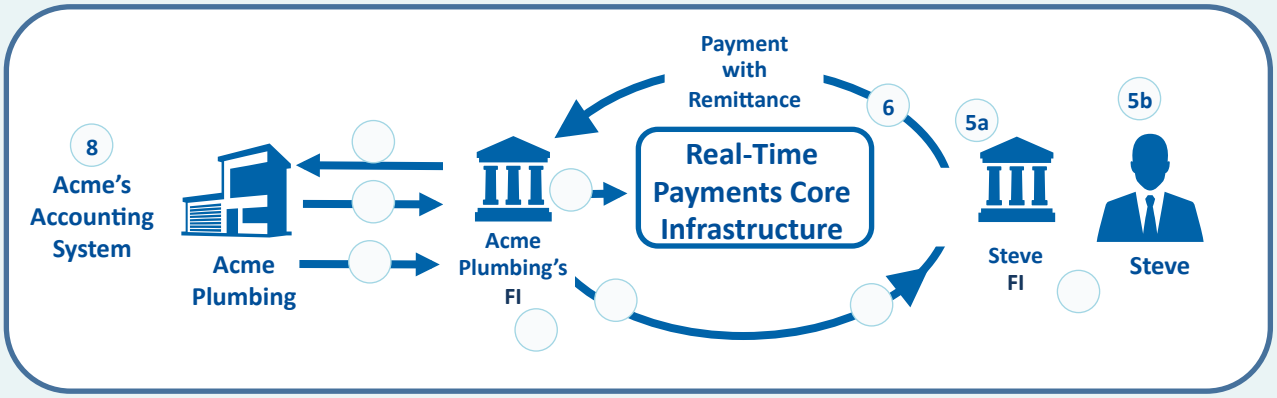
6b David's FI simultaneously credits his account with the claim amount sent by the insurance company so he can have immediate access to the funds.

7 The insurance company's FI confirms the status of the payment and provides transaction details to the insurance company. Each sending FI will decide how their customers will be notified of transaction status

Note: The exchange of information between buyer and seller goes beyond the remittance detail that typically accompanies B2C electronic payments. Remittance data is essential and enables the supplier to apply payment to the correct invoice, account for any differences, and reconcile those differences. In this immediate payment example, the payment request, notification message, and confirmation message all provide additional value for a time-sensitive transaction.

Sample C2B RTP Scenario

A consumer-to-business (C2B) transaction demonstrates that RTP offers many features beyond traditional money movement. One example is a small business that wants to send electronic invoices to its customers, along with the ability for customers to view and respond immediately with payment. The small business wants to have the payment and remittance data instantly downloaded to its accounting software program to avoid manually entering payment remittances, which can take time and introduce errors.



Use case scenario: *Consumer to Business scenario with request for payment. Steve, an Acme customer, is presented with a link from his FI's customer facing application that displays an invoice. An option to immediately pay all or a portion of the invoice is made available. Once Steve instructs his FI to pay, his FI sends the payment directly to Acme's checking account while Acme's FI routes the remittance information directly to Acme's accounting system.*

- Acme Plumbing creates an invoice to be presented to Steve, their customer, for payment. Acme's accounting system creates a file containing a link to the invoice, (including remittance info) and a Request for Payment for its customers.
- Acme's FI uses appropriate customer authentication and payment verification processes to verify Acme's Accounting personnel has authority to make payment requests.
- Acme's FI submits the Request for Payment (RFP) messages to the RTP core infrastructure.
- The RTP core infrastructure validates the payment request and routes the message to Steve's FI for distribution to the customer.

5a Once Steve's FI has received the payment request, it validates that Steve has elected to receive RFPs. Steve's FI then posts the message to his account.

5b Steve is presented with a RFP that has a "Pay Now" button. Upon selecting the "Pay Now" button, Steve is presented with a pre-populated payment message including all pertinent data (i.e., remittance information, payment amount, etc.).

6 Once the payment is authorized and submitted, Steve's FI sends the payment message including the related remittance information and a reference ID to the RFP to Acme's FI via RTP. RTP core infrastructure processes the payment as it would any other payment on the System.

7 Acme's FI informs Acme Plumbing that the customer's payment, and related remittance data, has been received and funds are available in Acme's account.

8 Acme Plumbing receives remittance information into their accounting system via their FI's interface, avoiding manual entry of payment information, and applies payment to the appropriate customer account.

9 Acme send confirmation that payment has been posted to Steve via a Payment Acknowledgement message through RTP

Note: The exchange of information between buyer and seller goes beyond the remittance detail that typically accompanies C2B electronic payments. Remittance data is essential and enables the supplier to apply payment to the correct invoice, account for any differences, and reconcile those differences. In this immediate payment example, the payment request, notification message, and confirmation message all provide additional value for a time-sensitive transaction.

04: Business Case Considerations

The RTP business case should be a collaborative effort with input and knowledge coming from the business, operations, and technology teams. This partnership is essential to building the business case for RTP as FIs analyze the current operating model that is supporting the products within the bank. The knowledge gathered by the Operations teams through their experience with the client, understanding of their organization's products and services, and processes that drive the FI's business makes their participation integral to developing a well-rounded and intelligent business case for RTP.

- **Client Needs and Expectations:** By assessing client needs and leveraging their knowledge of the client, Operations teams can combine their day-to-day experience with the business case to determine areas where there are opportunities to better serve or meet the needs and expectations of the client.
- **Products and Services:** The Operations team has an understanding of not only the organization's products and services, but also the customer's level of acceptance of its products. This unique view into the organization's functions will help strengthen the case for how the FI can leverage RTP to support an FI's existing product and service portfolio.
- **Operating Models and Processes**: The Operations team should assess existing operating models to identify any changes that may be needed to support RTP. This assessment should include an evaluation of resources that may be needed for 24/7 coverage or who have knowledge or skillset around a specific topic (e.g. ISO 20022). This assessment will help the Operations team understand the ways that RTP can drive value for the organization. This review can also provide an understanding of the operational costs associated with implementing RTP.

Optimizing the organization for client needs and aligning it against the internal business case for implementing the RTP model contributes to the cost analysis that supports the business case. The Operations team can provide additional value by assessing the various opportunities for implementing RTP and determining where the organization can drive the most value.

Business Case Considerations for RTP

New Product Ideation
Consider opportunities for new products and markets created by faster payments to deliver innovative products that transform the industry and drive adoption of RTP.

Impacted Products and Service Offerings
Assess customer needs alongside existing product and service offerings to determine the foundation for your organization's RTP strategy.

Competitive Opportunities
Understand competitive opportunities across use cases. Develop your own value-added products and pricing strategies that align with your customers' demand.

Impacted Investments and Associated Costs
Determine investment areas and associated costs to understand the overall cost and impact to your organization.

RTP Technology Overview

RTP operates 24 hours per day, every day of the year. To ensure availability, RTP runs "Active/Active" in both sites. Participants are required to maintain two sites, but may choose to run active/active or active/standby.

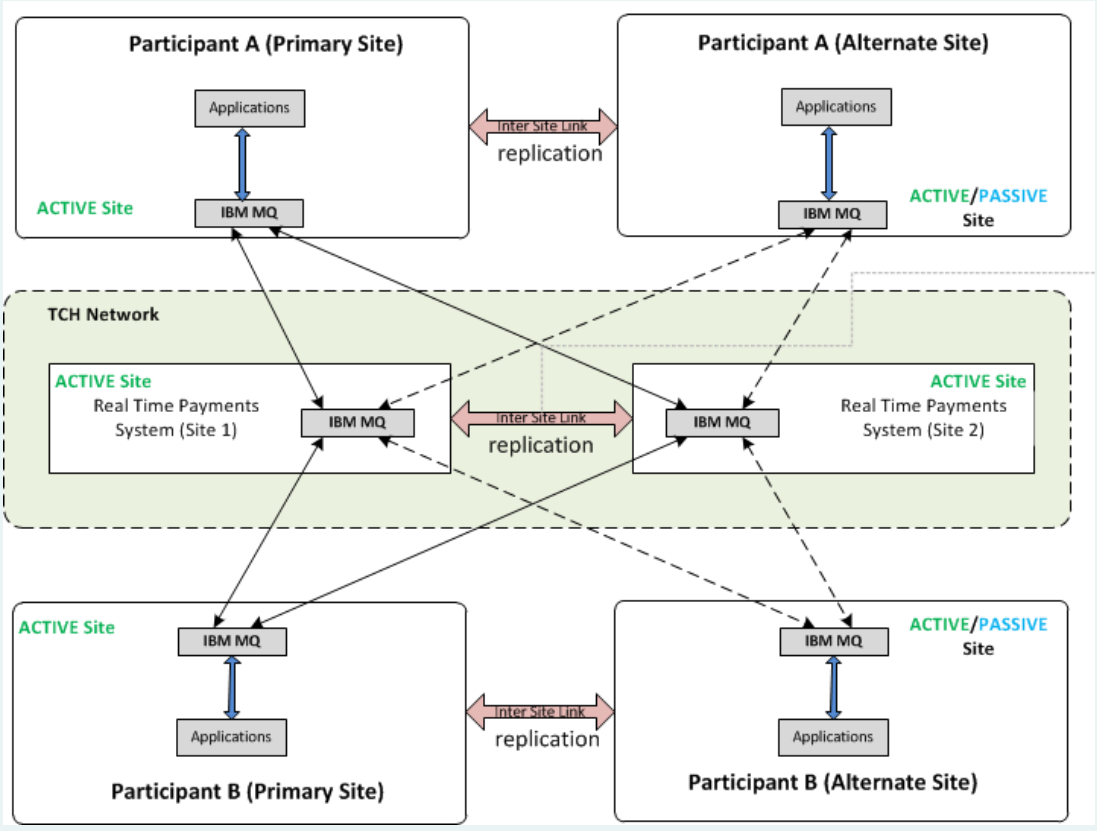
At its most basic level, the RTP system allows for the exchange of messages related to a payment event between two participants. Each message submitted to RTP receives a response within seconds. The real-time response indicates that the message has been received and has been processed by the receiving financial institution. Subsequent business-level responses (such as the Response to Request for Payment) must be submitted as new requests and will receive real-time responses.

Message transport for RTP is via IBM Message Queue (MQ). The interface employs an Outbound Queue Pair, an Inbound, Queue Pair, and a System Notification Message Queue. Queue naming conventions are defined in detail in the TCH Customer Documentation RTP System Interface Guide.

Network Connectivity is via MPLS or Secure VPN, and connectivity options are outlined in the *TCH RTP Network Connectivity Overview* document available upon request.

In addition to the security provided by the MPLS or Secure VPN connection, MQ Transport Layer Security (TLS) is utilized, and each message is digitally signed to ensure authenticity in accordance with ISO20022. RTP adheres to the latest FFIEC guidelines and Federal Information Processing Standards (FIPS-2).

A management portal will be provided to allow bank operations users to view transaction status, message volumes, liquidity positions, and manage reports. Participants will have the ability to administer users and permissions for their institution and will also be able to configure certain processing parameters such as the high-watermark and low-watermark thresholds. Users can also request a withdrawal of excess liquidity from the prefunded settlement account.



Key Technology Considerations

RTP is a new system that is unique from any other existing payment system in the U.S. today. Technology teams responsible for bank implementation of RTP will need to take certain attributes of the system into consideration when designing the system integrations that will make up a financial institution's implementation of RTP. TCH has identified five important considerations that technology teams must understand when considering an RTP implementation.

Five important considerations for Information Technology teams	
❑ 24/7/365	❑ Routing Table Management
❑ Message Processing SLAs	❑ Customer Notifications
❑ Network Infrastructure	

Topic 1: 24/7/365

Systems connected to RTP must be available to facilitate immediate funds availability for transactions received at any time of day, any day of the year. While some financial institutions have invested in real-time core account processing systems, the majority of financial institutions use core account processing systems that rely on batch processing. Those relying on batch processing must determine how "immediate funds availability" will be achieved technically.

Further, 24/7/365 nature of RTP may have an impact on planned maintenance to systems that interact with RTP. Given that there is no "green zone" for changes, while applications that are typically used in processing RTP transactions are down for maintenance, participants will need to determine how they will respond to incoming request messages.

Finally, in a 24/7/365 system these is no "start of day" or "end of day" process. TCH will provide intraday reconciliation points to help participants in ensuring that their transaction records match what is in the RTP system, but RTP does not have a beginning or end of day. Further, there is no "value date" on payments, but RTP validates to ensure that the message date is within 1 calendar day of the RTP System Time.

Important

Maintenance windows are essential for completing important security updates, replacing or updating hardware or software, and even daily for posting transactions. Given a payments system that operates 24/7/365 with "five-nines" uptime, an FI must consider what will happen when systems that typically receive messages from the system are down for scheduled maintenance.

- What will be the impact on users trying to send payment?
- What will be the impact on account holders who receive payments during an outage or maintenance window?
- Do maintenance windows align with low volume times for RTP activity to ensure that customer impact is minimized?

Key Technology Considerations (Continued)

Topic 2: Message Processing

RTP governance establishes Service Level Agreements (SLAs) that participants must meet regarding average response time to incoming requests. Generally, payment requests must complete within 15 seconds of initiation. Participants receiving messages must accept or reject the payment within five (5) seconds. These five seconds must include:

- Schema validation and Verification of the message signature
- Business validation (account exists, transaction type permitted for account, regulatory checks, etc.)
- Creation, signature, and transmission of response (accept/reject/accept without posting)

All outgoing messages must be digitally signed in accordance with algorithms specified by world wide web consortium (www.w3.org). Like wise, signatures must be validated on incoming messages. Details of how to sign messages are provided in the RTP Interface Guide (see resources section). Libraries of standard functions used to sign messages and validate signatures are available for most computer languages. However, depending on the volume of transactions expected, technology teams may want to consider the use of hardware security modules (HSMs) to perform cryptographic functions in order to ensure messages can be processed within SLAs.

RTP will automatically time out and cancel a transaction if the receiving participants does not respond in time. If a timeout occurs, RTP will notify both the sending and receiving participants that the transaction has been cancelled. The sending participant should also take action if no response is received within 15 seconds. If no response is received from RTP within 15 seconds, it is likely that an issue exists between the sender and RTP, and the sender may attempt to resend the transaction as a possible duplicate, or may indicate to their customer that the transaction could not be completed at this time. Please refer to the most recent version of the *RTP Customer Documentation System Message Flows* document to ensure proper use of the possible duplicate flag on various message types.

Resource

The *RTP Customer Documentation System Message Flows* outline the standard flows and use cases that a participant can expect for each of the supported message types in RTP. This document also includes a section describing RTP settlement, the required minimum prefunded balance, supplemental funding, and withdrawals from the settlement account.

In addition to technical resources, product managers may also find this resource helpful in planning features and functionality that must be included in the business requirements for any RTP integration project.

Topic 3: Network Infrastructure

Participants with an existing MPLS network connection to TCH may be able to use their existing communications circuits and infrastructure to connect to RTP, but changes in volume and required up-time may necessitate upgraded circuits and routers.

In establishing network infrastructure requirements, each participant must be able to accommodate the 24/7/365 availability requirements of RTP as well as the expected volume of all message types, including payments, payment related messages, extended remittance messages, and administrative messages. Infrastructure planning should take into account the ISO 20022 message types and expected volumes for each institution. Note that multiple messages may be associated with each transaction (for example, a Credit Transfer [pacs.008] may be generated in response to a Request for Payment [pain.013]).

Important

Infrastructure planning should take into account not just expected payment volume, but also overall message volume. Within RTP, payment-related messages like Request for Payment, Request for Information, Payment Acknowledgement, and Stand-Alone Remittance Advice will contribute significant message volume.

Decision Point

Participants with existing network connections to TCH must determine if those connections can be reused, or if dedicated RTP circuits are required.

Key Technology Considerations (Continued)

Topic 4: Routing Table Management

Message routing within RTP is based on R/T number and account number. To ensure that each participant is aware of each other participant in the network at sign-on and throughout each day, RTP will periodically publish a Routing Table and will send System Notification Messages indicating a change in status to other participants. The Routing Table is based on R/T number and includes information such as each R/T number's associated Participant ID, Financial Institution ID, Connection ID, and Receive Messages Supported.

It is recommended that each RTP Participant maintain a local version of the most current RTP Routing Table. TCH will make the current table available through the management portal for Participant and TPSP download; however, once downloaded, Participants should update their local copy when System Notification Messages are received indicating that other participants have:

- Signed-on or Signed-off;
- Become Connected or Disconnected; and
- Become Suspended or Reinstated by RTP.

Participants should avoid sending messages to R/T numbers that are unavailable through RTP as fees may be charged for these messages which will ultimately fail and provide no value to the sending participant.

Important

Participants are responsible for managing their own local routing tables, and therefore, they have options when it comes to how this table is managed. If a participant opts not to maintain and update their local version of the routing file using the System Notification Messages that broadcast participant status, they may experience more rejected messages as they submit transactions to routing and transit numbers that are not available. This may result in an increase in network fees for transactions that are unsuccessful.

Topic 5: Customer Notifications

RTP requires that information regarding payment status be made immediately available to the account holder through electronic means. This means that the status of each payment and payment-related message will need to be electronically communicated to account holders through available channels.

Account holders will have varying means through which they are able to receive notifications. Some account holders have access to online and mobile banking, while others only have access to online banking. Each participant will need to decide how these notifications are delivered to account holders and what options they will give account holders to update the settings for these notifications.

Integration with multiple applications may be necessary to achieve the notifications requirements determined by each participant's product management team.

Message Types

RTP supports a number of ISO 20022 message types that are used for a variety of purposes throughout the payment lifecycle. The RTP message set is designed to facilitate a number of payment use cases. Messages supported within RTP include:

- **Credit Transfer (pacs.008):** This basic multi-purpose payment message is used to push funds to an account designated by the sender. The credit transfer is the only financial transaction within the RTP message set, meaning that it is the only message that results in settlement. All funds associated with RTP credit transfers must be made immediately available to the Creditor and information related to the status of the credit transfer must be made immediately available to the Debtor.

- **Request for Payment (pain.013) & Response to RFP (pain.014):** The Request for Payment (RFP) is initiated by a Creditor to request funds be sent related to a debt owed by the debtor. Information related to the Request for Payment must be made immediately available via secure electronic means to the Debtor. Upon receive of the Request for Payment, the Debtor may initiate a Credit Transfer (pacs.008) in response or may decline to make a payment, in which case a Response to RFP (pain.014) is sent to the Debtor FI. The Credit Transfer that follows a Request for Payment includes a reference to the original RFP to allow for straight-through processing and simple reconciliation for the Creditor that initiated the RFP.

- **Payment Acknowledgement (camt.035):** The Payment Acknowledgement message is sent by a Creditor to a Debtor to confirm that funds sent in a previous Credit Transfer (pacs.008) have been received and applied to an account. This is especially useful for billers that must apply funds associated with a Credit Transfer to a specific account through their accounts payable system.

- **Request for Information (camt.026) and Response to RFI (camt.028)**: The Request for Information (RFI) is initiated by a Creditor to request additional or missing information regarding a previously received Credit Transfer (pacs.008). For example, if a Credit Transfer is received by the Creditor FI and applied to the Creditor's account, but the Credit Transfer did not include the invoice number against which the funds were to be applied, the Creditor has a means to request this information through the payment system. Upon receipt of a Request for Information, the Receiving FI must immediately make information related to the Request available to its account holder through secure electronic means. Should the Debtor respond with the missing information or decline to respond with the requested information, a Response to RFI (camt.028) is sent back to the Creditor FI including the missing information or a reason that indicates why such information cannot be provided.

- **Stand-Alone Remittance Advice (remt.001):** The Stand-Alone Remittance Advice message provides extensive remittance detail that cannot be included in the Credit Transfer message or the Request for Payment message. This message, which must be sent in reference to a Credit Transfer or Request for Payment, allows for up to 4,000 characters of remittance or invoice information.

Resource

The *RTP Message Specifications* describe in detail the structure, format, contents of each message supported in RTP. For the message types listed above refer to the following specifications:

- *RTP Credit Transfer Message Specification*
- *RTP Request for Payment Message Specification*
- *RTP Payment Acknowledgement Message Specification*
- *RTP Request for Information Message Specification*
- *RTP Stand-Alone Remittance Advice Message Specification*

Message Types (Continued)

RTP supports a number of ISO 20022 message types that are used for a variety of purposes throughout the payment lifecycle. The RTP message set is designed to facilitate a number of payment use cases. Messages supported within RTP include:

- **Request for Return of Funds (camt.056) and Response to RfRF (camt.029):** The Request for Return of Funds (RfRF) can be initiated by a Debtor FI if a Debtor reports a Credit Transfer was sent either fraudulently or in error. Upon receipt of a RfRF, the Creditor FI must initiate an investigation into the error and determine if funds associated with the original Credit Transfer can be returned to the Debtor. Upon completion of the investigation, the Creditor FI may respond with a Response to RfRF (camt.029) indicating whether or not funds will be returned to the Debtor. If funds are to be returned, the Creditor FI can do so through any means, including use of an RTP Credit Transfer (pacs.008).

- **Message Status Report (pacs.002):** The Message Status Report is the standard confirmation message that is sent in real-time by the Receiving Participant in response to all message types described above. This Status Report confirms that the message has been received by the Receiving Participant and indicates if the message could be successfully processed. If a message could not be successfully processed, the Message Status Report would include indication that the Receiving Participant is rejecting the message and the reason for the rejection. All request messages and their respective response messages must be responded to in real-time with a Message Status Report.

In addition to the message types listed above, Administrative messages are sent between Participants and the System for various purposes including sign-on, sign-off, echoes, and individual and broadcast system notifications. For more information regarding individual messages or standard message flows, please request access to the RTP Message Specifications and System Message Flows documents.

Finally, each message is sent with a Business Application Header which contains routing information used by TCH and a unique identifier for each end-point to end-point message leg. More information regarding the function of the Business Application Header can be found in the *Business Application Header Message Specification*.

Resource

The *RTP Message Specifications* describe in detail the structure, format, contents of each message supported in RTP. For the message types listed above refer to the following specifications:

- *RTP System Time-Out and Request for Return of Funds Message Specification*
- *RTP Message Status Report Message Specification*
- *RTP Administrative Messages Specification*

In addition to these specifications, more information regarding the Business Application Header can be found in the *RTP Business Application Header Message Specification*.

Integration Checklists

The implementation of RTP will likely impact a new participant's existing systems and applications. Since data related to inbound RTP messages may need to be fed to multiple systems, impact to the following systems should be analyzed to determine the scope of work related to RFP implementation. It is also important to consider the message types that will be supported as a result of your institution's level of participation (e.g. Receive Only, Send and Receive, Send Request for Payment).

- ❑ **Core Account Processing System** – used to post transactions (Credit Transfer) to accounts, for generation of statements including RTP activity, and movement of funds between accounts at the FI (GL Accounts and End-user accounts)
- ❑ **Network Infrastructure** – infrastructure will be needed to establish 24/7 connectivity to RTP to send and receive messages
- ❑ **Online Banking** – channel through which RTP Credit Transfer, Request for Payment, Request for Information, and Payment Acknowledgement activity may be made available to account holders.
- ❑ **Mobile Banking** – channel through which RFP Credit Transfer, Request for Payment, Payment Acknowledgement, and Request for Information activity may be made available to account holders.
- ❑ **Enterprise Alerts System** – system used to alert account holders of specific events in a manner agreed to by the account holder (for example, text, email, or mobile alerts)
- ❑ **Fraud Monitoring and AML Systems** – systems designed to detect and respond to suspected fraud or Anti-Money Laundering violations. These systems must have the ability to screen RTP activity in real-time. Fraudulent transactions reported by account holders must be reported to TCH in a timely manner as well.
- ❑ **OFAC Screening Tools** – these systems typically check account holder profiles for OFAC violations during new customer account creation and upon an account holder instructing the FI to send an international transaction. To the extent that RTP is used to move funds between accounts within the US and accounts of foreign affiliates of U.S. financial institutions, OFAC screening may need to be performed in real-time at the discretion of the financial institution.
- ❑ **Payments Hub / Payments Gateway** – centralized system used to process and manage the workflow for all payments going into and out of an institution.

Additionally, any applications through which account holders will have the ability to send Credit Transfers or Requests for Payment will be impacted by the RTP implementation. Examples could include:

- ❑ **Online Bill Pay**
- ❑ **Person to Person Payments**
- ❑ **External Account to Account Transfers**
- ❑ **Digital Invoicing**
- ❑ **Cash Concentration products**
- ❑ **Accounts Receivable products**
- ❑ **Accounts Payable products**

06: Operations Checklist

Below is a checklist organized by groups within a typical FI's organization that serves as a quick reference for some of the considerations listed throughout this document. This list is not intended to be inclusive of all considerations that must be made when implementing RTP, but it can help spur conversation about RTP impacts throughout an FI's operations.

Risk, Fraud, and Compliance

- ❑ How do Reg E consumer disclosures need to be updated to include RTP payments? What should the posting order of RTP transactions be relative to other transaction types (e.g. ACH, checks, card payments, wires)?
- ❑ How do account agreements with business customers need to be updated?
- ❑ How will the institution ensure compliance with all aspects of BSA for RTP transactions, including screening for potential OFAC violations as necessary?
- ❑ Do existing AML controls need to be updated given the implementation of RTP?
- ❑ How will the institution implement real-time fraud monitoring for RTP transactions?
- ❑ If sending transactions, what dollar limits will be implemented for retail customers? What dollar limits will be implemented for commercial and wholesale customers?
- ❑ What additional training will be necessary for fraud and OFAC analysts regarding RTP?
- ❑ What authentication methods are used prior to allowing an account holder to send an RTP payment?
- ❑ What due diligence process will be necessary to ensure that customers initiating Request for Payment messages are credible and using such transactions for a valid business purpose?
- ❑ What due diligence process will be necessary to allow payment service providers to access RTP services through our institution?

Payment Operations

- ❑ As a default, all account holders should be eligible to receive RTP. Should you allow your account holders to opt out of receiving RTP? If so, how will this process be managed, and how will the system prevent acceptance of payments for accounts that are opted-out?
- ❑ What end-of-day reconciliation processes need to be established?
- ❑ Will account holders be required to enroll to receive Requests for Payments? If so, what does this enrollment process look like? How will the FI track requests tor enrollment and opt-outs for RFPs?
- ❑ What will be the process for investigating a Request for Return of Funds received from another institution? Can this process be automated?
- ❑ What will the process be for account holders to initiate a Request for Return of Funds? To what extent can this be automated?
- ❑ What monitoring will be necessary to ensure that RTP SLAs regarding response times are consistently met? What additional monitoring will be necessary to ensure other performance metrics (% positive responses, % timeouts) will be met?
- ❑ How will customers initiating RFP messages be monitored to ensure proper use?

06: Operations Checklist (continued)

Product Management

- ❑ What will use of non-payment message—such as Request for Payment, Remittance Advice, and others—be incorporated into existing and new products?
- ❑ What level of participation is necessary to support products that will be integrated with or developed to leverage RTP? How will that level of participation impact Operations?
- ❑ Is the use of a directory service necessary for the products that will be offered? How will aliases be resolved and managed outside of RTP?

Customer Service and Communications

- ❑ What training will be given to call center and in-branch employees so that they will be able to speak generally about RTP and its impacts on customers?
- ❑ Will a specialized call center team be established to answer account holder questions related to RTP? If so, will customers be given a specific number to call for RTP-related questions?
- ❑ What additional personnel will be necessary to support RTP?

Treasury Management and Deposit Operations

- ❑ How will supplemental funding and drawdowns of the settlement account be supported operationally?
- ❑ How will treasury management prepare for weekends and holidays to ensure a sufficient balance is maintained in the settlement account until the next opportunity to provide supplemental funding?
- ❑ What is the process for monitoring the balance of the settlement account, especially upon RTP system notifications regarding the Low Watermark and High Watermark levels configured by the FI?
- ❑ What is the preferred reconciliation/reporting time, if TCH is offering multiple reconciliation windows per day?
- ❑ What process will be defined to respond to discrepancies identified through reconciliation?

Technology

- ❑ Will the FI connect directly to TCH or through a third-party service provider (TPSP)?
- ❑ If using third-party vendors for products and services that are already implemented but that are being integrated with RTP, what party will manage the technical connection and how will the integration be accomplished?
- ❑ How will the technology team respond to notifications of connection and/or timeout issues?
- ❑ How will the FI manage and monitor multiple connections, if necessary?
- ❑ If using a third-party service Provider (TPSP), how will the technology team ensure the vendor is notifying them of any outage or technical issues disrupting service to the FI's account holders?

Operating Rules

Network documentation will be published to provide the structure and on-going routines to ensure the effectiveness and integrity of the Real-Time Payments System. Operating rules will be established to ensure timely, secure, and accurate payments, messaging and settlement. Various attributes and schedules will be defined that participating FIs must be aware of such as due diligence requirements, settlement windows, and performance SLAs. These may change over time, but all changes will be well communicated. The general framework for the operating rules for TCH's RTP System is outlined below.

RTP Requirements	Operating Rules and Procedures	FI Requirements
All payments are originated by the payer	• A legal basis must be provided for credit transfers that are authorized by a payer • Rights and obligations of all parties to the transaction must be defined- including the payer, the payee, the sending FI, the receiving FI, and the payment system operator	• Customers must be provided with products and services to send and receive credit transfers
FI customers have the ability to send or receive payments 24 hours a day, 7 days a week, 365 days a year	• FIs must be able to receive and respond to payments and non-payment messages 24/7/365 within an established SLA	• 24/7/365 as a receiving FI • FIs must have the ability to perform necessary risk management and compliance functions such as customer authentication, authorization, regulatory compliance screening, and anti-fraud screening 24/7/365 in an automated fashion
Senders and receivers will have complete, timely information about the status of RTP	• Receiving FIs must accept or reject the majority of payments within seconds and all payments in a reasonable time • FIs must make immediate notification of payment status to senders and receivers or provide a channel for senders and receivers to view payment status	• FIs must integrate accurate RTP status inquiry, notification, and feedback into online and mobile banking services
Receiving FIs will provide immediate availability of funds to recipients 24/7/365	• Receiving FIs must make funds available to receivers within seconds for any accepted payment • Payments can be rejected for risk management, inability to post, or legal compliance • Payments may be held for review for a reasonable time only when necessary for risk management and legal compliance purposes (expected to be a small percentage of payments in the ordinary course of business). After review, FIs must accept or reject payments- not withhold availability	• Receiving FIs must either post or memo post funds for payments received immediately • Receiving FIs must be able to either accept or reject most payments automatically without manual review 24/7/365
Real-time exchange of financial and non-financial messages that support a variety of use cases	• Sending FIs must adhere to standard formats and usage rules for payment and non-payment messages • Receiving FIs must make all relevant information from payment and non-payment messages available to receivers • Receiving FIs must act on administrative messages	• FIs must develop products, services, and processes to create, deliver, and respond to payment, non-payment, and administrative messages

Operating Rules (Continued)

RTP Requirements	Operating Rules and Procedures	FI Requirements
System wide limits on transaction value, updated periodically based on objective criteria	• Limits on the value of transactions cleared through the payment system will be established by the RTP System • RTP System rules may include a process for revising the transaction value limit • Sending FIs may set lower value limits for their customers • Receiving FIs may not set a transaction limit lower than the system wide limit • An initial transaction limit will be established for the RTP system with the intention to review and raise the limit over time	• Policies and procedures must be available for a sending FI to set their transaction value limit and have it apply to payment origination • Risk management policies and procedures must be available to accept payments up to the system wide transaction value limit • FIs must have the ability to identify the potential structuring of transactions made to avoid established transaction limits
Funds cannot be taken back from the receiver; payer can request return of payment made in error	• The legal basis for payment finality will be established by the RTP System • The RTP System will not provide a basis for sending FIs to reclaim funds from receiving FIs for unauthorized payments (the sending FI only has obligation to verify payment authorization)	• FIs must have effective processes and technology to prevent unauthorized payment origination • Sending FIs must have policies and procedures in place for handling customer claims for unauthorized transfers and funds sent in error • Receiving FIs must have policies and procedures to respond to requests to reclaim funds sent in error
An inter-FI process including electronic messaging to support Requests for Return of Funds sent in error	• A process for senders to request return of payments sent in error must be established by each FI • An inter-FI process for handling Requests for Return of Payments sent in error will be established by each sending FI • Timely responses for Response to Request for Return of Funds will be requested.	• FIs must have products and services with features that prevent errors in sending payments • Sending FIs must establish policies and procedures for handling customer Requests for Return of Funds sent in error • Receiving FIs must establish policies and procedures for responding to requests to reclaim funds sent in error
Settlement process and legal framework that reduces or eliminates potential for settlement failure	• The RTP System must have rules that establish the legal basis for inter-FI net settlement and settlement procedures	• FIs must have the capability to monitor, manage, and fund their settlement pool or net settlement across all settlement windows • FIs must develop a process to respond to situations where settlement exposure has reached its limit
Use of a unique code in lieu of an account number that cannot be used to debit the account (token)	• The Secure Digital Payments company is developing an approach for tokenizing account numbers.	• FIs must create and operate their own Token Vault, outsource their tokenization process to a Token Service Provider, or leverage TCH's token services • FIs must integrate tokenization into products and services • FIs must have the ability to educate customers on tokenization

Operating Rules (Continued)

RTP Requirements	Operating Rules and Procedures	FI Requirements
Senders can initiate payment using an alias for the receiver such as a telephone number or e-mail address (Alias)	• RTP system should establish alias registration, maintenance, and routing policies and procedures	• FIs should support alias routing in payment products and services • FIs should administer alias enrollment and maintenance for customers
Participating FIs must meet minimum levels of standards for security and privacy protection	• RTP system rules should reference external security and privacy standards • All FIs must meet data protection standards • Sending FIs must meet rigorous standards for sender authentication and payment authorization • FIs should ensure their compliance with security and privacy standards are auditable and audited • An FI's security standards should not unnecessarily restrict usability	• Most security and data protection requirements should apply across all channels and products and not to a specific payment system
Support for anti-fraud, anti-money laundering, and OFAC / sanctions compliance processes	• Sending FIs should have rules that require them to provide the necessary data for regulatory compliance needed by the receiving FI	• FIs should have policies and procedures to obtain data required for regulatory compliance during the payment initiation process • Automated anti-fraud screening may be required to meet expectations to accept or reject payments in seconds or minutes
Use global message standards and define processes consistent with global practices	• RTP system should avoid unnecessary divergence from operating rules for payments systems in other countries • RTP System should develop rules to govern international payments for the long term	• FIs should adapt products and services to use international standard payment formats and processes

Tiered approach to fraud prevention and mitigation segmented by activity-based system participation	• RTP should ensure the minimum requirements for risk control are associated with the activities that a financial institution is offering and will be additive in nature for each increasing level of potential risk
	• RTP System to create a centralized utility that analyzes network-level data to identify and report potential fraudulent behavior (e.g., detect anomalous send/receive activity; excessive complaints)
	  ○ Velocity checks on origination, receive, and request for payment volumes
	  ○ Detection of patterns that indicate potential networked fraud or money mule activity
	  ○ Alerts with reason codes upon detection of anomalous activity for impacted financial institutions
		All participants must comply with FFIEC guidelines as applied through prudential regulator examination
		• All participants must report fraudulent behavior to TCH and/or sending FIs (note: this could be facilitated through TCH offering)
		• All participants must react to alerts from centralized activity monitoring utility
		• Sending FIs must establish a minimum of two factor authentication (as defined through RTP governance process)
		• Sending FIs must require registration of customers sending payments
		• Sending FIs must screen for fraud and risk in real-time for payments being originated (continued)

Operating Rules (Continued)

RTP Requirements	Operating Rules and Procedures	FI Requirements
Tiered approach to fraud prevention and mitigation segmented by activity-based system participation (continued)	• RTP will ensure the minimum requirements for risk control will be associated with the activities that a financial institution is offering and will be additive in nature for each increasing level of potential risk • FI needs to create a centralized utility that analyzes network-level data to identify and report potential fraudulent behavior (e.g., detect anomalous send/receive activity, excessive complaints) ○ Velocity checks on origination, receive, and request for payment volumes ○ Detection of patterns that indicate potential networked fraud or money mule activity ○ Alerts with reason codes upon detection of anomalous activity for impacted financial institutions	**Request for payment participants** (above requirements plus) • Make warranties and representations that Requests for Payment are for legitimate purposes • Screen and monitor request for payment initiators, with the ability to identify abusive or fraudulent use and take corrective actions including suspension of initiator access to the network (as defined through RTP governance process) • Respond to network reports of abuse of Request for Payment **Originated by third-party payment service participants** (above requirements plus) • Make warranties and representations that third-party is abiding by rules for payment origination • Apply same requirements to third-party payment services that are applied to FIs that send RTP and allow requests for payment (as applicable) • Follow FFIEC guidelines regarding third-party relationships • Allow network to enforce rules against FIs and third-parties by allowing network to levy fines and suspend activity on the network • Prohibit third-parties from originating volume greater than their financial resources can support in the case of third-party failure

Network Documentation

The table below identifies important documentation for technology teams to read as they prepare for an RTP implementation. These documents include important details regarding the RTP Interface, RTP Messages, and standard message flows that are imperative to understanding how the system operates. Access to these documents can be granted upon request. Please see the "Contact Us" section to request access to the documentation below.

Document Name	Purpose
TCH Customer Documentation RTP System Message Flows	Describes all RTP message types and outlines standard flows for each message. Includes diagrams of standard flows.
RTP Customer Documentation System Interface Guide	Describes the application interface to RTP including technical details and considerations for interface development.
RTP Network Connectivity Overview	Provides a high-level overview of the network connectivity options available to facilitate the exchange of data between TCH and its customers and how the RTP portal is accessed.
RTP Business Application Header Specification	Describes the structure, format, contents and usage of the Business Application Header in detail.
RTP Credit Transfer Message Specification	Describes the structure, format, and content of the Credit Transfer message (pacs.008) in detail.
RTP Message Status Report Specification	Describes the structure, format, and content of the Message Status Report (pacs.002) in detail. Provides a list of acceptable Reason Codes for reject responses used by TCH and by Participants.
RTP Request for Payment Message Specification	Describes the structure, format, and content of the Request for Payment (pain.013) and Response to Request for Payment (pain.014) in detail. Provides a list of acceptable Reason Codes for negative Response to Request for Payment messages.
RTP Request for Information Message Specification	Describes the structure, format, and content of the Request for Information (camt.026) and Response to Request for Information (camt. 028) in detail.
RTP Payment Acknowledgement Message Specification	Describes the structure, format, and content of the Payment Acknowledgement (camt.035) in detail.
RTP Stand-Alone Remittance Advice Message Specification	Describes the structure, format, and content of the Stand-Alone Remittance Advice message (remt.001) in detail.
RTP System Time-Out and Request for Return of Funds Message Specification	Describes the structure, format, content, and usage of the System Time-Out and Request for Return of Funds (camt.056) and Response to Request for Return of Funds (camt.029) messages in detail.
RTP Administrative Message Specification	Describes the structure, format, and content of the various Administrative messages used within RTP. This document includes details regarding each System Notification Message type, sign-on messages, sign-off messages, and heartbeat (echo) messages.

07: Contact Us

Your questions and comments are very important to us. For more information about RTP, please contact us using the information provided below.

Product Development & Strategy

Steve Ledford

Phone: (336) 769-5308
Email: Steve.Ledford@theclearinghouse.org

Irfan Ahmad

Phone: (212) 613-0195
E-Mail: Irfan.Ahmad@theclearinghouse.org

Mark Majeske

Phone: (212) 613-0137
E-Mail: Mark.Majeske@theclearinghouse.org

James Colassano

Phone: (212) 612-9244
E-Mail: James.Colassano@theclearinghouse.org

Michael Thomas

Phone: (212) 612-9205
E-Mail: Michael.Thomas@theclearinghouse.org

Customer Relationship Management

Hank Farrar

Phone: (336) 769-5352
Email: Hank.Farrar@theclearinghouse.org