

Real Time Payments® (RTP)

Self-Audit Reference Guide



First Published: July 1, 2025 v 1.0

Overview

The Clearing House has announced credit unions participating in [RTP must complete an annual audit](#). Credit unions participating in RTP are expected in the self-audit to report [material findings of non-compliance](#).

The RTP network is an instant payments system from The Clearing House. Instant payments over the RTP network provide consumers and businesses with the ability to conveniently send payments directly from their accounts at insured depository institutions 24/7, and to receive and access funds sent to them over the RTP network immediately.

RTP Participant Self-Audit

All RTP Participants must complete an annual audit to verify compliance with the RTP Participation and Operating Rules, as required by RTP Operating Rule IX.A.2. Once the self-audit is complete, Participants must return the RTP Self-Audit Form to The Clearing House.

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

CU*Answers, and by extension CU*BASE/CBX, are only a limited part of the RTP ecosystem, which includes [The Clearing House](#) as the service provider and [Corporate One](#) as the funding agent. Our purpose in providing this resource is to assist credit unions in completing the self-audit by providing information credit unions may not immediately have available. Some answers will depend on the configuration that each credit union individually configures, and some will depend on answers from other partners in the RTP system.

Contents

Overview	1
Executive Summary.....	2
Rules Summary and Responsibilities	2
The RTP Ecosystem.....	7
More Information.....	7
Ordering.....	7
Learn More.....	7
Self-Audit Guidance.....	8
A. General Participant Responsibilities	8
B. Sending Participant Obligations .	12
C. Receiving Participant Obligations	13
D. Funding (as applicable based on Participant status as Funding Participant or Non-Funding Participant).....	16
E. Non-Payment Messages	18
F. Fraud and Risk Management Topics	19
G. Errors & Unauthorized Payments	21
H. Sending Requests for Payment (RFP) (applicable if Participant has RFP Sender Customers)	22
I. Receiving Requests for Payment (applicable to Participants that receive RFPs under the RFP Receive or RFP Send Message Persona)	26
J. Payment Service Providers (PSPs)	27

*Note: This resource currently applies to **RTP receive only**. Once a credit union implements sending RTP, answers to the self-audit will change. CU*Answers is dedicated to updating this document and publishing a new version after sending RTP becomes available.*

This resource only applies to RTP and not FedNow®. Currently, FedNow does not require a self-audit.

Executive Summary

The Clearing House has set forth the broad outlines of the risk assessment requirements. While the risk assessment is entirely the requirement of The Clearing House, completing the risk assessment may also have benefits for the credit union during a state and/or federal examination.

Rules Summary and Responsibilities

A full review of the *Guide* is available on Page 7.

A. General Participant Responsibilities		
TOPIC	RESPONSIBILITY	DESCRIPTION
1. 24/7 Operation. Participant must operate RTP on a continuous 24/7 basis. Operating on a continuous basis also requires ability to successfully read and respond to a minimum SLA of 50 Transactions Per Second (TPS).	CU*Answers	CU*Answers operates a 24/7/365 data center, apart from standard maintenance, and meets the minimum SLA.
2. Message Capability. Participant must be able to receive and/or send all messages required for its selected message persona.	Corporate One	Corporate One is the leading party concerning all message requirements. Credit Unions may contact Corporate One for assistance at memexp@corporateone.coop.
3. Payment Status/Message Information. Participant must immediately make available payment status information; and all required message information consistent with its message persona.	Corporate One	Corporate One is the leading party concerning all message requirements. Credit Unions may contact Corporate One for assistance at memexp@corporateone.coop.
4. No Correspondent Participation. Participants may not submit a Payment instructed by a Sender or instructs a Payment to a Receiver that is a foreign depository institution. However, Sending Participants may send RTP Payments in which other Participants or other domestic depository institutions are the Senders and/or Receivers under certain conditions.	Corporate One	The recommended course of action is to contact Corporate One for message verification.
5. No Fee Netting. Participant must not reduce the amount of an RTP Payment to collect fees.	CU*Answers	CU*Answers has built no fee netting into any RTP features.

6. No Searching for Accounts. Participants may not submit Payments or messages solely to search for active accounts.	CU*Answers & Corporate One	Corporate One would be best equipped to provide this information.
7. No Foreign Payments. Participant must not permit payments to/from an account outside the United States (defined to include the 50 states, Washington, D.C., or Puerto Rico); and must provide Customers with required disclosures.	Corporate One	The recommended course of action is to contact Corporate One for message verification.

A. General Participant Responsibilities		
TOPIC	RESPONSIBILITY	DESCRIPTION
8. Transaction Limit. Participant must receive RTP payments up to the current maximum transaction limit.	Credit Union sets internally.	The credit union's limits are set with Corporate One.

B. Sending Participant Obligations		
TOPIC	RESPONSIBILITY	DESCRIPTION
9. Receiver Name. Sending Participant must provide the Receiver's name to Senders of Payments from Consumer Accounts or include a means of confirming that Sender's Payment Instruction instructs payment to intended recipient.	Corporate One	It would be best practice to contact Corporate One for this matter.
10. Directory Service. Participant using a directory service must ensure compliance.	Credit Union verifies internally.	Credit Unions should review their internal policies.

C. Receiving Participant Obligations		
TOPIC	RESPONSIBILITY	DESCRIPTION
11. Payment Message Response. Participant must respond correctly to Payment Messages.	CU*Answers & Corporate One	Credit Unions would benefit from reaching out to Corporate One for complete message verification.
12. Payment Response Time. Participant must respond to Payment Messages within the required timeframe, as set forth in the RTP Technical Specifications.	Corporate One	Credit Unions would benefit from reaching out to Corporate One for complete message verification.
13. Payment Message Acceptance. Participant must accept all Payment Messages other than for allowed exceptions.	CU*Answers & Corporate One	Credit Unions would benefit from reaching out to Corporate One for complete message verification.
14. Funds Availability. Receiving Participant must provide immediate funds availability for an accepted Payment Message.	CU*Answers & Corporate One	When CU*Answers receives funds, at the request of Corporate One, the funds are made immediately available.

D. Funding (as applicable based on Participant status as Funding Participant or Non-Funding Participant)		
TOPIC	RESPONSIBILITY	DESCRIPTION
15. Funding Obligations Participant must satisfy its funding obligations. A Participant with a funding obligation must monitor and manage its position to ensure it has sufficient liquidity to cover anticipated payment origination activity when Fedwire is closed.	Credit Unions	Credit Unions may utilize their General Ledger transactions and apply Tool #60 if necessary.
16. Funding for RPT Only. Funding Participant must maintain funds in the Prefunded Balance Account to support only its reasonably anticipated RTP needs.	Credit Unions	Credit Unions may utilize their General Ledger transactions and apply Tool #60 if necessary.

D. Funding (as applicable based on Participant status as Funding Participant or Non-Funding Participant)		
TOPIC	RESPONSIBILITY	DESCRIPTION
17. Non-Funding Participants. Non-Funding Participants must have appropriate arrangements with its Funding Agent (Funding Manager Model).	Credit Unions	Credit Unions may utilize their General Ledger transactions and apply Tool #60 if necessary.

E. Non-Payment Messages		
TOPIC	RESPONSIBILITY	DESCRIPTION
18. Non-Payment Messages. Participant must send Payment-related Message Responses, consistent with its message persona.	Corporate One	It would be best practice to contact Corporate One for this matter.

F. Fraud and Risk Management Topics		
TOPIC	RESPONSIBILITY	DESCRIPTION
19. Fraud Reporting and Acting on Alerts. Participant must report fraudulent the RTP System.	CU*Answers & Corporate One	Credit Unions can utilize internal measures for fraud, as well as request assistance from Corporate One & CU*Answers.
20. Controlled Access. Participant must properly limit access to equipment used in connection with RTP.	CU*Answers & Corporate One	Credit Unions should reach out directly to Corporate One, and CU*Answers utilizes secured data centers for RTP services
21. Multi-Factor Authentication (MFA). Participant must use MFA to confirm the Sender's identity.	Corporate One	The recommended course of action is to contact Corporate One for complete MFA comprehension.
22. Fraud/Risk Monitoring. Participants must perform appropriate fraud/risk monitoring for RTP transactions.	Credit Unions	Concerning fraud, it is up to both the Credit Union and CU*Answers to report any suspicious behavior or bad actors.
23. Respond to Reports of Abuse. Participant responds to reports or RTP system abuse.	Credit Unions	Concerning fraud, it is up to all partners to report any suspicious behavior or bad actors.
24. OFAC. Participant must have a written OFAC program.	Credit Unions	Concerning fraud, it is up to all partners to report any suspicious behavior or bad actors.

G. Errors and Unauthorized Payments		
TOPIC	RESPONSIBILITY	DESCRIPTION
25. Errors/Unauthorized Payments (Cooperation). Participant must cooperate with other Participants and TCH.	Corporate One	CU*Answers can reasonably cooperate as necessary with any fraudulent matters as they arise.
26. Request for Return of Funds (RFR) Response. Participant must respond to an RFR within the required timeframe.	Corporate One	Credit Union must contact Corporate One to facilitate assistance on Return of Funds.






H. Sending Requests for Payment (RFP) (applicable if Participant has RFP Sender Customers)		
TOPIC	RESPONSIBILITY	DESCRIPTION
27. RFP Due Diligence. Participant must perform appropriate, risk-based due diligence on RFP-sending Customers.	Credit Unions	Credit Unions are in the best position to internally provide evidence of their own due diligence.
28. RFP Monitoring. Participant must monitor Customer RFPs.	Credit Unions	Credit Unions are in the best position to internally provide evidence of their monitoring practices.
29. Permissible Uses, RFP Sender Registration with TCH and other Prerequisites to Sending an RFP.	Credit Unions	Credit Unions are in the best position to internally provide evidence of their own due diligence.
30. RFP Investigation. Participant must investigate reports of fraudulent or abusive RFPs.	Credit Unions	Credit Unions are responsible for investigation reports and may assert their request for assistance to CU*Answers when necessary.
31. RFP Corrective Action. Participant must take corrective action for inappropriate RFPs and responds to reports of abuse.	Credit Unions & Corporate One	Credit Unions would benefit from reaching out to Corporate One for complete message verification.
32. RFP Warranty Claims Process.	Credit Unions	Credit Unions should review The Clearing House's document discussing RFP Warranty Claims Procedures which can be requested from The Clearing House.

I. Receiving Requests for Payment (applicable to Participants that receive RFPs under the RFP Receive or RFP Send Message Persona)		
TOPIC	RESPONSIBILITY	DESCRIPTION
33. RFP Display Requirements.	Credit Unions	It is a best practice for Credit Unions to assess a quality control check on their messaging standards.
34. RFP Warranty Claims Process.	Credit Unions	Credit Unions should review The Clearing House's document discussing RFP Warranty Claims Procedures which can be requested from The Clearing House.

J. Payment Service Providers (PSPs)		
TOPIC	RESPONSIBILITY	DESCRIPTION
35. PSP Customers. Participant must have appropriate risk-based measures that are reasonably designed to prevent a Money Transmitter customer from engaging in unapproved money transmission activity as a Sender. For identified PSPs, Participant must comply with (and as applicable, ensure the PSP complies with) certain application, agreement, audit/ certification, and other requirements.	N/A	Credit Unions are not a PSP.

The RTP Ecosystem

There are several elements to the RTP process.

MEMBERS	CREDIT UNION	CU*ANSWERS	CORPORATE ONE	TCH
				
Members receive funds through RTP transactions initiated by a third party.	Agree to participate in the RTP network.	CU*Answers is responsible for servicing requests from Corporate One via servicing transactions.	Provides actual connection to RTP network and sends transactions to CU*Answers via RTP APIs.	Provides the underlying services.

More Information

Ordering

RTP can be ordered from the CU*Answers Store here:

<https://store.cuanswers.com/product/real-time-payments-with-corp-one/>

Learn More

Learn more about RTP from our Kitchen page:

<https://www.cuanswers.com/resources/kitchen/instant-payment-news-rtp-from-the-clearinghouse/>

There are also valuable articles in our Knowledge Base online:

[https://kb.cuanswers.com/cuanswers/ext/kbsearch.aspx?keyword=Third-Party%20Service%20Provider%20\(TPSP\)%20for%20RTP%C2%AE%20Receive-Only](https://kb.cuanswers.com/cuanswers/ext/kbsearch.aspx?keyword=Third-Party%20Service%20Provider%20(TPSP)%20for%20RTP%C2%AE%20Receive-Only)

Self-Audit Guidance

This *Guide* will be updated as information changes and/or new services become available.

A. General Participant Responsibilities		
Topic	Relevant Rule	Guidance
<p>1. 24/7 Operation. Participant must operate RTP on a continuous 24/7 basis.</p> <p>Operating on a continuous basis also requires ability to successfully read and respond to a minimum SLA of 50 Transactions Per Second (TPS).</p>	<p><u>Technical Specification: RTP Continuous Operations Documentation.</u> Participants are expected to operate and manage their RTP system activity on a “continuous basis” as defined herein. TCH will measure compliance with this requirement by way of Participants’ response (either directly or through their TPSP) to a frequent automated system message that is checking for connection. For purposes of the continuous Operation requirement, TCH has established a standard of 99.5% continuous connection measured monthly, which allows cumulative non-connectivity of roughly 3.6 hours per month. In addition, TCH will not consider any non-connectivity during a maintenance window each Sunday from 2 AM to 6 AM Eastern Time towards its assessment of the continuous operations standard. See also RTP Participation Rule I.A.4.</p> <p>Note that a Participant may consider assessing its compliance by reviewing records of its relevant system messages (sign- on, sign-off, and echo response); and/or other records or policies relating to its ability to receive RTP Payments in compliance with this obligation.</p>	<p>CU*BASE/CBX is available 24/7 aside from the standard maintenance events. These maintenance events and windows can be reviewed on CU*Answers’ System Uptime page. CU*Answers has tested the ability to meet the SLA requirement.</p> <p>Corporate One also has its own standard maintenance windows.</p>
<p>2. Message Capability. Participant must be able to receive and/or send all messages required for its selected message persona.</p>	<p><u>Technical Specifications, Business Application Header, pages 15-17.</u> The RTP message personas are “Payment Receive,” “Payment Send,” “Test RFP,” “RFP Receive” and “RFP Send.” Each persona has a set of Mandatory and Optional messages. Refer to the RTP Document Library for the Message Persona Specifications.</p> <p>Note that before TCH enables a Participant to use the RTP system with a selected message persona, TCH tests and certifies that a Participant can receive and/or send all messages required for that persona.</p>	<p>Corporate One is the leading party concerning all message requirements. Corporate One facilitates send messages, and CU*Answers only has the capacity to obtain receive messages. CU*Answers does not configure messages which is the responsibility of Corporate One.</p> <p>Contacting Corporate One for assistance on message verification is the best course of action.</p> <p>Credit Unions may contact Corporate One for assistance at memexp@corporateone.coop.</p>

A. General Participant Responsibilities

Topic	Relevant Rule	Guidance
3. Payment Status/Message Information. Participant must immediately make available payment status information; and all required message information consistent with its message persona.	<p>Operating Rule II.F. Payment Status & Message Information.</p> <p>Payment Status. Sending Participants and receiving Participants must immediately make available information regarding the status of an RTP Payment to the Sender and Receiver, respectively, as specified in the RTP Technical Specifications. However, a Receiving Participant that has provided a “reject” message in response to a Payment Message due to reasons specified in V(C)(1), (2), or (3) of these Rules has no obligation to provide status information to the Receiver.</p> <p>Message Information. Participant must make available their respective Customers any information contained in the fields of a Payment Message, Payment Message Response, or a Non-Payment Message that are designated as required to be made available in the RTP Technical Specifications, except that Participants shall not be obligated to make available information:</p> <ul style="list-style-type: none"> • That would violate the Participant’s reasonable stands for messaging that prohibit offensive or threatening language or unlawful activity; • Contained in a Payment Message if the Participant has provided a “reject” message in response to the Payment Message; • Contained in a Request for Payment Message, if the Participant’s Customer, has elected to not receive (i) Requests for Payment from the Person that initiated the Requests for Payment, or (ii) all Requests for Payment; or if the Participant’s Customer is not enrolled in online or mobile banking. <p>Note that the RTP Rules do not define the term “immediately” or establish a specific timeline in seconds or other units for making payment status information available under Operating Rule II.F.1. Participants may establish their own standards and technical process for compliance with this rule, and for purposes of the self-audit, assess compliance with those standards and/or verify the technical process they have established provides for compliance with the standards they have set. As the network matures, TCH may establish a specific service level requirement regarding the term “immediately” for purposes of this rule.</p>	Corporate One would be best equipped to provide information concerning messages or the third-party source application the Credit Union is using.

A. General Participant Responsibilities

Topic	Relevant Rule	Guidance
4. No Correspondent Participation. Participants may not submit a Payment instructed by a Sender or instructs a Payment to a Receiver that is a foreign depository institution. However, Sending Participants may send RTP Payments in which other Participants or other domestic depository institutions are the Senders and/or Receivers under certain conditions.	<p>Operating Rule II.B. No Correspondent Participation.</p> <ol style="list-style-type: none"> 1. A Participant may not submit a Payment Message to the RTP System that is instructed by a Sender or instructs payment to a Receiver that is a foreign depository institution; Is instructed by a Sender or instructs payment to a Receiver that is a Participant or a domestic depository institution, unless one of the following exceptions apply: <ul style="list-style-type: none"> • The Participant serves as a Third-Party Service Provider for another Participant and is submitting a Payment Message for the other Participant as a Third-Party Service Provider and not as the Sending Participant; • The Sending Participant is submitting a Payment Message for a Sender that is not a depository institution to a Receiving Participant that is the Receiver of the Payment, and there is no further Person on whose behalf the Receiving Participant is receiving the Payment; <p>The Sending Participant is submitting a Payment Message for itself as Sender or a Sender that is a Participant or other domestic depository institution to a Receiver that is not a depository institution and there is no further depository institution or Person on whose behalf the Sender is sending the Payment; or</p> <p>The Sending Participant is submitting a Payment Message for itself as Sender or a Sender that is a Participant or other domestic depository institution to a Receiver that is a Participant or other domestic depository institution, the Payment is not a Cover Payment, and there is no further Person on whose behalf the Sender is sending the Payment and no further Person on whose behalf the Receiver is Receiving the Payment.</p> 2. A Sending Participant that submits Payment Messages to the RTP System that is instructed by a Sender or instructs payment to a Receiver that is a Participant or a domestic depository institution warrants to TCH that each such Payment meets the requirements set forth in subsections 1(b) (ii), (iii), or (iv) above (as applicable to the Payment), and must have measures in place that are reasonably designed to ensure compliance with the requirements of subsections 1(b) (ii), (iii), or (iv) above (as applicable to its Payment origination). 	<p>Corporate One is the leading party concerning all message requirements. Corporate One facilitates send messages, and CU*Answers only has the capacity to obtain receive messages. CU*Answers does not configure messages, which is the responsibility of Corporate One.</p> <p>Contacting Corporate One for assistance on message verification is the best course of action.</p> <p>Credit Unions may contact Corporate One for assistance at memexp@corporateone.coop.</p>

A. General Participant Responsibilities

Topic	Relevant Rule	Guidance
5. No Fee Netting. Participant must not reduce the amount of an RTP Payment to collect fees.	<u>Operating Rule II.D. No Fee Netting.</u> Participants in RTP are not permitted to reduce the principal amount of an RTP Payment as a means of collecting fees. This provision does not restrict a Participant's ability to separately charge its Customers for RTP Payments. Note that TCH has issued an RTP Rules interpretation further providing that a Participant that receives a Request for Return of Funds and elects to return funds, may not deduct a fee from the amount of funds available to be returned in order to cover the cost of the Participant's handling of the request for return. <i>For further detail, see RTP Rules Interpretation.</i>	CU*Answers has built no fee mechanism into any of our RTP Send features. CU*Answers will not change until credit union clients start conversations about charging fees. When CU*Answers receives a transaction, we do not reduce the transaction value by assessing a fee. Within fee netting, an institution may not take part of the payment as a means of collecting fees.
6. No Searching for Accounts. Participants may not submit Payments or messages solely to search for active accounts.	<u>Operating Rule II.E.1. Searching for Accounts.</u> RTP Payment Messages or Non-Payment Messages should only be used to determine if account numbers, whether in tokenized or untokenized form, are associated with valid, active Accounts when an account number has been given to the Sender (or Message Sender) by an intended Receiver (or Message Receiver) who is expecting to receive one or more Payments from the Sender.	CU*Answers does not require any account information to process the request, therefore no sending takes place. Corporate One only asks to verify account and accept incoming funds. CU*Answers does not handle this functionality, so the Credit Union must contact Corporate One to interpret the configuration.
7. No Foreign Payments. Participant must not permit payments to/from an account outside the United States (defined to include the 50 states, Washington, D.C., or Puerto Rico); and must provide Customers with required disclosures.	<u>Operating Rule II.E.2. Prohibited Transactions.</u> The RTP System shall be used by Participants only to effectuate RTP Payments between a Sender and Receiver whose Accounts are located in the United States of America. To the extent a Sender sends or a Receiver receives a Payment on behalf of another Person, whether such Sender or Receiver is a Payment Service Provider or not, the Person on whose behalf the Sender sends or the Receiver receives must be a resident of or otherwise domiciled in the United States. Participants must inform Senders and Receivers of their obligation to comply with this restriction regarding Payments sent or received on behalf of other Persons and with OFAC regulations in the legal terms that govern their Customers' use of RTP.	CU*Answers does not handle this functionality, so the Credit Union must contact Corporate One. This is because CU*Answers does not have the send functionality equipped. CU*Answers does not have submission of payments. Once the send portion of RTP is turned on, this section will be updated with the appropriate measures.
8. Transaction Limit. Participant must receive RTP payments up to the current maximum transaction limit.	<u>Operating Rule II.C.2. Eligible Payments.</u> An RTP Payment may not exceed the general transaction limit of \$1,000,000. Sending Participants may establish a lower transaction limit for their Senders. Receiving Participants may not establish a lower transaction limit for their Receivers.	The credit union's limits are set with Corporate One. Credit Union limits will be set by Corporate One when the Credit Union signs up for the service, and Corporate One will be responsible for making changes to those limits. It is best practice for Credit Unions to list their limits here when completing this.

B. Sending Participant Obligations

(See Section III of the Operating Rules.)

Topic	Relevant Rule	Guidance
9. Receiver Name. Sending Participant must provide the Receiver's name to Senders of Payments from Consumer Accounts or include a means of confirming that Sender's Payment Instruction instructs payment to intended recipient.	<p><u>Operating Rule III.C.3. Prerequisites to Sending a Payment Message.</u></p> <p>Prior to submitting a Payment Message to the RTP System, a Sending Participant must:</p> <p>With respect to RTP Payments originating from Accounts of Consumers, provide the Sender with the name of the Receiver that is associated with the routing information the Sender has provided to the Sending Participant in the Sender's Payment Instruction. Alternatively, a Sending Participant must include in the Payment origination process or the design of a Payment origination service a means of confirming with reasonable assurance that a Sender's Payment Instruction instructs payment to the account of the Sender's intended recipient. A Payment in response to a Request for Payment that uses the Message Sender information from the Request for Payment to identify the Receiver of the Payment satisfies this rule.</p> <p>Note that TCH has issued an RTP Rules interpretation providing that a Sending Participant does not need to provide the Receiver's name if a Consumer instructs payment to an account and certain conditions are met. The Rules interpretation also provides that in addition to relying on a directory service to satisfy the Receiver name rule, Participants may use other "reliable methods" (such as an in house capability, a third-party service, or combination of the two) as set forth in the interpretation.</p> <p><i>For further detail, see RTP Rules Interpretation.</i></p>	<p>Credit Unions provide Corporate One with the sender information. CU*Answers is only responsible for the receiving portion. Thus, the Credit Union would need to make certain their procedures for confirming Sender information aligns with the process that Corporate One follows. It would be best practice to contact Corporate One for this matter.</p>
10. Directory Service. Participant using a directory service must ensure compliance.	<p><u>Operating Rule III.G. Directory Services.</u></p> <p>For purposes of this rule "routing information" means information that the RTP Technical Specifications permit a Sending Participant to use to identify the Receiving Participant and Receiver's Account in a RTP Payment Message. A Sending Participant that permits its Senders to provide Payment Instructions that identify the Receiver's account with an email address, phone number, or other social alias ("social identifiers") must have risk management in place with respect to any directory the Participant uses to associate such social identifiers with routing information. Such risk management should take into consideration the irrevocable nature of RTP Payments and the need for routing information to be associated with a Sender's intended Receiver.</p>	<p>CU*Answers does not oversee sending a payment message, only receiving. Further, CU*Answers can confirm their portion of receiving is fully function. Credit Unions will need to obtain confirmation from Corporate One that their sending portion is fully functional.</p>

C. Receiving Participant Obligations

(See Section V of the Operating Rules.)

Topic	Relevant Rule	Guidance
11. Payment Message Response. Participant must respond correctly to Payment Messages.	<p><u>Operating Rule V.E. Receiving Participant Responses to Payment Messages.</u></p> <p>1. Accept An “accept” message submitted to the RTP System, whether as an initial response to a Payment Message or an acknowledgement message following an initial response of “accept without posting” as provided in Rule V(E)(2)(d), means that the Receiving Participant will accept the Payment Message and will provide immediate funds availability to the Receiver...</p> <p>2. Accept Without Posting An “accept without posting” message submitted to the RTP System means that the Receiving Participant 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 review the RTP Payment for legal or compliance purposes....</p> <p>A Payment Message accepted without posting is immediately and finally settled as provided in Rule VI(E) of these RTP Operating Rules...</p> <p>A Receiving Participant that accepts without posting is expected to determine by 11:59 p.m. local time the next business day following its “accept without posting” message whether the Receiving Participant will make funds available to the Receiver, except in cases in which the RTP Payment is being reviewed for compliance with sanctions laws applicable to or otherwise complied with by the Receiving Participant...</p> <p>3. Reject A “reject” message submitted to the RTP System means that the Receiving Participant has rejected the Payment Message...</p> <p>The Receiving Participant must include a valid and most appropriate reason code with the “reject” message as specified in the RTP Technical Specifications. Rejected RTP Payments will not be settled.</p>	<p>Credit Unions will have to reach out directly to Corporate One as they handle complete payment messages. CU*Answers does not respond to RTP messages.</p> <p>CU*Answers fulfills the accept messages provided by the RTP System. When CU*Answers accepts a Payment Request from Corp and accepts it, funds are immediately available to the receiver.</p> <p>If request is made from Corp One, CU*Answers either accepts or rejects immediately.</p> <p>CU*Answers provides a code to Corp One and then Corporate One has to provide reason code that complies with technical explanation.</p>

C. Receiving Participant Obligations

(See Section V of the Operating Rules.)

Topic	Relevant Rule	Guidance
12. Payment Response Time. Participant must respond to Payment Messages within the required timeframe, as set forth in the RTP Technical Specifications.	<u>Operating Rule V.A. Immediate Response.</u> A Receiving Participant must respond to a Payment Message within the timeframe established in the RTP Technical Specifications. Technical Specifications: RTP System Interface Guide; 5.9 Message Expiration and Timeout. Payment messages must be processed in a timely manner or they will be timed out by the RTP system. For any message that requires a response, the Receiving Participant must respond to the message within 5 seconds.	It may be in the best interest for Credit Unions to contact CU*Answers concerning the APIs that are applicable. Corporate One monitors the Payment Response Time and their exactness. CU Answers does not have specific response requirements, but it is monitored through response tools via Corporate One. CU*Answers does not measure the entire timeline, simply the correspondence between its internal system and Corporate One. For exactness, that would need to be communicated by Corporate One.
13. Payment Message Acceptance. Participant must accept all Payment Messages other than for allowed exceptions.	<u>Operating Rule V.C. General Acceptance Requirement.</u> A Receiving Participant agrees to accept all Payment Messages that conform to the RTP Technical Specifications, unless: The identified Receiver Account is closed, invalid, or being monitored for suspected fraudulent or other illegal activity, or is not a “transaction account” as defined in the Federal Reserve Board’s Regulation D (12 C.F.R 204); The owner of an Account has indicated that it does not wish to accept all or certain specified RTP Payments for the The Payment Message cannot be accepted due to legal or regulatory compliance requirements.	CU*Answers does not oversee sending payment messages, only receiving. CU*Answers responds to Corporate One’s request to verify if an account is valid.

C. Receiving Participant Obligations

(See Section V of the Operating Rules.)

Topic	Relevant Rule	Guidance
14. Funds Availability. Receiving Participant must provide immediate funds availability for an accepted Payment Message.	<p><u>Operating Rule V.E.1. Receiving Participant Responses to Payment Messages.</u></p> <p>1. Accept</p> <p>An “accept” message submitted to the RTP System, whether as an initial response to a Payment Message or following an initial response of “accept without posting” as provided in Rule V(E)(2)(d), means that the Receiving Participant will accept the Payment Message and will provide immediate funds availability to the Receiver....</p> <p>A Receiving Participant (including a Non-Funding Group Member) that returns an “accept” message must make funds from the RTP Payment available to the Receiver identified by the account number in the accepted Payment Message upon receipt of a message from the RTP system acknowledging receipt of the Receiving Participant’s “accept” message.</p> <p><u>Operating Rule V.B. No Inconsistent Cut-Off Times</u></p> <p>Notwithstanding Section 4-A-106 of the New York Uniform Commercial Code, Receiving Participants may not establish cut-off times for receiving Payment Messages that would cause the Payment related to a Payment Message to be made on a different RTP Day than the RTP Day on which the Payment Message was received or otherwise delay funds availability as required by these RTP Operating Rules.</p> <p>Note that the RTP Rules do not currently define the term “immediate” or establish a specific funds availability timeline in seconds or other units under Operating Rule V.E.1. Participants may establish their own standards and technical process for compliance with this rule, and for purposes of the self-audit, assess compliance with those standards and/ or verify the technical process they established provides for compliance with the standards they have set. As the network matures, TCH may establish a specific service level requirement regarding the term “immediately” for purposes of this rule.</p>	When CU*Answers receives funds, at the request of Corporate One, the funds are made immediately available.

D. Funding (as applicable based on Participant status as Funding Participant or Non-Funding Participant)

(See Section VI of the Operating Rules)

Topic	Relevant Rule	Guidance
<p>15. Funding Obligations Participant must satisfy its funding obligations.</p> <p>A Participant with a funding obligation must monitor and manage its position to ensure it has sufficient liquidity to cover anticipated payment origination activity when Fedwire is closed.</p>	<p><u>Operating Rule VI.A. Funding Participants.</u> A Participant that is a Funding Participant is obligated to satisfy its funding obligations in accordance with the RTP Participation Rules and these RTP Operating Rules.</p> <p><u>Operating Rule VI.B. Non-Funding Participants.</u> A Non-Funding Participant may choose a Funding Agent that uses the Funding Manager or Funding Provider model. A Non-funding Participant uses a Funding Manager (and has a Current Prefunded Position) is obligated to satisfy its funding obligations (if any) through a Funding Manager an in accordance with the RTP Rules.</p> <p><u>Operating Rule III.C.1. Prerequisites to Submitting a Payment Message.</u> Prior to submitting a Payment Message to the RTP System, a Sending Participant must have satisfied its Prefunded Requirement as specified in the RTP Participation Rules and the RTP Operating Rules.¹</p> <p><u>Operating Rule VI.D.2. and VI.D.3.</u> A Participant with a funding obligation must monitor its Current Prefunded Position and provide supplemental funding to the Prefunded Balance Account if its Current Prefunded Position falls below its Prefunded Requirement during Fedwire operating hours.</p>	<p>CU*Answers uses General Ledger transactions to complete the RTP payments, and it is best practice that Credit Unions have a General Ledger setup specifically for RTP. Therefore, Credit Unions should look internally to address this relevant rule. Credit Unions may utilize Tool #60 in CBX to assist their efforts.</p>
<p>16. Funding for RPT Only. Funding Participant must maintain funds in the Prefunded Balance Account to support only its reasonably anticipated RTP needs.</p>	<p><u>Operating Rule VI.C.1.e. Prefunded Balance Account.</u> The Prefunded Balance Account may only be used in support of RTP activities. Participants are expected to maintain Excess Liquidity for no purpose other than their reasonably anticipated liquidity needs for their RTP Payments (including such messages sent in response to a Request for Return of Funds or to refund funds upon rejection of a Payment Message that was accepted without posting, as described in Rule V(E)(2)(e)(i)) on a daily or non-Fedwire operating period basis. TCH reserves the right to require a Participant to request disbursement of funds, as provided in Rule VI(G), in order to reduce the Participant's Excess Liquidity if TCH determines that the Participant's Excess Liquidity is not consistent with the Participant's RTP send activity. A Participant may consider assessing its compliance by reviewing and determining the existence of a pattern of disbursements and/or supplemental funding to maintain its Current Prefunded Position above its Prefunded Requirement in relationship to its expected payment activity.</p>	<p>CU*Answers users General Ledger transactions to complete the RTP payments, and it is best practice that Credit Unions have a General Ledger setup specifically for RTP. Therefore, Credit Unions should look internally to address this relevant rule. Credit Unions may utilize Tool #60 in CBX to assist their efforts.</p>

¹ Note also that if a Sending Participant or its Funding Agent does not have sufficient liquidity, a Payment will be rejected (with the AM04 message and NSF code).

D. Funding (as applicable based on Participant status as Funding Participant or Non-Funding Participant)

(See Section VI of the Operating Rules)

Topic	Relevant Rule	Guidance
17. Non-Funding Participants. Non-Funding Participants must have appropriate arrangements with its Funding Agent (Funding Manager Model).	<u>Operating Rule VI.B.2. Funding Agents & Non-funding Participants.</u> A Non-funding Participant that uses a Funding Manager must have appropriate communication and financial arrangements in place to ensure that the Funding Manager meets the Non-funding Participant's funding obligations in a timely and reliable manner.	CU*Answers uses General Ledger transactions to complete the RTP payments, and it is best practice that Credit Unions have a General Ledger setup specifically for RTP. Therefore, Credit Unions should look internally to address this relevant rule. Credit Unions may utilize Tool #60 in CBX to assist their efforts.

E. Non-Payment Messages

(See Section VII of the Operating Rules.)

Topic	Relevant Rule	Guidance
18. Non-Payment Messages. Participant must send Payment-related Message Responses, consistent with its message persona.	<u>Operating Rule VII.A. Non-Payment Message Types & Responses</u> A Message Receiving Participant must transmit any Payment-related Response Message provided by its Customer to the Message Sending Participant. <u>Technical Specifications, Business Application Header, pages 15-17.</u> Refer to the RTP Document Library on the TCH website.	CU*Answers does not handle this message functionality, so the Credit Union must contact Corporate One. Based upon the network structure, Corporate One has all the information concerning payment messages.

F. Fraud and Risk Management Topics

(See RTP Operating Rules II.G.1 and II.G.2 and Risk Management & Fraud Control Requirements Schedule.)

Topic	Relevant Rule	Guidance
19. Fraud Reporting and Acting on Alerts. Participant must report fraudulent activity to TCH and the other Participant involved in a Fraudulent RTP Payment.	<p><u>Operating Rules II.G.1 and II.G.2 Participant Response and Fraud Reporting Obligations</u></p> <p>1. Participants must act on alerts from TCH regarding suspected fraud in connection with the RTP System.</p> <p>2. Participants must report fraudulent activity involving the RTP System in accordance with the RTP Technical Specifications and Risk Management and Fraud Control Requirements.</p> <p>Note that TCH has issued a Rules Interpretation regarding the requirement to act on alerts from TCH and to report fraudulent activity involving the RTP system. With respect to the reporting requirement, a Participant must report a fraudulent RTP Payment (one that the Sending Participant has determined was not authorized by the Sender) to the Receiving Participant by sending a Request for Return of Funds message (camt.056) with the “FRAD” reason code. The Participant must also report material findings regarding unauthorized Payments or authorized Payments sent in response to a Request for Payment that the Sender claims was deceptive or misleading to RTPRules@theclearinghouse.org (Participants should not send individual RTP Payment information or nonpublic personal information in such reports.)</p> <p>For further information, see the RTP Rules Interpretation.</p>	<p>CU*Answers does not handle this message functionality. CU*Answers does not handle this functionality for reversals, so the Credit Union must contact Corporate One.</p> <p>Credit union can internally recognize these unauthorized transactions themselves.</p> <p>CU*Answers can reasonably cooperate as necessary with any fraudulent matters as they arise.</p>
20. Controlled Access. Participant must properly limit access to equipment used in connection with RTP.	<p><u>Risk Management & Fraud Control Requirements Schedule § 7-8.</u></p> <p>A participant must limit access to any equipment used in connection with the RTP System, including, without limitation, equipment used to submit Payment Messages and Non-payment Messages to the RTP System, to only those individuals that have a legitimate business purpose to access such equipment.</p> <p>A Participant must maintain any TCH-issued equipment in a safe and secure location that regulates and limits access to the TCH-issued equipment to only those individuals that have a legitimate business purpose to access such TCH-issued equipment.</p>	<p>CU*Answers utilizes secured data centers for RTP services. Credit Unions should reach out directly to Corporate One for additional response guidance. For CU*Answer’s operations and services, anyone can reference the SOC Report here.</p>
21. Multi-Factor Authentication (MFA). Participant must use MFA to confirm the Sender’s identity.	<p><u>Risk Management & Fraud Control Requirements Schedule § 1.</u></p> <p>Sending Participants must, at a minimum, utilize multi-factor authentication (something you know and something you have or something you are) to authenticate the identity of customers who transmit Payment Instructions to the Sending Participant.</p> <p>See also <i>Operating Rule III.A.1.</i></p>	<p>CU*Answers does not handle this message functionality given that it is a send message. Corporate One has set up Multi-Factor Authentication within their construct. Therefore, Credit Unions may contact Corporate One for assistance at memexp@corporateone.coop.</p>

F. Fraud and Risk Management Topics

(See RTP Operating Rules II.G.1 and II.G.2 and Risk Management & Fraud Control Requirements Schedule.)

Topic	Relevant Rule	Guidance
22. Fraud/Risk Monitoring. Participants must perform appropriate fraud/risk monitoring for RTP transactions.	<u>Risk Management & Fraud Control Requirements Schedule §§ 2-3.</u> Sending Participants must perform appropriate fraud monitoring prior to submitting a Payment Message to the RTPS. A Participant must regularly review the performance of its fraud monitoring systems and make appropriate updates to address evolving fraud risks. <i>See also Operating Rule III.A.2.</i>	<p>Concerning fraud, it is up to both the Credit Union and CU*Answers to report any suspicious behavior or bad actors.. CU*Answers being on receiving end does not run any scans past original verification of account. Credit Unions may utilize Tool #101 for Deposits Only to set up pattern(s). Additionally, Credit Unions may utilize Tool #537 to review alerts. For any further questions concerning fraud monitoring, Credit Unions may reach out to AuditLink for consultation.</p> <p>Further, Credit Unions should look within their internal policies on how to best handle these situations.</p>
23. Respond to Reports of Abuse. Participant responds to reports of RTP system abuse.	<u>Risk Management & Fraud Control Requirements Schedule § 6.</u> A participant must be able to respond to any report of abuse from the RTP and must retain the right and ability to suspend any Customer from initiating Payment Messages or Request for Payment Messages if the Customer is suspected of misusing the RTP System.	It would be most advantageous for Credit Unions to keep internal records of any RTP system abuse, and any fraud found on their platform. This would include the record of any remedial measures further taken. Credit Unions may also refer to Tools #101 & #537 as shown above.
24. OFAC. Participant must have a written OFAC program.	<u>Operating Rule II.J. OFAC Compliance Program.</u> A Participant must have a written OFAC compliance program reasonably designed to promote and monitor compliance with OFAC sanctions programs and regulations. <i>See also Operating Rule II.E.2.</i>	Credit Unions may reference OFAC compliance here , and well as refer to their own internal policies for how they promote and monitor compliance with OFAC sanctions.

G. Errors & Unauthorized Payments

Topic	Relevant Rule	Guidance
25. Errors/Unauthorized Payments (Cooperation). Participant must cooperate with other Participants and TCH.	<u>Operating Rule II.I.3.</u> Without prejudice to the rights or responsibilities of the parties to an unauthorized or erroneous RTP Payment under Article 4-A of the New York Uniform Commercial Code or the EFTA, Participants shall reasonably cooperate among themselves and with TCH in attempts to address and recover unauthorized and erroneous RTP Payments.	CU*Answers does not handle this functionality for reversals, so the Credit Union must contact Corporate One. Credit union can internally recognize these unauthorized transactions themselves. CU*Answers can reasonably cooperate as necessary with any fraudulent matters as they arise.
26. Request for Return of Funds (RFR) Response. Participant must respond to an RFR within the required timeframe.	<u>Operating Rule VII.C.1-2, 4. Requests for Return of Funds.</u> A Participant may send a Request for Return of Funds for any reason, including to request a return of funds related to an unauthorized or erroneous RTP Payment or an RTP Payment made in response to a fraudulent Request for Payment... <ol style="list-style-type: none"> 1. A Receiving Participant must respond to a Request for Return of Funds with a Response to Request for Return of Funds, but a Receiving Participant shall be under no obligation to return funds related to an RTP Payment in response to a Sending Participant's Request for Return of Funds. 2. The process for sending and responding to a Request for Return of Funds for RTP Payments is set forth in the RTP Technical Specifications. A Receiving Participant must send its Response to Request for Return of Funds within ten banking days of receiving the Request for Return of Funds, except for Request for Return of Funds messages that are sent due to claimed fraud ("FRAD") or breach of a Request for Payment warranty ("UPAY"). With respect to such Request for Return of Funds messages, the Receiving Participant may take longer than ten banking days to send a Response to Request for Return of Funds message to allow time for the Receiving Participant to investigate the claimed fraud or breach of warranty. In such situations the Receiving Participant is expected to promptly perform its investigation and send its Response to Request for Return of Funds upon completion of its investigation. 3. A Sending Participant may not resubmit a Request for Return of Funds if it has previously sent a Request for Return of Funds for the same payment and received a negative ("RJCR" status) Response to Request for Return of Funds due to the Receiver's refusal to return the funds ("CUST" reason code). This prohibition does not apply if the Sending Participant is resubmitting a Request for Return of Funds because TCH requires such resubmission in the RTP Technical Specifications or a published interpretation of these RTP Operating Rules. 	CU*Answers does not handle this functionality for reversals, so the Credit Union must contact Corporate One.

H. Sending Requests for Payment (RFP) (applicable if Participant has RFP Sender Customers)

(See Operating Rule VII.B, Minimum Requirements for Requests for Payment Schedule, Permissible Uses for Requests for Payment Rules Interpretation.)

Topic	Relevant Rule	Guidance
27. RFP Due Diligence. Participant must perform appropriate, risk-based due diligence on RFP-sending Customers.	<u>Requirements for RFP Customers Schedule § 1.</u> Implement documented procedures for performing appropriate, risk-based due diligence on a Customer that seeks to initiate Requests for Payment. <ul style="list-style-type: none"> With respect to non-consumer Customers, such procedures must include at a minimum: A review of information related to the Customer's background and business sufficient for the Participant to evaluate and determine, at a minimum, that the Customer is conducting legitimate business and that the Customer does not have a history of regulatory violations excessive Consumer complaints, or fraudulent activity; Documentation of the Customer's legitimate business purpose for sending Requests for Payment. With respect to consumer Customers, such procedures must include, at a minimum, a determination that the Participant has no information regarding the Customer that would indicate the Customer is likely to misuse Requests for Payment. On a risk-based basis, Participants are expected to conduct periodic reviews of a Customer who has been approved to initiate Requests for Payment to ensure that the ability to initiate Requests for Payment remains appropriate for that Customer. 	At this time, CU*Answers does not send to Consumers, but only receives. Therefore, it is a best practice that a Credit Unions risk-based due diligence is adopted into their internal policies that concern Requests for Payments. Once the send portion of RTP is turned on, this section will be updated with the appropriate measures.
28. RFP Monitoring. Participant must monitor Customer RFPs.	<u>Requirements for RFP Customers Schedule § 2.</u> Implement documented procedures for monitoring Requests for Payment submitted by a Customer. Such procedures must include, at a minimum, the following: <ul style="list-style-type: none"> A monthly monitoring and tracking of a Customer's Request for Payment volume and any reports made to the Participant of a Customer's fraudulent or abusive Requests for Payment. A process for identifying and investigating anomalous volume identified during the monthly review of the Customer's Request for Payment activity. Any investigation into anomalous activity must include, at a minimum, an inquiry with the Customer to determine whether the increase or decrease in the Customer's Request for Payment volume occurred in the ordinary course of business. 	CU*Answers does not send to Consumers, but only receives. Therefore, it is a best practice that a Credit Unions risk-based due diligence is adopted into their internal policies that concern Requests for Payments.

H. Sending Requests for Payment (RFP) (applicable if Participant has RFP Sender Customers)

(See Operating Rule VII.B, Minimum Requirements for Requests for Payment Schedule, Permissible Uses for Requests for Payment Rules Interpretation.)

Topic	Relevant Rule	Guidance
29. Permissible Uses, RFP Sender Registration with TCH and other Prerequisites to Sending an RFP.	<p><u>Operating Rule VII.B.2.a-d. Requirements for Sending RFP Messages.</u></p> <p>A Participant may send an RFP only for a Permissible Use as defined in a public RTP Rules interpretation. As set forth in the RTP Rules interpretation regarding Permissible Uses for RFPs, a Message Sending Participant that will send RFPs (RFP Sending Participant) must provide certain information to TCH about the Message Sender (RFP Sender) and its Permissible Use(s) before the Customer may send RFPs.</p> <p>In addition, a Message Sending Participant that submits a Requests for Payment to the RTP System must:</p> <ul style="list-style-type: none"> • Ensure that the Request for Payment complies with the RTP Technical Specifications; • Comply with the Requirements for Request for Payment Customers; • Have reasonable basis for determining that the Message Sender's RFPs will only be used for Permissible Uses (as defined in a published RTP Rules Interpretation) and have made such a determination prior to submitting an RFP for the Message Sender; • Warrant to TCH and the Message Receiving Participant that the Request for Payment is made a legitimate purpose and is not part of a fraudulent scheme to induce payment harassing; or otherwise unlawful, including violations of the prohibition on unfair, deceptive or abusive acts or practices (UDAAP). <p>TCH has issued rules interpretation on the scope of the RFP warranty that provides further information and examples.</p>	<p>CU*Answers does not send to Consumers, but only receives.</p> <p>Therefore, it is a best practice that a Credit Unions risk-based due diligence is adopted into their internal policies that concern Requests for Payments.</p>

Additional information about the RFP Sender registration requirement is available in the RTP Document Library, which is available here:

<https://www.theclearinghouse.org/payment-systems/rtp/document-library>.

H. Sending Requests for Payment (RFP) (applicable if Participant has RFP Sender Customers)

(See Operating Rule VII.B, Minimum Requirements for Requests for Payment Schedule, Permissible Uses for Requests for Payment Rules Interpretation.)

Topic	Relevant Rule	Guidance
30. RFP Investigation. Participant must investigate reports of fraudulent or abusive RFPs.	<u>Requirements for RFP Customers Schedule § 3.</u> Implement documented procedures for investigating any report of fraudulent or abusive Requests for Payment received from any source, including TCH, a Customer, or another Participant. Fraudulent or abusive use of Requests for Payment include, but are not limited to: <ul style="list-style-type: none"> • The use of deceptive or misleading information in a Request for Payment in order to induce a Payment in response, such as a misrepresentation regarding the true identity of the Customer that initiates the Request for Payment or the purpose of the Request for Payment. • The use of language in a Request for Payment Message that could reasonably be perceived by the Customer of the Message Receiving Participant as threatening or intimidating. • The origination of repeated Requests for Payment to the same Customer of the Message Receiving Participant within a timeframe that could be reasonably perceived by that Customer as harassing. 	CU*Answers does not send to Consumers, but only receives. Therefore, it is a best practice that Credit Unions review their internal policies for reports of fraud and follow their protocol for any incidents that occur.
31. RFP Corrective Action. Participant must take corrective action for inappropriate RFPs and responds to reports of abuse.	<u>Operating Rule.VII.B.2.e-f. Requirements for RFP Messages.</u> A Message Sending Participant that submits a Request for Payment to the RTP System must: <ul style="list-style-type: none"> • Take corrective action with respect to a Message Sender when a Message Sending Participant determines, or should have determined based on information available to it, that the Message Sender has initiated Requests for Payment that are not made for (i) a Permissible Use; or (ii) a legitimate purpose or are fraudulent, abusive or unlawful. Such corrective actions may include suspension of a Customer's ability to initiate Requests for Payment and, under appropriate circumstances, the ability to receive RTP Payments, as determined by the Message Sending Participant or by TCH through Rules Enforcement Proceedings; and respond to RTP reports of abuse of Requests for Payment. 	CU*Answers does not send to Consumers, but only receives. However, if any inappropriate measures are found, it is best if Credit Unions report any remedial measures that have taken place and document their responses.

H. Sending Requests for Payment (RFP) (applicable if Participant has RFP Sender Customers)

(See Operating Rule VII.B, Minimum Requirements for Requests for Payment Schedule, Permissible Uses for Requests for Payment Rules Interpretation.)

Topic	Relevant Rule	Guidance
32. RFP Warranty Claims Process.	<p><u>Operating Rule VII.C. and RFP Warranty Claims Procedures.</u></p> <p>The RTP Rules establish a process for initiating and responding to RFP warranty claims. The requirements for responding to an RFP warranty claim apply to any RFP Sending Participant. (The requirements for initiating an RFP warranty claim apply to RFP Receiving Participants that choose to use the RFP warranty claims process to attempt to recover funds.)</p> <p>TCH has issued a detailed procedures document (the RFP Warranty Claims Procedures), which is an RTP Technical Specification that further implements the requirements of the RFP warranty claim rule.</p> <p>When an RFP Sending Participant receives a warranty claim, it is required to investigate the claim and respond within 20 business days. The rule prohibits the denial of a claim based solely on the RFP Sending Participant's inability to recover funds from its Customer, the RFP Sender. If the RFP Sending Participant denies the claim, it must provide either (i) a statement as to why RFP warranty was not breached, or (ii) a statement (or other evidence) that the RFP Sender has already provided the RFP Receiver a remedy.</p>	<p>CU*Answers does not send to Consumers, but only receives. Thus, Credit Unions should review The Clearing House's document discussing RFP Warranty Claims Procedures. In doing so, it is most likely a best practice to implement the guidelines set forth in this action. The RFP Warranty Claims Procedure Document is available upon request from The Clearing House. This is not available on the public website and Credit Unions will need to gain access to the document through submitting a request to The Clearing House.</p>

I. Receiving Requests for Payment (applicable to Participants that receive RFPs under the RFP Receive or RFP Send Message Persona)		
Topic	Relevant Rule	Guidance
33. RFP Display Requirements.	<p>RFP Display Requirement (Operating Rule II.F.2)</p> <p>Under RTP Operating Rule II.F.2., a Participant that has implemented the RFP Send or RFP Receive “message persona” is generally required to make available information to its customers from the fields of an RFP message as directed in the RTP Technical Specifications.* There are certain exceptions. Specifically, a Participant is not required to make RFP message information available if: the RFP is suspected to be fraudulent, the RFP violates the Participant’s reasonable standards on offensive or threatening language or unlawful activity, the Customer has opted out of receiving all RFPs or RFPs from that particular RFP Sender, or the Customer is not enrolled in online or mobile banking.</p>	CU*Answers does not send to Consumers, but only receives. For this message persona inquiry, it would most likely be best if the Credit Union does a quality control check on their messaging standards and consults with the RTP Document Library found on The Clearing House website.
34. RFP Warranty Claims Process.	<p>Operating Rule VII.C. and RFP Warranty Claims Procedures.</p> <p>The RTP Rules establish a process for initiating and responding to RFP warranty claims. The requirements for initiating an RFP warranty claim apply to RFP Receiving Participants that choose to use the RFP warranty claims process to attempt to recover funds. (The requirements for responding to an RFP warranty claim apply to any RFP Sending Participant.) TCH has issued a procedures document (the RFP Warranty Claims Procedures), which is an RTP Technical Specification that further implements the requirements of the rule.</p> <p>An RFP Receiving Participant may initiate an RFP warranty claim by sending a RFRF (camt.056) message to the RFP Sending Participant related to the Responding Payment(s) that resulted from the RFP(s) alleged to have breached the warranty and providing other required information. Under RFP warranty claim the rule, the claim must be initiated within 95 calendar days of the Responding Payment and certain information must be provided when initiating the claim. The procedures contemplate use of “Out of Network Messages” (i.e., secure emails using a contact list maintained by TCH) for providing certain required information, as well as optional supplemental information and documentation.</p>	This Relevant Rule is in conjunction with #32, Credit Unions should review The Clearing House’s document discussing RFP Warranty Claims Procedures. This is to further ensure compliance with messaging procedures.

*Note that the RFP Test Persona is an additional message persona that provides a Participant additional discretion to reject (not display) RFPs while the Participant conducts testing and works to implement the RFP Receive or RFP Send message persona. The RTP Persona Specifications is available in the RTP Document Library, <https://www.theclearinghouse.org/payment-systems/rtp/document-library>

J. Payment Service Providers (PSPs)

(See Operating Rule II.H.)

Topic	Relevant Rule	Guidance
35. PSP Customers. Participant must have appropriate risk-based measures that are reasonably designed to prevent a Money Transmitter customer from engaging in unapproved money transmission activity as a Sender. For identified PSPs, Participant must comply with (and as applicable, ensure the PSP complies with) certain application, agreement, audit/certification, and other requirements.	<p><u>Operating Rules I.A.52. Definitions.</u></p> <p>Payment Service Provider or PSP: A Person, other than a payroll processor or an entity that sends and receives payments for corporate affiliates, that (i) is a Money Services Business, as defined in FinCEN's regulations (31 CFR §1010.100), due to its activities as a Money Transmitter, as defined in FinCEN regulations (31 CFR § 1010.100(ff)(5)) and as interpreted by public FinCEN rulings and guidance; and (ii) sends RTP Payments to complete payments between other parties. For the avoidance of doubt, RTP payments that are sent for the purpose of funding a stored balance used as part of a Money Transmitter's service are not RTP payments "between other parties" when the Sender and Receiver of the RTP Payment are the Money Transmitter's customer and the Money Transmitter, respectively. Similarly, RTP Payments that are sent for the purpose of returning funds from a stored balance used as part of a Money Transmitter's service are not RTP payments "between other parties" when the Sender and Receiver of the RTP Payment are the Money Transmitter and Money Transmitter's customer, respectively.</p> <p><u>Operating Rules II.H.5. Prohibition Against Unapproved PSP Activity.</u></p> <ul style="list-style-type: none"> • A Sending Participant must have appropriate, risk-based measures that are reasonably designed to prevent any Customer that is a Money Transmitter, as defined in FinCEN regulations (31 CFR § 1010.100(ff)(5)) and as interpreted by public FinCEN rulings and guidance, from engaging in money transmission activities as a Sender, unless the Customer has been approved by TCH as a PSP and entered into a PSP Agreement with TCH. • A Participant shall be fully responsible and liable to TCH for its failure to have appropriate, risk-based measures that are reasonably designed to prevent unapproved PSPs from engaging as Senders in money transmission activities in the RTP System through such Participant. <p><u>Operating Rules II.H.1-4.</u></p> <p>See Operating Rules II.H.1-4 and the TCH website RTP Library for the PSP application, agreement, audit/certification, and other requirements.</p>	<p>Credit Unions are not a PSP. A PSP is a Payment Service Provider (PSP) that can be a financial institution or a technology company that facilitates electronic transactions between businesses and consumers, enabling secure and efficient payment processing. Major PSPs include PayPal, Stripe, Adyen, and Worldpay. Therefore, this is not applicable for credit unions.</p>