RTP Participant Self-Audit Workbook

Annual Self-Audit Requirement. RTP Participants are required to complete an annual self-audit to verify compliance with the RTP Participation and Operating Rules (RTP Rules), including RTP Rules-Related Schedules and RTP Technical Specifications. Participants must also complete and return the RTP Self-Audit Form to The Clearing House (TCH) to attest that the self-audit has been completed, and that any material findings of non-compliance (as determined by the Participant's audit standards or risk management framework) were reported to the Participant's audit committee or equivalent body responsible for overseeing the Participant's internal controls. TCH does not require this audit to be completed using any specific set of procedures or approach. The audit should be performed using standard auditing procedures and for example, may utilize sampling to review and assess compliance. The audit should be completed by the Participant's internal audit division, audit committee, compliance department, or similar internal division; or by an independent third-party auditor.

When designing and implementing compliance programs and controls for RTP, Participants may wish to consider how they will document and provide evidence of compliance with the RTP Rules for purposes of this self-audit. This may include, for example, establishing policies, processes, and internal metrics (or "SLAs"), as appropriate, that may be considered when evaluating compliance and determining whether a finding of non-compliance is material.

Some Participants may rely on a TPSP or other service provider to support certain aspects of their RTP functionality. However, the Participant is ultimately responsible for its compliance with the RTP Rules. In connection with the self-audit, Participants that rely on TPSPs or other third-party vendors may wish to obtain evidence or information from the third-party regarding compliance with the RTP Rules relevant to the functions the third party performs. For example, a TPSP may audit the TPSP's own systems and processes for compliance with the RTP Rules, as if it were a Participant, and provide Participants with an overall report regarding its compliance.

Self-Audit Workbook. TCH developed this workbook as a resource that Participants may wish to utilize as they design and execute the required RTP self-audit. The workbook identifies key RTP Rules requirements that TCH expects Participants to evaluate in the course of the self-audit. Each numbered item has a short title and summary or "shorthand" description of the relevant RTP Rule or requirement and is accompanied by (i) the full text of such RTP Rule or requirement; and/or (ii) a reference to the document that contains the full text, and for some topics, (iii) supplementary information regarding establishing compliance. The "shorthand" description of each Rule or requirement is not intended to modify or limit the meaning of the RTP Rules, or Participants' obligations under the Rules. **This workbook is not a substitute for a Participant's own review of the RTP Rules and Participants should be aware that the RTP Rules may change from time to time**. The RTP Rules and related documents are available on the TCH website at: https://www.theclearinghouse.org/payment-systems/rtp/document-library**.**

Self-Audit Form. Once a Participant has performed the annual self-audit for a calendar year, it must complete and submit the Self-Audit Form to RTPEnforcement@theclearinghouse.org by March 31 of the following calendar year. See the Self-Audit Form for additional information.

TCH Audit Rights. TCH maintains the right to audit a Participant for compliance with RTP Rules and may request additional documentation or information from a Participant related to its RTP Rules compliance.

Summary of Key Rules Topics to Consider in Self-Audit:

1. **24/7 Operation**
2. **Message Persona**
3. **Payment Status/Message Information**
4. **No Correspondents**
5. **No Fee Netting**
6. **No Searching for Accounts**
7. **No Foreign Payments**
8. **Transaction Limit**
9. **Receiver Name**
10. **Directory Service**
11. **Payment Message Response**
12. **Payment Response Time**
13. **Payment Message Acceptance**
14. **Funds Availability**
15. **Funding Obligation**
16. **Funding**
17. **Non-Funding Participants**
18. **Non-Payment Messages**
19. **Fraud Reporting and Acting on Alerts**
20. **Controlled Access**
21. **Multi-Factor Authentication**
22. **Fraud/Risk Monitoring**
23. **Respond to Reports of Abuse**
24. **OFAC**
25. **Errors/Unauthorized Payments (Cooperation)**
26. **RFR Response**
27. **RFP Due Diligence**
28. **RFP Monitoring**
29. **RFP Investigation**
30. **RFP Corrective Action**
31. **PSP Customers**

Topic	Relevant Rule
A. General Participant Responsibilities *[See Section II of the Operating Rules.]*	
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).	**Technical Specification: RTP Continuous Operations Documentation.** 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****.* 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.

Topic	Relevant Rule
2. Message Capability. Participant must be able to receive and/or send all messages required for its selected message persona.	**Technical Specifications, Business Application Header, pages 15-17.** The RTP message personas are "Receive Payment", "Send Payment", "Receiver RFP" and "Send RFP." Each persona has a set of Mandatory and Optional messages. Refer to the RTP Intralinks site for the Message Persona Specifications. 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.
3. Payment Status/Message Information. Participant must immediately make available payment status information; and all required message information consistent with its message persona.	**Operating Rule II.F. Payment Status & Message Information.** **1. 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. **2. Message Information.** Participants must make available to 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 a. that would violate the Participant's reasonable standards for messaging that prohibit offensive or threatening language or unlawful activity; b. contained in a Payment Message if the Participant has provided a "reject" message in response to the Payment Message; c. contained in a Request for Payment Message, if the Participant's Customer, has elected not to receive (i) Requests for Payment from the Person that initiated the Request for Payment, or (ii) all Requests for Payment; or if the Participant's Customer is not enrolled in online or mobile banking. 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.

Topic	Relevant Rule
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. .	**Operating Rule II.B. No Correspondent Participation.** 1. A Participant may not submit a Payment Message to the RTP System that a. is instructed by a Sender or instructs payment to a Receiver that is a foreign depository institution; b. 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: i. 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; ii. 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; iii. 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 iv. 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. 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 a. 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 b. 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). *See also Summary of RTP Rule Operating Rule Changes Effective January 31, 2021, which provides example scenarios regarding this rule:: https://www.theclearinghouse.org/-/media/new/tch/documents/paymentsystems/summary_changes_rtp_operating_rules_schedules_effective_01-31-21.pdf*

Topic	Relevant Rule
5. No Fee Netting. Participant must not reduce the amount of an RTP Payment to collect fees.	**Operating Rule II.D. No Fee Netting.** 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. *See **RTP Rules Interpretation** available at*: https://www.theclearinghouse.org/payment-systems/rtp/-/media/C7D336BA340849ECB8DC6FCDDA6E1D76.ashx.
6. No Searching for Accounts. Participants may not submit Payments or messages solely to search for active accounts.	**Operating Rule II.E.1. Searching for Accounts.** 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.
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.	**Operating Rule II.E.2. Prohibited Transactions.** **Foreign Payments.** 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.
8. Transaction Limit. Participant must receive RTP payments up to the current maximum transaction limit.	**Operating Rule II.C.2. Eligible Payments.** 2. An RTP Payment may not exceed the general transaction limit of $1,000,000. a. Sending Participants may establish a lower transaction limit for their Senders. b. Receiving Participants may not establish a lower transaction limit for their Receivers.

Topic	Relevant Rule
B. Sending Participant Obligations *[See Section III of the Operating Rules.]*	
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.	**Operating Rule III.C.3. Prerequisites to Sending a Payment Message.** Prior to submitting a Payment Message to the RTP System, a Sending Participant must: 3. 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. 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 a combination of the two) as set forth in the interpretation. *For further detail, see **RTP Rules Interpretation** available at:* https://www.theclearinghouse.org/payment-systems/rtp/-/media/0bbf8e34e214422e8c7d5c19bf0f6b26.ashx
10. Directory Service. Participant using a directory service must ensure compliance.	**Operating Rule III.G. Directory Services.** 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.

Topic	Relevant Rule
C. Receiving Participant Obligations *[See Section V of the Operating Rules.]*	
11. Payment Message Response. Participant must respond correctly to Payment Messages.	**Operating Rule V.E. Receiving Participant Responses to Payment Messages.** **1. Accept** a. 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.... **2. Accept Without Posting** a. 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.... b. A Payment Message accepted without posting is immediately and finally settled as provided in Rule VI(E) of these RTP Operating Rules.... c. 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.... **3. Reject** a. A "reject" message submitted to the RTP System means that the Receiving Participant has rejected the Payment Message.... b. The Receiving Participant must include a valid and most appropriate reason code with the "reject" message as specified in the RTP Technical Specifications. c. Rejected RTP Payments will not be settled.
12. Payment Response Time. Participant must respond to Payment Messages within the required timeframe, as set forth in the RTP Technical Specifications.	**Operating Rule V.A. Immediate Response.** 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 pages 40-42**. **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. Note that for a (pacs.008) Credit Transfer, the RTP system automatically times out and sends a DS24 reject code when the Receiving Participant exceeds the timeline in the Technical Specifications (). Auditors may wish to review DS24 reject counts as a potential means of assessing compliance with this Technical Specification.

Topic	Relevant Rule
13. Payment Message Acceptance. Participant must accept all Payment Messages other than for allowed exceptions.	**Operating Rule V.C. General Acceptance Requirement.** A Receiving Participant agrees to accept all Payment Messages that conform to the RTP Technical Specifications, unless: 1. 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); 2. the owner of an Account has indicated that it does not wish to accept all or certain specified RTP Payments for the 3. the Payment Message cannot be accepted due to legal or regulatory compliance requirements.
14. Funds Availability. Receiving Participant must provide immediate funds availability for an accepted Payment Message.	**Operating Rule V.E.1. Receiving Participant Responses to Payment Messages.** 1. Accept a. 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.... b. 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. **Operating Rule V.B. No Inconsistent Cut-Off Times.** 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. 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.

Topic	Relevant Rule
D. Funding (as applicable based on Participant status as Funding Participant or Non-Funding Participant) *[See Section VI of the Operating Rules VI.]*	
15. Funding Obligations. Participant must satisfy its funding obligations.	**Operating Rule VI.A. Funding Participants.** 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. **Operating Rule VI.B. Non-Funding Participants.** A Non-funding Participant may choose a Funding Agent that uses the Funding Manager or Funding Provider model. A Non-funding Participant that uses a Funding Manager (and has a Current Prefunded Position) is obligated to satisfy its funding obligations (if any) through a Funding Manager and in accordance with the RTP Rules. **Operating Rule III.C.1. Prerequisites to Submitting a Payment Message.** Prior to submitting a Payment Message to the RTP System, a Sending Participant must: 1. Have satisfied its Prefunded Requirement as specified in the RTP Participation Rules and the RTP Operating Rules. **Operating Rule VI.D.2. and VI.D.3.** 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. 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.
16. Funding for RTP Only. Funding Participant must maintain funds in the Prefunded Balance Account to support only its reasonably anticipated RTP needs.	**Operating Rule VI.C.1.e. Prefunded Balance Account.** 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 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.

Topic	Relevant Rule
17. Non-Funding Participants. Non- Funding Participant must have appropriate arrangements with its Funding Agent (Funding Manager model).	**Operating Rule VI.B.2. Funding Agents & Non-funding Participants.** 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.
E. Non-Payment Messages *[See Section VII of the Operating Rules.I]*	
18. Non-Payment Messages. Participant must send Payment- related Message Responses, consistent with its message persona.	**Operating Rule VII.A. Non-Payment Message Types & Responses.** 2. A Message Receiving Participant must transmit any Payment-related Response Message provided by its Customer to the Message Sending Participant. **Technical Specifications, Business Application Header, pages 15-17.** Refer to the RTP Document Library on the TCH website https://www.theclearinghouse.org/payment-systems/rtp/document-library for message persona details on non-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.]*	
19. Fraud Reporting and Acting on Alerts Participant must report fraudulent activity to TCH and the other Participant involved in a Fraudulent RTP Payment	**Operating Rules II.G.1 and II.G.2. Participant Response and Fraud Reporting Obligations** 1. Participants must act on alerts from TCH regarding suspected fraud in connection with the RTP System. 2. Participants must report fraudulent activity involving the RTP System in accordance with the RTP Technical Specifications and Risk Management and Fraud Control Requirements. 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 RTPEnforcement@theclearinghouse.org. (Participants should not send individual RTP Payment information or nonpublic personal information in such reports.) *For further information, see the RTP Rules Interpretation at:* https://www.theclearinghouse.org/payment-systems/rtp/-/media/D8765383FC804BC6A8F5E4CCE2E1BE61.ashx

Topic	Relevant Rule
20. Controlled Access. Participant must properly limit access to equipment used in connection with RTP.	**Risk Management & Fraud Control Requirements Schedule § 7-8.** 7. 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. 8. 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
21. Multi-Factor Authentication (MFA). Participant must use MFA to confirm the Sender's identity.	**Risk Management & Fraud Control Requirements Schedule § 1.** 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. *See also **Operating Rule III.A.1.***
22. Fraud/Risk Monitoring. Participant must perform appropriate fraud/risk monitoring for RTP transactions.	**Risk Management & Fraud Control Requirements Schedule §§ 2-3.** 2. Sending Participants must perform appropriate fraud monitoring prior to submitting a Payment Message to the RTPS. 3. A Participant must regularly review the performance of its fraud monitoring systems and make appropriate updates to address evolving fraud risks. *See also **Operating Rule III.A.2.***
23. Respond to Reports of Abuse. Participant responds to reports of RTP system abuse.	**Risk Management & Fraud Control Requirements Schedule § 6.** 6. 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.
24. OFAC. Participant must have a written OFAC program.	**Operating Rule.II.J. OFAC Compliance Program.** A Participant must have a written OFAC compliance program reasonably designed to promote and monitor compliance with OFAC sanctions programs and regulations. *See also **Operating Rule II.E.2**.*

Topic	Relevant Rule
G. Errors & Unauthorized Payments	
25. Errors/Unauthorized Payments (Cooperation). Participant must cooperate with other Participants and TCH.	**Operating Rule II.I.3. Cooperation among Participants with respect to Unauthorized or Erroneous RTP Payments.** 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.
26. Request for Return of Funds (RFR) Response. Participant must respond to an RFR within the required timeframe.	**Operating Rule VII.C.1-2, 4. Requests for Return of Funds.** 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 … 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. 4. 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.

Topic	Relevant Rule
H. Request for Payment (RFP) (applicable if Participant has RFP Customers) *[See Operating Rule VII.B and Minimum Requirements for Requests For Payment Schedule.]*	
27. RFP Due Diligence. Participant must perform appropriate, risk-based due diligence on RFP-sending Customers.	**Requirements for RFP Customers Schedule § 1.** 1. Implement documented procedures for performing appropriate, risk-based due diligence on a Customer that seeks to initiate Requests for Payment. a. With respect to non-consumer Customers, such procedures must include, at a minimum: i. 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. ii. Documentation of the Customer's legitimate business purpose for sending Requests for Payment. b. 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. c. 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.
28. RFP Monitoring. Participant must monitor Customer RFPs.	**Requirements for RFP Customers Schedule § 2.** 2. Implement documented procedures for monitoring Requests for Payment submitted by a Customer. Such procedures must include, at a minimum, the following d. 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. e. 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. **Operating Rule VII.B.2.a-d. Requirements for RFP Messages.** 2. A Message Sending Participant that submits a Request for Payment to the RTP System must: a. ensure that the Request for Payment complies with the RTP Technical Specifications; b. comply with the Requirements for Request for Payment Customers; c. have a reasonable basis for determining that the Message Sender's RFPs will only be used for Permissible Uses and have made such a determination prior to submitting an RFP for the Message Sender; d. warrant to TCH and the Message Receiving Participant that the Request for Payment is made for a legitimate purpose and is not fraudulent, abusive, or unlawful;

Topic	Relevant Rule
29. RFP Investigation. Participant must investigate reports of fraudulent or abusive RFPs.	**Requirements for RFP Customers Schedule § 3.** 3. 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: ▪ 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.
30. RFP Corrective Action. Participant must take corrective action for inappropriate RFPs and responds to reports of abuse.	**Operating Rule.VII.B.2.e-f. Requirements for RFP Messages.** 2. A Message Sending Participant that submits a Request for Payment to the RTP System must: e. 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 f. respond to RTP reports of abuse of Requests for Payment Note that TCH has issued an RTP Rules interpretation further describing the permissible uses for RFPs and optional, non-exclusive ways a Message Sending Participant may have a reasonable basis for determining that a Message Sender will only use RFPs for one or more permissible uses. *See* ***RTP Rules Interpretation*** *available at*: https://www.theclearinghouse.org/-/media/new/tch/documents/payment-systems/rules_interp_permissible_uses_for_rfp_effective_06-10-2022.pdf.

Topic	Relevant Rule
I. Payment Service Providers (PSPs) *[See Operating Rule II.H.]*	
31. 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.	**Operating Rules.I.A.52. Definitions.** **52. 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. **Operating Rules II.H.5. Prohibition Against Unapproved PSP Activity.** a. 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. b. 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. **Operating Rules II.H.1-4.** See Operating Rules II.H.1-4 and the TCH website RTP Library for the PSP application, agreement, audit/certification, and other requirements.