Issued 9.9.19

RTP Rules Interpretation
Fraud Reporting and Acting on Alerts
RTP Operating Rules II.G.1 and II.G.2

Effective January 1, 2020

This document is issued pursuant to RTP Operating Rule I.C. and describes The Clearing House's expectations regarding compliance with RTP Operating Rules II.G.1 and II.G.2 (and related requirements in Sections 4 and 5 of the Risk Management and Fraud Control Requirements). All capitalized terms have the meanings ascribed to them in the RTP Operating Rules.

Operating Rule II.G.1 (Fraud Alerts)

Operating Rule II.G.1 requires Participants to act on alerts from TCH regarding suspected fraud in connection with the RTP System in accordance with the Risk Management and Fraud Control Requirements.[1] Section 4 of the Risk Management and Fraud Control Requirements further states that "[a] Participant must act on fraud alerts from TCH's fraud-monitoring program by promptly investigating the transaction or activity related to the alert and incorporating alerts related to confirmed fraud into the Participant's standard fraud-detection practices."

TCH may become aware of suspected or confirmed fraud involving the RTP System through its own system monitoring, information reported by Participants pursuant to Operating Rule II.G.2, or other sources. Under such circumstances, TCH may provide notifications at (i) a system level through system bulletins or (ii) an individual Participant level (via communication from a TCH representative) regarding suspected or confirmed fraud or other misuse of the RTP system. System level notifications will contain information that all Participants should be aware of. Participant level notifications will contain information that is specific to the Participant, such as unusual fraud rates or concerns about a particular Customer based on trends TCH has observed in its System monitoring or information that has been reported to TCH by other Participants.

Participants that receive such notifications are expected to take reasonable steps in a timely manner to (i) incorporate the information into existing fraud prevention processes, procedures or programs, and (ii) use the information to take appropriate action with respect to particular Customers, to the extent TCH has provided the notice on an individual Participant level.

In response to inquiries, TCH is issuing this interpretation to clarify that Participants are not required under Operating Rule II.G.1 to make technical changes to their fraud or RTP systems to receive or respond to TCH fraud notices. Rather, Participants are expected to (i) have in place capabilities to

[1] The RTP Risk Management and Fraud Control Requirements are a schedule to the RTP Operating Rules, and describe the minimum level of risk management and fraud control measures that an RTP Participant must employ in connection with the Participant's use of RTP. This schedule can be accessed at https://www.theclearinghouse.org/payment-systems/rtp/-/media/b214d36fb00241e781159989c6056084.ashx.

investigate all RTP fraud alerts relating to transactions or activities involving their institution and (ii) incorporate information from TCH about confirmed fraud into their existing fraud programs. While a Participant's specific approach to incorporating this information into its fraud program may vary based on various factors including the size, complexity, products, systems, and risk profile of a particular Participant, at a minimum The Clearing House expects that each Participant will have procedures (such as having a designated staff member or automated process) to review and consider TCH fraud notices and make a determination about whether additional action is necessary.

Operating Rule II.G.2 (Fraud Reporting)

Operating Rule II.G.2 requires Participants to report fraudulent activity involving the RTP System to TCH and the other Participant involved in a fraudulent RTP Payment in accordance with the RTP Technical Specifications and Risk Management and Fraud Control Requirements. Section 5 of the Risk Management and Fraud Control Requirements further states that "[a] Participant must report any instance of fraudulent activity or suspected fraudulent activity to TCH subject to and in accordance with the RTP Operating Rules and other procedures established by TCH from time to time."

This interpretation establishes the current reporting requirements that Participants must follow in order to be in compliance with Operating Rule II.G.2. For purposes of this interpretation, "fraudulent RTP Payment" means a Payment that the Sending Participant has determined was not authorized by the Sender ("Unauthorized Payment") based on the Participant's investigation of the means by which the Payment was instructed to the Participant. For clarity, a Payment that the Sender authorized but which the Sender was induced to send under false pretenses is not an Unauthorized Payment.

To comply with Operating Rule II.G.2., each Participant must:

1. Report an Unauthorized Payment to the Receiving Participant that received the Unauthorized Payment by sending a Request for Return of Funds message (camt.056) with the "FRAD" reason code. Sending such a message satisfies both the Participant's obligation to report the fraudulent activity to TCH and to the relevant Participant. The FRAD code must not be used in a Request for Return of Funds message unless the Sending Participant has determined that a Payment is an Unauthorized Payment. For Payments that a Sender claims were made under false pretenses, the CUST code must be used. If the Sending Participant sent a previous Request for Return of Funds for a Payment that the Participant later determines is an Unauthorized Payment, it must send another Request for Return of Funds with the FRAD code. The Sending Participant should follow any guidelines that TCH has established for sending multiple Request for Return of Funds messages for a single Payment.

2. Report material findings regarding (i) Unauthorized Payments or (ii) authorized Payments that were sent in response to a Request for Payment that the Sender claims was deceptive or misleading (Potential Fraudulent RFP) via email to RTPEnforcement@theclearinghouse.org. Material findings regarding Unauthorized Payments or authorized Payments in response to Potential Fraudulent RFPs means any of the following developments that a Participant would reasonably believe merit TCH's attention as the system operator: (i) an increase in the level, nature or frequency of Unauthorized Payments or authorized Payments in response to Potential Fraudulent RFPs; (ii) persistent threats that may result in Unauthorized Payments or authorized Payments in response to Potential Fraudulent RFPs; or (iii) other fraud-related developments (e.g., new phishing schemes that target authentication of RTP Payments). Participants should

not submit specific, individual RTP Payment information or nonpublic personal information (as defined in the Gramm-Leach-Bliley Act and Regulation P) or other information that identifies an affected Customer in such reports.

Compliance with Operating Rule II.G.2 does not require a Participant to adopt new technological capabilities in order to detect Unauthorized Payments or authorized Payments in response to Potential Fraudulent RFPs or identify material findings.