Requirements for Request for Payment Customers

This document describes the due diligence and monitoring requirements applicable to Participants that TCH has approved and authorized to submit Requests for Payment. In addition to all other applicable RTPS requirements, such a Participant must:

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.

2. Implement documented procedures for monitoring Requests for Payment submitted by a Customer. Such procedures must include, at a minimum, the following:

    a. 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.

    b. 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.

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 Receiver as threatening or intimidating.

- The origination of repeated Requests for Payment to the same Customer of the Message Receiver within a timeframe that could be reasonably perceived by that Customer as harassing.

4. Retain the right to suspend a Customer's ability to initiate Requests for Payment immediately upon the Participant's determination that the Customer is misusing Requests for Payment or at TCH's direction.