PSP Compliance Criteria Schedule

To the extent a PSP is subject to the application requirement set forth in the RTP Operating Rules, it shall, at all times and in connection with all RTP Payments, comply with the following PSP Compliance Criteria. Except as otherwise provided herein, where any criterion identifies a specific statute and/or regulation that applies to "financial institutions," the PSP shall be required to satisfy the obligations of a "financial institution" under such statute and/or regulation whether or not the PSP actually constitutes a "financial institution" thereunder.

1. Customer Protections

    a. EFTA and Regulation E. To the extent a PSP is providing Money Transmission Transactions for Consumers, the PSP must, at all times, comply with applicable Consumer protection requirements of the Electronic Fund Transfer Act and Subpart A of Regulation E.

    b. Prohibition on UDAAPs. The PSP shall not engage in or commit any unfair, deceptive, or abusive acts or practices under federal or state law in connection with any EFT for or on behalf of a Consumer through the RTP System.

    c. Pass-Through Insurance Disclosure. The PSP shall disclose to customers whether the customers' funds are covered by pass-through insurance by the Federal Deposit Insurance Corporation or through a similar government-sponsored insurance arrangement when such funds are in the PSP's possession.

2. Prudential Requirements (Safety and Soundness) – Interagency Guidelines Establishing Standards for Safety and Soundness

    a. Surety Bond Requirement. The PSP shall establish and maintain an excess coverage surety bond that will apply in the event of a failure by the PSP to fulfill its obligations. The amount of the bond must be equal to or greater than the difference between the aggregate amount of all surety bonds held by the PSP pursuant to state laws governing money transmission, and the average daily money transmission volume of the PSP (inclusive of volume processed through the RTP System) during the prior calendar year. For newly operating PSPs, the amount of the bond must be equal to or greater than the difference between the aggregate of all surety bonds held by the PSP pursuant to state laws governing money transmission, and the PSP's anticipated average daily money transmission volume (inclusive of volume processed through the RTP system) during the PSP's first full calendar year of operation as a money transmitter. The required bond amount must be re-assessed and, if necessary, adjusted annually. TCH reserves the right to require a higher bond based on TCH's assessment of the risk of loss due to the activities of the PSP.

b. Error Resolution Reserve Requirement. The PSP shall establish and maintain, at all times, a reserve of funds for satisfying its error resolution obligations under these PSP Compliance Criteria. The amount of funds in the error resolution reserve shall be no less than the aggregate amount of reimbursements made by the PSP to customers pursuant to its error resolution obligations under these PSP Compliance Criteria during the immediately preceding calendar quarter. The initial amount of funds to be held in reserve will be determined by TCH, in its sole discretion, based upon anticipated volumes of the PSP.

c. Tangible Shareholder Equity Requirement. The PSP shall, at all times, maintain tangible shareholder's equity of not less than $500,000.

d. Permissible Investments Requirement. The PSP shall maintain permissible investments in an amount of not less than the face value of all outstanding obligations of the PSP to customers plus the amount of the PSP's error resolution reserve.

e. Internal Controls and Information Systems. The PSP shall have internal controls and information systems that are appropriate to the size of the PSP and the nature, scope, and risk of the PSP's activities. Such internal controls and information systems shall, at a minimum, provide for clear lines of authority, monitoring of the PSP's adherence to established policies, effective risk assessment, timely and accurate reporting, and compliance with Applicable Law and these PSP Compliance Criteria. Among the PSP's internal controls shall be a business continuity and disaster recovery plan that is reasonably designed to avoid interruption or unavailability of the PSP's services, as well as policies and procedures designed to limit and track employee access to customer and transaction information.

f. Internal Audit System. The PSP shall have an internal audit system that is appropriate to the size of the PSP and the nature, scope, and risk of the PSP's activities. The internal audit system shall, at a minimum, provide for adequate monitoring of the system of internal controls, independence and objectivity, adequate testing and review, adequate documentation, verification and review of management actions, and review by the PSP's board of directors.

g. Risk Mitigation Controls. The PSP shall maintain safeguards to prevent the PSP from engaging in acts or practices that could lead to material financial loss to the PSP.

h. Prohibition of Foreign Transactions. The PSP shall ensure that all senders and all recipients of the payments facilitated by the PSP using the RTP System are (i) residents of or otherwise domiciled in the United States of America, and (ii) not engaged in the further transmission of such funds.

3. Anti-Money Laundering and Anti-Terrorist Financing Requirements

   a. General. The PSP shall establish and maintain procedures reasonably designed to assure and monitor the PSP's compliance with the BSA. The PSP shall also have a written OFAC compliance program reasonably designed to promote and monitor compliance with OFAC sanctions programs and regulations. The PSP shall develop and provide for the continued administration of a program reasonably designed to assure and monitor compliance with the BSA and compliance with OFAC sanctions and restrictions. The compliance program must be written, approved by the PSP's board of directors, and reflected in the minutes of the PSP.

   b. AML Program. The PSP shall develop, implement, and maintain an AML program that is reasonably designed to prevent the PSP from being used to facilitate money laundering and to finance terrorist activities. The AML program shall be commensurate with the risks posed by the location and size of, and the nature and volume of the financial services provided by, the PSP. The AML program shall include a customer identification program and a system of internal controls to assure ongoing compliance and independent testing for compliance.

   c. Record Retention. The PSP shall retain all records required by the BSA, and such records shall be maintained pursuant to the corresponding timing and format requirements set forth thereunder.

   d. Information Sharing. The PSP shall comply with all information sharing requirements pursuant to the BSA, including with regard to record searches, reporting to FinCEN, designation of a contact, and limitations on the use of an information request.

4. Data Security and Privacy – Interagency Guidelines Establishing Information Security Standards and OCC Bulletin 2011-26

   a. Authentication. The PSP shall establish multifactor authentication, and implement a layered security program that includes fraud detection and monitoring and other effective controls. The layered security program shall include, at a minimum, processes designed to detect anomalies and effectively respond to suspicious or anomalous activity related to the initial login and authentication of a customer and the initiation of EFTs to third parties. For business accounts, the layered security program shall include enhanced controls for system administrators.

   b. Information Security Program. The PSP shall develop and implement an information security program that satisfies the following requirements:

      i. *Safeguarding Customer Information*. The PSP shall develop and implement administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information, as well as to ensure the

proper disposal of customer information. The PSP shall implement a comprehensive written information security program that includes such safeguards and that is appropriate to the size and complexity of the PSP and the nature and scope of the PSP's activities.

ii. *Use of Third Parties or Technology*. The PSP shall not use, and shall prohibit the use of, any third party or technology, including any robot, to access an Account at a Participant; provided, that this restriction shall not apply with regard to any third party or technology expressly authorized pursuant to a direct agreement with a Sending Participant responsible for initiating a Payment Message to the RTP System. The PSP shall prohibit the use of, and shall develop and implement safeguards to prevent the use of, any third party or technology, including any robot, to access a customer's account with the PSP to initiate a transfer, any part of which is or will be processed through the RTP System.

iii. *Board of Directors*. The PSP's board of directors, or a designated committee thereof, must approve the PSP's written information security program and oversee the development, implementation, and maintenance of such program.

iv. *Risk Assessment*. The PSP shall identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems. The PSP shall assess the likelihood and potential damage of these threats and shall consider the sensitivity of customer information, as well as the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control such risks.

v. *Risk Management and Control*. The PSP shall design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the PSP's activities. The PSP also shall train its staff to implement the information security program, and regularly test the key controls, systems, and procedures of the system.

vi. *Service Provider Oversight*. The PSP shall exercise appropriate due diligence in selecting its service providers, require any such service providers, by contract, to implement appropriate measures designed to meet the objectives of the PSP's information security program, and monitor such service providers to ensure compliance.

vii. *Updating the Program*. The PSP shall monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the PSP's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems.

viii. *Reporting to the Board*. The PSP shall report to its board of directors or an appropriate committee thereof at least annually to describe the overall status of the information security program, as well as the PSP's compliance with these PSP Compliance Criteria. The report shall discuss material matters related to the information security program and shall address any issues, including risk assessment, risk management and control decisions, service provider arrangements, testing results, security breaches or violations and management's responses, and recommendations for changes in the information security program.

ix. *Response Program*. The PSP shall develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems that is appropriate to the size and complexity of the PSP and the nature and scope of the PSP's activities. The response program shall, at a minimum, include procedures requiring the PSP to assess the nature and scope of an incident, notify appropriate regulatory and law enforcement authorities as necessary, take appropriate steps to contain and control the incident, and notify customers when warranted.

c. Update. The PSP shall perform periodic risk assessments and adjust its customer authentication controls, as appropriate, in response to new threats. The PSP shall implement more robust controls as the risk level of the transaction increases.

d. Consumer Financial Privacy. To the extent a PSP is providing services for Consumers, the PSP shall provide notices to Consumers about the PSP's privacy policies and practices, including an initial notice to Consumers and an annual notice to the PSP's customers. The PSP shall comply with all applicable data privacy laws and regulations, and shall permit Consumers to opt out of sharing information with non-affiliated third parties.