RTP Operator – Customer Information Security Standards

The Clearing House (TCH) as RTP Operator shall take the following measures designed to (i) ensure the security and confidentiality of nonpublic personal information, as defined in the Interagency Guidelines Establishing Information Security Standards, of a customer of a Participant obtained by TCH as a result of its processing any Payment Message, Payment Message Response, or Non-Payment Message ("Customer Information"); (ii) protect against any anticipated threats or hazards to the security or integrity of Customer Information, (iii) protect against unauthorized access or use of Customer Information that could result in substantial harm to a Participant's customer, and (iv) ensure the proper disposal of such information, and to address incidents of unauthorized access to the Participant's Customer Information, including notification to the Participant as soon as possible of any such incident, to enable the Participant to expeditiously implement its response program:

1. Information Security Program

(a) TCH shall maintain and implement a written information-security program that will, at a minimum contain the following elements:

(1) Physical access to computer equipment, storage media (including electrical, optical, and physical media), and other aspects of the system that would permit access to customer information shall be restricted to properly authorized individuals, 24 hours per day, 7 days per week.

(2) Logical access to programs, data, or any other aspect of the system that would permit access to Customer Information shall be limited to authorized individuals and TCH will use a change control process to ensure that access to Customer Information is controlled and recorded.

(3) TCH shall destroy Customer Information in accordance with its record retention policy.

(b) The information-security program shall describe the following features as applicable:

(1) the detail of the system architecture of all environments, including, as applicable, the logical topology of routers, switches, Internet firewalls, management or monitoring firewalls, servers (web, application, and database), intrusion detection systems, network and platform redundancy;

(2) the specifications of the firewalls in use;

(3) the intrusion-detection system environment and the security breach and event escalation process;

(4) the change-management process for automated systems used to provide services;

(5) the business and technical disaster recovery management process;

(6) the management and staff positions that perform administrative functions on servers,

firewalls, or other devices within the application and network infrastructure;

(7) each logon process to be followed by Participants to obtain access to services;

(8) policies, procedures, and controls used to protect Customer Information when it is in printed or other perceptible forms;

(9) operating system security controls and configurations;

(10) technology and usage of encryption for protecting Customer Information, including passwords and authentication information, during transit and in all forms and locations;

(11) services, tools and connectivity required to manage the application and network environment;

(12) arrangements for physical security;

(13) privacy and security policies;

(14) location of servers; and

(15) security of Customer Information held at TCH's service providers, to the extent such service providers have access to customer information.

(c) TCH will permit a Participant to inspect this information security program in accordance with RTP Operating Rule IX.A.3 (Participant Audit Rights and Vendor Management).

(d) TCH shall provide for regular audits of the controls related to the information-security program by independent auditors (*e.g.,* SOC-1 audits). A copy of the audit report shall be provided to each Participant upon request.

(e) TCH shall permit inspection by appropriate federal and state bank supervisory agencies.

(f) TCH shall review the effectiveness of its information-security program and report its findings to its board of directors at least annually. Such review may be based upon and made in conjunction with the reports of independent auditors or bank supervisors as provided in paragraphs d and e of this section.

(g) If necessary, TCH shall make commercially reasonable changes or modifications to its information-security program to remediate any findings determined through the processes of (d)-(f) above.

2. Detection of Security Breaches

(a) TCH shall monitor its system and its procedures for security breaches, violations, and suspicious activity, including suspicious external activity (including unauthorized probes, scans, or break-in attempts) and suspicious internal activity (including unauthorized system administrator access, unauthorized changes to its system or network, system or network

misuse, or theft or mishandling of customer information).

(b) TCH shall permit a Participant to inspect its physical system equipment, operational environment, and customer information handling procedures in accordance with RTP Operating Rule IX.A.3 (Participant Audit Rights and Vendor Management).

(c) TCH shall notify a Participant if TCH determines that Customer Information about a Participant's customer has been compromised due to a breach of security. Such notification shall be made to the Participant's designated contact for such events and shall be made promptly, but in no event more than 24-hours after TCH's determination of the compromise.

(d) TCH shall monitor industry-standard information channels for newly identified system vulnerabilities regarding the technologies and services (including application software, databases, servers, firewalls, routers and switches, hubs, etc.) and fix or patch any identified security problem as soon as commercially reasonable, based on TCH's determination of the severity level of the security problem.

3. Contingency Plans

(a) TCH shall maintain and implement appropriate plans to assure its continued operation. These plans shall include the following: recovery strategy, documented recovery plans covering all areas of operations necessary to delivering services as required by the RTP Operating Rules, vital records protection, and testing plans. The plans shall provide for backup of critical data files, Customer Information, application software, documentation, forms and supplies. The recovery strategy shall provide for recovery after both short and long term disruptions in facilities, environmental support, and data processing equipment. Subject to TCH's right to terminate or suspend a Participant under RTP Participation Rule VIII, TCH shall continue to provide service to a Participant if the Participant activates its contingency plan or moves to an interim site to conduct its business, including during tests of the Participant's contingency operations plans.

(b) TCH's contingency plans for disruptions in facilities, environmental support, and data processing equipment shall provide the ability to bring any impacted operations that are necessary to delivering services as required by the RTP Operating Rules up to full capacity at its back-up site within 60 minutes of a declared disaster.

(c) TCH shall provide to a Participant upon request copies of all contingency exercise final reports in accordance with RTP Operating Rule IX.A.3 (Participant Audit Rights and Vendor Management). If requested, TCH shall allow a Participant, at its own expense, to observe a contingency test.

(d) TCH shall participate in a Participant's data center's exercise to validate recovery connectivity, if requested and upon reimbursement of any expenses incurred by TCH.

4. Background Checks

TCH shall maintain and implement a written procedure that will contain background checks requirements for employees and contractors with access to Customer Information.