

The Clearing House Payments Company L.L.C.

Report on The Clearing House Payments Company L.L.C.'s Description of its Electronic Payments Network (EPN), Clearing House Interbank Payments System (CHIPS), Image Exchange Network (IXN), and RTP® Services System and on the Suitability of the Design and Operating Effectiveness of its Controls Relevant to Security and Availability

SOC 2® Type 2 Report

For the period November 1, 2019 to October 31, 2020

Contents

| | | |
|-------------|--|----|
| Section I | Independent Service Auditor's Report..... | 1 |
| Section II | The Clearing House Payments Company L.L.C.'s Assertion..... | 6 |
| Section III | The Clearing House Payments Company L.L.C.'s Description of its EPN, CHIPS, IXN, and RTP® Services System..... | 9 |
| | Overview of company and services..... | 10 |
| | Company background | 10 |
| | Scope of the report | 11 |
| | Principal service commitments and system requirements..... | 12 |
| | Disclosure of known incidents..... | 13 |
| | Components of the system | 14 |
| | Infrastructure..... | 14 |
| | Software..... | 19 |
| | People | 21 |
| | Procedures | 24 |
| | Data..... | 40 |
| | System boundary | 43 |
| | Relevant aspects of the control environment, risk assessment, control activities, monitoring, and information and communication | 44 |
| | Control environment | 44 |
| | Risk assessment | 45 |
| | Control activities..... | 45 |
| | Monitoring..... | 46 |
| | Information and communication | 48 |
| | Complementary subservice organization controls | 50 |
| | Complementary user entity controls..... | 52 |
| Section IV | Trust services criteria and The Clearing House Payments Company L.L.C.'s related controls, and KPMG LLP's test procedures and results | 53 |

| | |
|---|-----|
| Completeness and accuracy of information produced by the entity | 54 |
| AICPA trust services categories..... | 55 |
| CC 1.0 – Common criteria related to control environment | 56 |
| CC 2.0 – Common criteria related to communication and information..... | 70 |
| CC 3.0 – Common criteria related to risk assessment | 90 |
| CC 4.0 – Common criteria related to monitoring activities | 106 |
| CC 5.0 – Common criteria related to control activities | 115 |
| CC 6.0 – Common criteria related to logical and physical access..... | 123 |
| CC 7.0 – Common criteria related to system operations..... | 182 |
| CC 8.0 – Common criteria related to change management..... | 204 |
| CC 9.0 – Common criteria related to risk mitigation | 220 |
| Additional criteria for availability | 225 |
| Section V Other information provided by The Clearing House Payments Company L.L.C. | 236 |
| Management responses to exceptions | 237 |

Section I Independent Service Auditor's Report



KPMG LLP
345 Park Avenue
New York, NY 10154-0102

Independent Service Auditor's Report

Board of Directors of The Clearing House Payments Company L.L.C.:

Scope

We have examined The Clearing House Payments Company L.L.C.'s accompanying description of its system titled "The Clearing House Payments Company L.L.C.'s Description of its EPN, CHIPS, IXN and RTP® Services System" throughout the period November 1, 2019 to October 31, 2020, ("description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout the period November 1, 2019 to October 31, 2020 to provide reasonable assurance that The Clearing House Payments Company L.L.C.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The information included in Section V, "Other Information Provided by The Clearing House Payments Company L.L.C.", is presented by management of The Clearing House Payments Company L.L.C. to provide additional information and is not a part of The Clearing House Payments Company L.L.C.'s description. Information about The Clearing House Payments Company L.L.C.'s management's responses to exceptions has not been subjected to the procedures applied in the examination of the description and of the suitability of the design and operating effectiveness of controls to achieve The Clearing House Payments Company L.L.C.'s service commitments and system requirements based on the applicable trust services criteria, and accordingly, we express no opinion on it.

The Clearing House Payments Company L.L.C. uses subservice organizations to provide a data center facility, services for initial network access for transmissions between The Clearing House Payments Company L.L.C. and its customers via the internet, and a private Multiprotocol Label Switching (MPLS) network (Dual Carriers) for communications between The Clearing House Payments Company L.L.C. and its customers. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at The Clearing House Payments Company L.L.C., to achieve The Clearing House Payments Company L.L.C.'s service commitments and system requirements based on the applicable trust services criteria. The description presents The Clearing House Payments Company L.L.C.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of The Clearing House Payments Company L.L.C.'s controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at The Clearing House Payments Company L.L.C., to achieve The Clearing House Payments Company L.L.C.'s service commitments and system requirements based on the applicable trust services criteria. The description presents The Clearing House Payments Company L.L.C.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of The Clearing House Payments Company L.L.C.'s controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.



Service organization's responsibilities

The Clearing House Payments Company L.L.C. is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that The Clearing House Payments Company L.L.C.'s service commitments and system requirements were achieved. The Clearing House Payments Company L.L.C. has provided the accompanying assertion titled "The Clearing House Payments Company L.L.C.'s Assertion" ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. The Clearing House Payments Company L.L.C. is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service auditor's responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of CPAs (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization would achieve its service commitments and system requirements based on the applicable trust services criteria if those controls operated effectively
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.



Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that each individual report user may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are listed in Section IV.

Opinion

In our opinion, in all material respects,

- a. The description presents The Clearing House Payments Company L.L.C.'s EPN, CHIPS, IXN and RTP® Services System that was designed and implemented throughout the period November 1, 2019 to October 31, 2020 in accordance with the description criteria.
- b. The controls stated in the description were suitably designed throughout the period November 1, 2019 to October 31, 2020 to provide reasonable assurance that The Clearing House Payments Company L.L.C.'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organizations and user entities applied the complementary controls assumed in the design of The Clearing House Payments Company L.L.C.'s controls throughout that period.
- c. The controls stated in the description operated effectively throughout the period November 1, 2019 to October 31, 2020 to provide reasonable assurance that The Clearing House Payments Company L.L.C.'s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of The Clearing House Payments Company L.L.C.'s controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of The Clearing House Payments Company L.L.C., user entities of The Clearing House Payments Company L.L.C.'s EPN, CHIPS, IXN and RTP® Services System during some or all of the period November 1, 2019 to October 31, 2020, business partners of The Clearing House Payments Company L.L.C. that were subject to risks arising from interactions with The Clearing House Payments Company L.L.C.'s EPN, CHIPS, IXN and RTP® Services System, and practitioners providing services to such user entities and business partners, who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties



- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be and should not be used by anyone other than these specified parties.

KPMG LLP

April 30, 2021
New York, New York

Section II The Clearing House Payments Company L.L.C.'s Assertion



The Clearing House Payments Company L.L.C.'s Assertion

We have prepared the accompanying description of The Clearing House Payments Company L.L.C.'s system titled "The Clearing House Payments Company L.L.C.'s Description of its EPN, CHIPS, IXN and RTP® Services System" throughout the period November 1, 2019 to October 31, 2020 ("description"), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria"). The description is intended to provide report users with information about the EPN, CHIPS, IXN and RTP® Services System that may be useful when assessing the risks arising from interactions with The Clearing House Payments Company L.L.C.'s system, particularly information about system controls that The Clearing House Payments Company L.L.C. has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

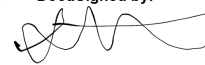
The Clearing House Company L.L.C. uses subservice organizations to provide a data center facility, services for initial network access for transmission between The Clearing House Payments Company L.L.C. and its customers via the internet, and a private Multiprotocol Label Switching (MPLS) network (Dual Carriers) for communications between The Clearing House Payments Company L.L.C. and its customers. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at The Clearing House Payments Company L.L.C., to achieve The Clearing House Payments Company L.L.C.'s service commitments and system requirements based on the applicable trust services criteria. The description presents The Clearing House Payments Company L.L.C.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of The Clearing House Payments Company L.L.C.'s controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at The Clearing House Payments Company L.L.C., to achieve The Clearing House Payments Company L.L.C.'s service commitments and system requirements based on the applicable trust services criteria. The description presents The Clearing House Payments Company L.L.C.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of The Clearing House Payments Company L.L.C.'s controls.



We confirm, to the best of our knowledge and belief, that:

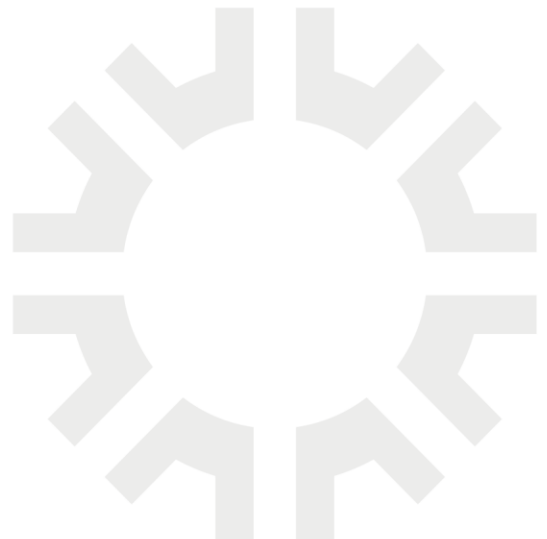
- a. The description presents The Clearing House Payments Company L.L.C.'s EPN, CHIPS, IXN and RTP[®] Services System that was designed and implemented throughout the period November 1, 2019 to October 31, 2020 in accordance with the description criteria.
- b. The controls stated in the description were suitably designed throughout the period November 1, 2019 to October 31, 2020 to provide reasonable assurance that The Clearing House Payments Company L.L.C.'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of The Clearing House Payments Company L.L.C.'s controls throughout that period.
- c. The controls stated in the description operated effectively throughout the period November 1, 2019 to October 31, 2020, to provide reasonable assurance that The Clearing House Payments Company L.L.C.'s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of The Clearing House Payments Company L.L.C.'s controls, operated effectively throughout that period.

DocuSigned by:

E6AA2C6B9C2647D...

Lee Alexander

EVP & CIO

April 30, 2021



Section III The Clearing House Payments Company L.L.C.'s Description of its EPN, CHIPS, IXN, and RTP[®] Services System

Overview of company and services

Company background

The Clearing House Payments Company L.L.C. is an affiliate of The Clearing House Association L.L.C. (formerly named The New York Clearing House Association L.L.C., which was the successor to The New York Clearing House Association, an unincorporated association that was established in 1853 as the center for the exchange of checks and coupons and settlement among its member banks.) Fifty two banks participated in the first exchange, during which checks worth \$22.6 million were exchanged manually.

In March 1998, The New York Clearing House Association converted into a limited liability company named The New York Clearing House Association L.L.C. (The Clearing House) and restructured to reflect the different services offered to the banking institutions. From 1998 through 2004, The Clearing House reorganized its organization structure to reflect the services provided.

In 2004, The Clearing House formed an affiliate, The Clearing House Payments Company L.L.C. (TCH) to provide U.S. dollar clearing and settlement and related services. Payment services include paper, paper to electronic, and Automated Clearing House and wire electronic payments.

The followings are key services/products provided by TCH:

Electronic Payments Network (EPN) – an automated clearing house, i.e., a computerized, batch processing funds transfer system that processes domestic and international consumer and commercial financial transactions among depository institutions.

Clearing House Interbank Payments System (CHIPS) – a computerized funds transfer system for domestic and international banking transactions in U.S. dollars.

Image Exchange Network (IXN) – a computerized check settlement system that streamlines the check image exchange, clearing, collection and return process system enabling the secure exchange of digital check images between financial institutions. IXN provides check image exchange between Financial Institutions (FIs) and third-party processors acting on behalf of FIs and settlement processing through the Federal Reserve Bank of New York (FRBNY).

RTP® – RTP® (RTP) enables Participants to initiate credit transfers, receive final and irrevocable settlement for credit transfers, and make available to Receivers funds associated with such credit transfers in real-time. The system also enables Participants to initiate and/or receive non-payment messages associated with payments. Both the credit transfer and non-payments messages can be sent/received twenty-four (24) hours a day, seven (7) days a week, fifty-two (52) weeks a year. The Clearing House launched RTP® in November 2017.

Secure Token Exchange (STE) – The Secure Token Exchange Hosted Vault and Authentication Service is a multi-network, multi-issuer solution that implements the EMVCo specification with network integration while providing additional value-added services that enhance the safety and soundness of the payments ecosystem.

Today, TCH is a private sector, global payment systems infrastructure that clears and settles approximately \$1.66 trillion per day. It also serves as an industry forum addressing strategic and regulatory issues around U.S. payments.

Management of TCH is under the direction of two boards of directors: the Supervisory Board of Directors and the Managing Board of Directors (“PayCo Board”). The Supervisory Board of Directors has overall responsibility for the business of TCH and for setting the strategic agenda, while the Managing Board of Directors, which reports to the Supervisory Board of Directors, is responsible for oversight of TCH’s business and financial performance, risk management and compliance with supervisory expectations.

The following general description of operations provided by TCH is intended to give readers an overview of certain features and relevant controls related to EPN, CHIPS, IXN and RTP. STE is not in the scope of this report. Each system supports computerized funds transfer of domestic consumer and commercial, treasury and settlement transactions among financial institutions. This report should not be used to interpret EPN, CHIPS, IXN, and RTP Operating Rules or Agreements in relation to the legal obligations between EPN, CHIPS, IXN, and RTP customers, respectively, and TCH.

Scope of the report

This report has been prepared to provide information on The Clearing House Payments Company L.L.C. controls in areas that may be relevant in assessing the internal system controls for security and availability for EPN, CHIPS, IXN, and RTP clients of The Clearing House Payments Company L.L.C. This report covers The Clearing House Payments Company L.L.C.’s EPN, CHIPS, IXN, and RTP Services system. The scope is further outlined in the table below.

Some control activities follow common processes and are considered homogenous for the purposes of this report. Common process areas include aspects of Logical Access and Network, Computer Operations, Environmental Control Systems, HR, Systems Development and Maintenance, Operating System, System Software and Infrastructure Change Management, and Physical Access.

The scope of this report covers the security and availability categories.

| Application | Operating system | Database | Location where hosted | Categories covered |
|-------------|---------------------------------------|--------------------------|-----------------------------|--|
| EPN | Unisys ClearPath Libra | Unisys DMSII | North Carolina/Pennsylvania | Security – Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity’s ability to achieve its objectives. |
| EPNAccess | Windows Server | SQL Server | North Carolina/Pennsylvania | |
| CHIPS | Unisys ClearPath Libra | Unisys DMSII | North Carolina/Pennsylvania | |
| CHIPSWeb | Windows Server | SQL Server | North Carolina/Pennsylvania | |
| IXN | Windows Server/Unisys ClearPath Libra | Unisys DMSII /SQL Server | North Carolina/Pennsylvania | Availability – Information and systems are available for operation and use to meet the entity’s objectives. |
| SVPCOView | Windows Server | SQL Server | North Carolina/Pennsylvania | |

| Application | Operating system | Database | Location where hosted | Categories covered |
|-------------|---|----------|-----------------------------|--------------------|
| RTP | Red Hat Enterprise Linux (RHEL), and IBM AIX Unix | IBM DB2 | North Carolina/Pennsylvania | |

It should be noted that TCH alternates the EPN, CHIPS and IXN applications, and RTP components between data centers on a recurring basis each year to demonstrate a readiness stance for a disaster recovery situation.

Principal service commitments and system requirements

TCH designs its processes and procedures related to EPN, CHIPS, IXN, and RTP to meet its objectives for its services. Those objectives are based on the service commitments that TCH makes to user entities, the laws and regulations that govern the provision of EPN, CHIPS, IXN, and RTP Services, and the financial, operational, and compliance requirements that TCH has established for the services. The services of TCH are subject to the principal security and availability service commitments in TCH contracts and operating rules, as follows:

EPN

- TCH as a result of a Participant's use of the Network ("Customer Information"); protects against anticipated threats or hazards to the security of Customer Information, protects against unauthorized access or use of Customer Information that could result in harm to a Customer, and addresses incidents of unauthorized access to Customer Information, including notification to the Participant of any such incident, to enable the Participant to implement its response program.
- Availability commitments to user entities are documented and communicated in TCH's EPN Membership and Operating Rules. The Clearing House's responsibilities include the following:
 - (a) The main processing platform for EPN will be available at a monthly level of 99.9% during EPN's published operating hours.
 - (b) TCH will ensure that the availability of ACH output files will be at an annual rate of no less than 99.5% in accordance with EPN's published file output schedule. The performance calculation is based on the number of missed deliveries divided by the total number of deliveries in any given month.
 - (c) In an emergency, if it becomes necessary to relocate EPN's processing operations to a contingency center, a transfer will take place.
 - (d) TCH operations support services are available to Participating Depository Financial Institutions (DFIs) 24 hours a day, 7 days a week.

CHIPS

- TCH as a result of a Participant's use of the Network ("Customer Information"); protects against anticipated threats or hazards to the security of Customer Information, protects against unauthorized access or use of Customer Information that could result in harm to a Customer, and addresses incidents of unauthorized access to Customer Information, including notification to the Participant of any such incident, to enable the Participant to implement its response program.

IXN

- TCH as a result of a Participant's use of the Network ("Customer Information"); protects against anticipated threats or hazards to the security of Customer Information, protects against unauthorized access or use of Customer Information that could result in harm to a Customer, and addresses incidents of unauthorized access to Customer Information, including notification to the Participant of any such incident, to enable the Participant to implement its response program.

RTP

- TCH as a result of a processing Payment Message, Payment Message Response, or Non-Payment Message ("Customer Information"); protects against anticipated threats or hazards to the security of Customer Information, protects against unauthorized access or use of Customer Information that could result in harm to a Participant's Customer, and ensures the proper disposal of such information, and addresses incidents of unauthorized access to Participant's Customer Information, including notification to the Participant of any such incident, to enable the Participant to implement its response program.

All Services

- TCH provides support to its customers through the Customer Services, Client Services and Payment Specialist departments. In addition, personnel in the Network Operations Center are available to support customers during business hours as well as after business hours (24 x 7).
- TCH provides systems which include load balancing and redundancy as well as disaster recovery infrastructure to meet defined recovery time objectives and recovery point objectives.
- TCH monitors its systems for network and system availability as well as utilization and capacity thresholds.

Security and availability commitments to user entities are documented and communicated via various methods including in customer and service agreements, as well as in the description of the service offerings provided online. TCH establishes operational requirements that support the achievement of security and availability commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in TCH's system policies and procedures, and system design documentation. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. System requirements for availability include redundant infrastructure, network and system monitoring, disaster recovery and BCP planning and testing, environmental systems and an incident management response program. Standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of EPN, CHIPS, IXN and RTP.

Disclosure of known incidents

There were no incidents that occurred during the period of November 1, 2019 through October 31, 2020 related to CHIPS, EPN, IXN, or RTP that had a significant impact on TCH's ability to achieve service commitments and system requirements noted above.

Components of the system

The following components of The Clearing House Payments Company L.L.C.'s system are used to provide the services within the scope of this report:

- Infrastructure – The collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT and hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that the service organization uses to provide the services.
- Software – The application programs and IT system software that support application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external-facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.
- People – The personnel involved in the governance, management, operation, security and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel and managers).
- Data – The types of data the system uses, such as transaction streams, files, databases, tables, and other output used or processed by a system.
- Procedures – The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed and delivered, and reports and other information prepared.

Infrastructure

The Clearing House Payments Company L.L.C. hosts the EPN, CHIPS, IXN, and RTP Services systems on behalf of their customers in data center facilities located in North Carolina and Pennsylvania. The data center facility in North Carolina is managed and controlled by TCH and the data center in Pennsylvania is managed and controlled by Iron Mountain. Both data center facilities have similar capacity with respect to central processing units, magnetic disks, printers, and telecommunications for EPN, CHIPS, IXN, and RTP processing. For EPN/CHIPS/IXN, each computer facility has two independent Unisys ClearPath Libra systems. A stand-alone Unisys ClearPath Libra system, located at each data center, is used for program development. In addition, a number of servers at each data center are used for front-end applications which support the EPN, CHIPS, and IXN processing environment, as well as a front-end server that supports EPN Connect:Direct with Secure Plus and FTP-S, and CHIPS message/payment communications using IBM MQ. For RTP, each computer facility has two independent IBM E880 "frames". Each frame runs multiple logical partitions (LPARS) supporting Production, Bank Test, QC and Development environments. RTP services for each environment are deployed on all four frames, providing intra-site and inter-site redundancy. In the event of a site outage, RTP will continue processing payments on the remaining site. RTP transaction processing can continue uninterrupted with the loss of up to 3 of the 4 frames.

For EPN, CHIPS and RTP, records are written from the active database system to the local standby database in North Carolina and routed to the remote database system in Pennsylvania through the use of leased lines that allow file operations to occur between local and remote hosts. All files associated with a given processing cycle are updated and mirrored real time at both data centers. Database transactions associated with RTP are updated simultaneously at both data centers. Online replication activities are monitored by the computer operators as documented in the Operator Schedules. Any issues are followed up and resolved.

EPN and CHIPS databases are backed up onto a virtual tape library (VTL) and databases containing IXN transaction history are backed up locally utilizing LiteSpeed for SQL Server tool based on a schedule and retained based on an approved retention period. For RTP, all servers are backed up by Avamar (for AIX servers) and Networker (for Red Hat Enterprise Linux (RHEL) servers) at both North Carolina and Pennsylvania data centers. A backup storage system is used to facilitate this process. The backup management system logs backup activities and any backup issues are followed up and resolved within a ServiceNow Incident ticket. RTP database environments are backed up daily using native DB2 shells scripts with 3 days of backups maintained locally on the file system including transaction logs. Backup images are archived using the Avamar system.

It should be noted that TCH alternates the applications between data centers on a recurring basis each year to demonstrate a readiness stance for a disaster recovery situation.

TCH periodically tests and updates documented contingency procedures in connection with disaster recovery planning.

The Network Operations Center group uses the SolarWinds application and the Microsoft System Center Operations Manager Console (SCOM) for real-time monitoring of the network and services. ServiceNow is used to record and track the status of problems encountered in the telecommunications area. TCH also uses ServiceNow for the management and discovery of IT assets. Management conducts a monthly review of devices newly detected by ServiceNow Discovery. A monthly report is generated for devices added in the last 30 days so management is provided visibility of newly discovered devices. Management meets monthly to review the report and takes action if necessary.

TCH laptops have hard drive encryption technology installed and activated.

TCH authorizes the use of both mobile computing and telecommuting. Security measures are adopted to protect against the risks associated with using mobile computing and communication facilities.

Redundancy resiliency

TCH uses redundant processing systems located at the two data centers in order to ensure system availability and maximum uptime. EPN, CHIPS and IXN customers are required to provide connectivity from their backup data center to TCH.

RTP transaction processing runs “active-active” in the North Carolina and Pennsylvania data center (which is managed and controlled by Iron Mountain). RTP customers are required to maintain connectivity to both TCH data centers from their primary and back up sites.

Networks and data transmissions

The TCH EPN, CHIPS, IXN, and RTP networks are segregated from TCH’s corporate network and from the networks supporting other TCH applications (including each other) and include provisioning for redundancies. The TCH networks consist of routers, firewalls, a Virtual Private Network (VPN), optical point-to-point leased lines between the North Carolina and Pennsylvania data centers, and an intrusion detection system to provide network security.

EPN

The EPN network includes Connect:Direct with Secure Plus, and Multiprotocol Label Switching (MPLS); and the Internet using EPNAccess via a Pulse Secure MAG VPN application security gateway or File Transfer Protocol (FTP-S).

EPN customers may elect to transmit to and receive files from TCH's data center using the following methods:

Connect:Direct with Secure Plus

Profiles are established for customers using Connect:Direct with Secure Plus and users are restricted to specific directories. A valid user ID and netmap (network map) related to the customer profile is required for transmitting files to TCH through Connect:Direct with Secure Plus. EPN data transmissions via Connect:Direct with Secure Plus software is achieved using Transport Layer Security (TLS) which provides a secure layer on top of TCP/IP which allows customers to communicate with TCH over the MPLS network, managed by AT&T.

MPLS is a mechanism in high performance telecommunications networks which directs and carries data from one network node to the next. MPLS is a highly scalable, protocol agnostic, data carrying mechanism. In an MPLS network, data packets are assigned labels. Packet forwarding decisions are made solely on the contents of this label, without the need to examine the packet itself. This allows one to create end to end circuits across any type of transport medium, using any protocol.

The MPLS network is encrypted using router configurations which use IP Security (IPSec), a standardized framework for securing internet Protocol communication. IPSec policy uses AES 256 as the encryption algorithm.

EPN customer files transmitted over the MPLS network are provisioned with a network end to end IPSec VPN tunnel using 256 AES encryption. Additional hardware configurations consisting of Access Control Lists (ACLs) and NATs (Network Address Translation) control customer access to TCH systems.

Customers are required to use Connect:Direct with Secure Plus (encryption software) to provide point-to-point file encryption (Secure Plus was previously optional).

EPNAccess

EPNAccess is a web based front-end system used for transmission of customer files as well as for the generation of return items. EPNAccess maintains databases containing historical data including returns. EPNAccess provides an option for EPN customers to activate dual validation whereby certain administrative tasks such as user administration and setting limits for originator, respondent or third party, must be approved by a second user before they are effective. EPNAccess provides activity logs that can be viewed by customers' administrative users.

EPNAccess is accessed through a third-party application security gateway, a Pulse Secure Appliance (PSA) VPN Appliance, to provide security through the internet. Access through the PSA is controlled through a series of controls including RSA multi-factor authentication (token technology), user groups and ACLs. The PSA integrates standards based security and session encryption support is based on TLS.

All files transmitted to and from EPN utilize encrypted links to ensure that the files are sent from an authorized source and are not altered or visible during transmission.

FTP-S

EPN FTP-S transmission is secured using TLS and PGP (Pretty Good Privacy) encryption and can be used to transmit files to TCH via the internet. PGP encrypts and digitally signs files before sending them via the internet. EPN generates a pair of keys – a public key and a private key. TCH sends the public key to the EPN FTP-S customer via Privacy-Enhanced Mail (PEM). The customers are required to import the public key into its key files. The customer follows a required process to generate the public key and private key. The customers are required to send acknowledgement of receipt of the PEM to TCH. FTP-S transmissions are routed through the firewalls that allow only authorized customers to send and receive files based on IP address.

Data transmissions via the internet are validated for authorized sending points by firewall. All customer connectivity to the FTP-S system is controlled by allowing only customer host IP address and required port numbers.

CHIPS

The CHIPS network includes an MPLS and Integrated Service Digital Network (ISDN) backup connection. All connections are encrypted router to router using IPsec 256 AES encryption. Router configurations include Access Control Lists (ACLs), NATs (Network Address Translation) and IPsec to provide end to end network security.

CHIPS data transmissions are achieved using a TCP/IP protocol which allows customers to communicate with TCH over the MPLS network, managed by AT&T.

CHIPS data transmissions transmitted over the MPLS network are provisioned with a network end to end IPsec VPN tunnel using 256 AES encryption. Additional hardware configurations consisting of Access Control Lists (ACLs) and NATs (Network Address Translation) control customer access to TCH systems.

MQ Communications

CHIPS customers utilize IBM MQ to exchange CHIPS messages. The MQ messaging utilizes TCP/IP protocol to interconnect over the proprietary TCH MPLS network.

IBM MQ is a middleware product/tool used for commercial messaging and queuing. IBM MQ runs on a variety of platforms allowing programs to communicate with each other across a network of unlike components, such as processors, subsystems, operating systems and communication protocols.

IBM MQ provides application-to-application encryption with configured Transport Layer Security (TLS) protocol that provides additional data security and integrity, and digital certificates for authentication.

Transport Layer Security (TLS) and Authentication Measures

The TLS channel provides two key security features:

- Authentication of the sender/receiver using channel digital certificates
- Encryption data protection as the payment data is transmitted over the network using an encryption algorithm agreed by TCH and the customers.

Channel Verification for TCP/IP

All CHIPS customers connect using a TCP/IP interface and TCH performs a channel verification for the TCP/IP interface. At the MQ application level, the receiver channel at TCH uses a custom channel verification. The IP address that is contained in a channel initiation request is verified against the designated IP address that is assigned to the CHIPS customer that should be using the channel. The address is controlled at the customer's premises. If the IP address matches the expected address, the receiver channel is started; any other result will be rejected.

IXN

TCH provides customers with two access methods to exchange Image files. Access is available using AT&T's managed MPLS network via Connect:Direct with Secure Plus encryption, or via the internet using FTP-S. Both methods use a collection of routers, firewalls and an intrusion detection system to provide network security. In

addition, customers utilizing the MPLS network and Connect:Direct with Secure Plus may opt to use MQ messaging for data transmissions.

The AT&T managed router configurations consisting of Access Control Lists (ACLs) and NATs (Network Address Translation) control customer access to TCH systems.

Customers are required to use Connect:Direct Secure Plus (additional encryption software) to provide point-to-point file encryption (it is no longer optional).

Please refer to FTP-S, Connect:Direct with Secure Plus, and MQ Communications sections above for additional details.

RTP

The RTP network design includes:

- MPLS; and
- VPN network systems that provide a secure transport between TCH and its customers

Connect:Direct with Secure Plus is used to send reconciliation and standard reports, and all customer originated payment and non-payment messages are delivered via IBM MQ through the MPLS network or secure VPN connections. The MQ messaging utilizes TCP/IP protocol to interconnect over the proprietary TCH MPLS network. The endpoint routers between the customer site and TCH create an encrypted tunnel. The encryption between the customer router and the TCH data centers ensure all traffic between the sites is encrypted.

Please refer to Connect:Direct with Secure Plus, and MQ Communications sections above for additional details.

Digital Certificates and Message Validation

All RTP messages are encrypted twice during transmission – at the router level using AES 256 encryption and between the customers' MQ managers and the TCH MQ managers using TLS 1.2. In addition, RTP messages are digitally signed to ensure they have not been altered during transmission. RTP participants must digitally sign their messages to ensure authenticity. Each participant provides a trusted certificate upon onboarding to be used to validate their digital signatures. The RTP system will reject any message that fail this validation.

AT&T Network Management

TCH has a service agreement with AT&T to provide a Managed Network Service (MNS) to provide an MPLS network which connects customers to TCH for the Image Network. AT&T provides and manages customer premises routers which perform NAT, ACLs and IP routing.

AT&T is responsible for providing and managing the MPLS network and the services provided by AT&T and the alternate carrier. AT&T has subcontracted with an alternate carrier that provides alternate network connectivity. AT&T is responsible for managing the service issues attributed to the alternate carrier.

AT&T is responsible for ensuring the alternate carrier meets the security requirements of the Image system. AT&T provides network services and network devices at the Major Financial Institutions (MFI). AT&T also manages network services which include firewalls, switches and routers at TCH premises.

The equipment installed and managed at each MFI location includes:

- Local exchange carrier (LEC) facility termination, which may be AT&T Local Services, a LEC leased line service provided via AT&T, or a LEC transport service provided by the MFI in coordination with TCH and AT&T.
- AT&T provided router

The encrypted Image files are exchanged between MFIs and TCH over the MPLS network. The MPLS IP VPN with Managed Router Services provides the feature-rich capability of a fully managed IP network while providing the security of a private network environment. Each MFI has one or more data centers where it generates and processes ANSI DSTU X9.37 2003 or X9.100.187 formatted ECP and IXN files. Each MFI also has at least two locations, one on each Image Network carrier, where it provides a firewalled network interface to a co-located TCH DTA server.

Software

The following major applications are hosted and maintained by TCH:

- **Electronic Payments Network (EPN)** – an automated clearing house, i.e., a computerized, batch processing funds transfer system that processes domestic and international consumer and commercial financial transactions among depository institutions.
- **EPNAccess** – a web based front-end system used for transmission of EPN customer files as well as for the generation of return items.
- **Clearing House Interbank Payments System (CHIPS)** – a computerized funds transfer system for domestic and international banking transactions in U.S. dollars.
- **CHIPSWeb** – A web-based front-end system used by CHIPS customers to view and manage their activity.
- **Image Exchange Network (IXN)** – a computerized check settlement system that streamlines the check image exchange, clearing, collection and return process system enabling the secure exchange of digital check images between financial institutions. IXN provides check image exchange between Financial Institutions (FIs) and third-party processors acting on behalf of FIs and settlement processing through the Federal Reserve Bank of New York (FRBNY).
- **SVPCOView** – A web-based front-end system that allows IXN customers to manage their virtual Distributed Traffic Agents (DTAs) and their profile data and view administrative reports, including the status of transmissions.
- **RTP** – enables Participants to initiate credit transfers, receive final and irrevocable settlement for credit transfers, and make available to Receivers funds associated with such credit transfers in real-time. The system also enables Participants to initiate and/or receive non-payment messages associated with payments.
- **RTP Management Console** – a web-based front-end system used by TCH and bank operations' users to monitor status of transactions and perform certain administrative functions.

These applications are supported by a Windows® network, Lightweight Directory Access Protocol, Unisys ClearPath Plus Libra Model Mainframes, RHEL and AIX Unix and Windows operating systems, IBM DB2 and SQL server database management systems.

In addition, the following utilities are used to support the processing environment within TCH's system:

- Connect:Direct with Secure Plus – A transmission system used to transmit EPN, IXN files, and RTP reconciliation and other report files from TCH's data centers using Transport Layer Security (TLS) protocol which allows customers to communicate with TCH over the MPLS network.
- FTP-S – A transmission system used to transmit EPN and IXN files via the internet using TLS and PGP (Pretty Good Privacy) encryption.
- IBM MQ – A middleware product/tool used to exchange CHIPS, IXN, and all RTP customer originated payment and non-payment messages.
- Internet Protocol Security (IPSec) – A transmission system used to transmit IXN files between virtual DTAs and encrypt EPN, IXN, CHIPS, and RTP traffic router to router using a standardized framework for securing Internet Protocol communication.
- Unisys ClearPath Master Control Program (MCP) – Unisys mainframe operating environment software which controls access to the Unisys production and development environments and also provides daily activity logs, hardware performance messages, and error diagnostic messages.
- InfoGuard access control package – Security features of the Unisys ClearPath MCP operating system which controls logical access to the mainframe.
- Active Directory (AD) – a Windows operating system directory service that facilitates working with interconnected, complex, and different network resources in a unified manner.
- LDAP – used for authentication to RTP Unix jump servers.
- Courion – workflow tool used to manage the request, approval, and provisioning for new employee access, and review processes for existing user access to systems, applications, and databases.
- ArcSight Enterprise Security Management System (ESM) – The security information event management (SIEM) tool in ArcSight is used to facilitate information security administration. ArcSight is interfaced with all computing environments including databases, servers and networks to capture access activities including access violations.
- ServiceNow (SNAP) – Ticketing system used to document, track, and manage the workflow for change requests, incident resolution and modifications to existing user access. ServiceNow is also used for asset inventory and discovery.
- Archer – Tool used to document and monitor enterprise risk.
- CA Project & Portfolio Management (CA PPM) – Tool used to record and track the progress of major projects and corporate initiatives.
- Project Management (PM) Sharepoint – The approval workflow function within this Sharepoint site is used to obtain electronic signatures of approval for all critical documents prepared for the design, development, or testing of all major projects and corporate initiatives.
- Microsoft System Center Operations Manager (SCOM) – Third-party monitoring software used to track state, health, and performance information of TCH computer systems.
- Tenable Nessus – Vulnerability scanner software used by TCH to perform monthly vulnerability scans on internal TCH systems.
- IBM BigFix – used for managing server hardening compliance.
- RSA SecurID and Security Console – multi-factor authentication software used for access to the TCH VPN via laptop and mobile devices. Console used for the administration of RSA tokens.

- SolarWinds – IT management software used for real-time monitoring of the TCH network and services as well as network inventory.
- BL Library (BL LIB) – a fully automated tape library system that operates in the Unisys database environment for CHIPS and EPN.
- LiteSpeed – backup and recovery software used for SQL servers for IXN transaction history.
- Dell EMC Avamar – duplication and recovery software used for IXN, and RTP AIX server data.
- EMC NetWorker – data protection and backup software used for RTP RHEL server data.
- LG IrisAccess 7000 – Iris recognition software used by TCH to control entry and exit to doorways at the New York and North Carolina facilities.
- C-Cure 9000 – physical access management software used by TCH to monitor badge activity for the facilities and data centers.
- ADP Reporting – used for generation of HR new hire and termination employee listings among other functionality.
- PassagePoint Global – used for visitor and badge reporting for the New York facilities.
- CarbonBlack – Intrusion Detection System software used by TCH.
- Urbancode – Migration tools used for the deployment of application code changes.
- Checkactive program – an internally-developed program automatically executed periodically in the mainframe environment based on schedules to monitor disk space.
- Checkfiles program – an internally-developed program automatically executed in the mainframe environment to compare the names of production programs, system software and parameters and their compilation and creation dates with the information in the Control File.

People

Organization charts are published on the company intranet and written job descriptions have been documented for all departments. TCH's system is supported by the key functions described below:

Operations and Technology (O&T)

Operations and technology is responsible for all aspects of planning, developing, operating and supporting the data processing services offered by TCH, including maintaining the business continuity plan and coordinating the testing of the plan. The O&T department is comprised of the following business units: Enterprise Architecture, Network Operations, Customer Services and Payment Specialists, Implementations and Account Services, Quality Control, Operations and Technology Administration, Infrastructure, and Systems Development.

Enterprise Architecture

Enterprise Architecture provides both Solution as well as Enterprise Architecture services. Solution Architecture involves collaboration across O&T as well as with Information Security to develop detailed architectures that support both software and hardware projects. This typically involves producing artifacts such as architecture diagrams along with design documentation. Enterprise Architecture involves the development and execution of a technology governance program. Examples of the current governance activities and work products include the Architecture Review Board (ARB), reference architectures and standards. In addition, Enterprise Architecture is responsible for delivering key strategies such as the O&T Strategic Plan and the TCH Cloud Strategy.

Network Operations

Network Operations is responsible for day to day computer operations, telecommunications, client services, technical services and integration management, database services and payments processing services. This involves the overall daily management, planning, monitoring and administration of all operational activities involved in operating TCH's data centers, network and the environment in the data centers. These responsibilities are organized as follows: New York Network Operations Center; and North Carolina Network Operations Center.

Customer Services and Payment Specialists

Customer Services and Payment Specialists perform client activity monitoring and support clients with inquiries and requests.

Implementations and Account Services

Implementations and Account Services coordinate and execute client onboarding and maintenance requests.

Quality Control (QC)

QC is responsible for testing both system and application changes for all production environments.

Operations & Technology Administration

Operations & Technology Administration is responsible for implementing project management best practices to support the Technology group's software and non-software development projects. This group also is responsible for the Operations and Technology budgets and expenses as well as Operations and Technology contract management as part of the procurement function.

Infrastructure

Infrastructure is responsible for network engineering, maintenance and support, connectivity and vendor integrations, for mainframe, distributed systems engineering and desktop support.

- Mainframe Support is responsible for the acquisition, planning, and installation of system software for the mainframe environment.
- Distributed Systems Engineering is responsible for the strategy, design and implementation of TCH's distributed systems server environment.
- Network Engineering is responsible for the design of the network environment, selection of the network hardware, and configuration of the firewalls, routers and switches. The group interfaces with the external internet Services Providers and network carriers and is responsible for network performance.
- Database Administration is responsible for designing, developing and maintaining the databases.
- Desktop Support is responsible for laptops and mobile computing support services.

Systems Development

Systems Development is divided into the following groups:

- Mainframe System Development is responsible for the development and maintenance of applications for the mainframe environment.
- Distributed System Development is responsible for the development and maintenance of system software and applications for the distributed system environment.

- Project Management and Business Analysis is responsible for management of all development activities related to the RTP application and for development of functional specifications and user guides.
- RTP technology supports the RTP environment. Duties include integrating vendor software development of supporting applications such as interfaces to external and internal systems such as Fedwire, Billing, Data and Business Intelligence. The RTP team also provide level 3 production support for both the vendor and in-house software.

Finance and Real Estate Management incorporating Corporate Real Estate Management

Corporate Real Estate Management is responsible for managing and maintaining the physical security and environmental controls for the North Carolina data center and New York and North Carolina NOCs. Corporate Real Estate Management (CREM) is also responsible for performing monitoring controls over Iron Mountain for the Pennsylvania data center.

Risk office

Risk Office is comprised of the following groups:

- Information Security – is responsible for monitoring logical access for all systems.
- Enterprise Risk Management – is responsible for executing efficient and effective assessment of risks, increase and promote a risk aware culture, and improve the management of risk throughout the organization by performing its risk governance and oversight role as the second line of defense across the organization.
- Systemic and Liquidity Risk Management – is responsible for maintaining regulatory compliance with regard to CHIPS, supporting industry initiatives related to systemic and liquidity risk, execution of simulation stress testing and related Participant communication functions, model risk management, and evaluation and enhancement of risk analytics, monitoring and reporting to support TCH products.

Product development & management

Product Development & Management is responsible for managing and administering the payments products and services to meet the needs of targeted financial institution markets and the strategic goals of TCH.

Other departments

In addition, the following departments support the operations of TCH:

- Customer Relationship Management
- External Affairs and Board Relations
- Human Resources
- Internal Audit
- Legal

Segregation of duties

TCH provides segregation of duties to effectively control the concentration of functions within the organization. The separation of technology and operations duties from TCH's Product Development & Management Division

and other Administrative functions, which include accounting and finance, audit and human resources, provides an additional level of segregation of functions within TCH.

The fact that TCH is an entity separate from EPN, CHIPS, IXN, and RTP customers provides a certain amount of inherent segregation of function. TCH's employees are not able to initiate, authorize, or initially record transactions or correct or modify customer files (except for the CHIPS name and address database as noted below).

Access Management training addresses segregation of duties and includes descriptions of "toxic pairs" (entitlements that should not be granted to certain roles). Management reviews and recertifies access entitlements throughout the year and rejects any access entitlements that are not least privileged or segregated as appropriate. In the event that "toxic pair" entitlements are required for an individual, there is a policy exception and registration process for risk acceptance.

Procedures

TCH has developed the following policies and standard operating procedures to operate, maintain, and secure the EPN, CHIPS, IXN, and RTP Services systems, and to achieve the trust services criteria relevant to security and availability.

Security monitoring

TCH uses the ArcSight Enterprise Security Management System. The Security Information Event Management (SIEM) tool in ArcSight is used to facilitate information security administration. ArcSight is interfaced with all computing environments including databases, servers and networks to capture access activities including access violations. Security related activities such as user data change, file security attribute change and security violation including inappropriate user activity, unauthorized software, virus and firewall alerts are captured, logged and reported using ArcSight. ArcSight is configured to send an alert to the responsible Information Security personnel through the Information Security workstation and their mobiles when there is an event that meets the defined criteria such as a possible security violation. Each alert is reviewed and triaged by the managed security service provider, Cipher, and followed up and cleared by Information Security, as necessary.

ArcSight captures and maintains logs of access activities and provides a reporting feature for security administration. The responsible Information Security personnel and third-party vendor, Cipher, review access activities online as activities occur. A report from ArcSight can be generated when needed.

The TCH networks include an Intrusion Detection System (IDS) (CarbonBlack). Information Security management are alerted of intrusion activities. Incidents noted are recorded in ArcSight and depending on the nature and type of problem, the incident is escalated to the designated group for follow-up and resolution.

TCH has established procedures for incident response which address the process and controls for problem/incident response, notification, escalation, logging and resolution. Designated management members are responsible for notifying customers or other external parties, if applicable. TCH uses ServiceNow to record, escalate, report and track incidents encountered. Through ServiceNow, each incident is escalated to designated individuals based on the nature of the incident.

Availability monitoring

SCOM software is in place to monitor system availability, uptime, performance, the health of systems, hard disk space utilization, etc., in the distributed systems environment. Alerts are configured within the software to notify relevant parties via email once a configured threshold regarding system performance has been met.

Operators receive the alerts and open incidents in ServiceNow (SNAP) to triage and may notify additional support teams to address the issue. Once the alert is resolved, the ticket is closed. Issues including outages/downtime are reported via SCOM alerts and Network Operations raise a corresponding ServiceNow incident ticket as needed. Issues, if any, are followed up and resolved. Any incident causing actual downtime is rated a Severity 1 or 2 incident, and the duration is managed and reported. On a monthly basis, Operations calculates overall system uptime based on Severity 1 and 2 tickets impacting production, and reports as a key metrics to TCH management.

System availability, and network usage is tracked, summarized and reported in a monthly management report (O&T KPI Executive Summary). For any breached threshold (including system uptime and availability and system capacity), a ServiceNow ticket is escalated to the designated group for follow-up and resolution. Once an incident is resolved, the ticket is closed.

The Checkactive program, an internally-developed program, is automatically executed periodically in the mainframe environment throughout the day based on schedules to monitor disk space and reduce the risk of a disk error not being addressed. An alert message for a mismatch condition is sent to the Network Operations console. Network Operations follows-up and resolve the mismatched condition. The alert message for a mismatch condition is displayed on the console until the mismatch is resolved. A ServiceNow ticket is escalated to the designated group for follow-up and resolution. Once the mismatch is resolved, the ticket is closed.

Capacity Management

TCH's Communication and Operations Management policy documents established procedures for capacity management including TCH resources are to be monitored, tuned, and capacity projections made for future capacity requirements to ensure system performance.

Transmission monitoring

Network Operations monitor all communication lines on an ongoing basis. Incidents noted are recorded in ServiceNow tickets. Depending on the nature and type of problem, the incident is escalated to the designated group for follow-up and resolution.

Daily telecommunications error reports are summarized weekly and reviewed by management to determine any trends in issues that may indicate any security or control issues. All network problems are recorded in the ServiceNow system by opening an incident or change ticket.

Network maintenance

TCH has documented network management procedures, which include network application maintenance, infrastructure management and change management. Changes in the network components including hardware, software and configuration must follow TCH's change control procedures. The Network Engineering group maintains a database of current network devices and configurations. In addition, the ServiceNow system scans all network subnets which also builds a device database. Network Engineering management meets regularly to discuss needs for upgrades or changes in the network devices and configurations. Policy and procedures for network management are documented and available for reference. All changes are recorded in ServiceNow.

The Network Operations Center group uses the SolarWinds application and the Microsoft System Center Operations Manager (SCOM) for real-time monitoring of the network and services. ServiceNow is used to record and track the status of problems encountered in the telecommunications area.

Vulnerability management

TCH uses Tenable Nessus, a vulnerability scanner system, to perform weekly vulnerability scans of the network and servers. Information Security receive the results of the weekly scans each week via email. The results and identified vulnerabilities are then communicated to the responsible teams and IT management for risk analysis via a weekly vulnerability meeting and a remediation plan is put in place as necessary. If necessary, the change management process is initiated as a result of any findings. The responsible team may open a ServiceNow ticket to track remediation actions that include patch installation, system or network configuration change, proxy setup, and firewall filtering as required. Validation that the vulnerabilities were adequately remediated is addressed during weekly vulnerability meetings and ongoing vulnerability scans.

In addition, third-party software inspection and vulnerability management systems are used to notify TCH system administrators of the discovery of new vulnerabilities and availability of patches. Third-party and industry groups (e.g., FS-ISAC & US-CERT) broadcast notifications of new vulnerabilities on a periodic and ad-hoc basis. Notifications are actioned upon as needed by IS personnel for applicability to the current TCH environment.

TCH provides hardening standards for system administrators in order to implement secure server configurations within the company's infrastructure. The guidelines are reviewed and updated when changes occur by the Information Security team.

Monthly validation of compliance to hardening standards occurs through the use of BigFix. Tickets are created for remediation or a policy exception is documented in Archer.

TCH utilizes Symantec Endpoint Protection to protect against viruses, malware, malicious code and unauthorized software. Virus definitions are kept current and infected files are quarantined. Security alerts are logged, reported and analyzed via ArcSight.

Physical access

Physical assets are protected 24 hours a day, 365 days a year by either guards, alarms or surveillance cameras. Access to the New York Network Operations Center and processing facility and North Carolina data center, Network Operations Center and processing facility are controlled by biometric access control system.

Courion, an automated tool, is used to document and notify CREM of new employee physical access requests. The Corporate Real Estate group is responsible for administering access to the data centers. Access for an individual is provisioned based on access requested within the Courion notification form. Access for an individual is based on least privilege through the automated tool. Once approved by the new employee's manager, Courion automatically routes the access request to the Corporate Real Estate group for the provisioning of the request. The Courion requests must be approved by the Hiring Manager. The Courion system is used for requesting new employee access and requesting the removal of access privileges for an individual. The same Courion request form is used for new employee's requesting logical access to the systems and applications. Any change to existing access is requested and approved by the individual's manager through emails. Access to the Courion system is controlled through the security features of Active Directory.

Strategic locations such as the entrance to the computer and telecommunications room, high security areas and the passing from a less secure to a more secure area are monitored by closed circuit television. A guard is required to tour the facility several times during each shift. Employees are granted the level of access required to carry out their job responsibilities.

Guard stations are located at the facility entrances of the New York and North Carolina processing facilities 24 hours a day, 7 days a week. Visitors are required to be pre-announced and authorized, sign in, wear a visitor's badge, and be escorted by a TCH employee while in the facility.

Both employees and visitors must pass through two successive doorways to access the New York and North Carolina processing facilities of TCH. The guard locks and releases the first and second entrance doors with remote electronic switches for authorized visitors. Employees use a biometric iris scanner to control entry and exit to doorways. The corridor between these doors serves as a "man trap".

The biometric access control system is installed on a stand-alone computer located in a secure area at each location and logical access is limited to the Information Security team.

Physical access security for the Pennsylvania data center as a facility is managed and administered by Iron Mountain. TCH is responsible for notifying Iron Mountain regarding provisioning and de-provisioning of users with badge access to the Iron Mountain data center. For the Pennsylvania data center, access is granted and terminated by Iron Mountain upon email notification from Network Operations or Corporate Real Estate management. Iron Mountain access profiles are included as part of a monthly status call between TCH Operations, Corporate Real Estate management & Iron Mountain Operations.

Environmental control systems

TCH utilizes data center facilities in North Carolina and Pennsylvania. The data center in North Carolina is managed and controlled by TCH and the data center facility in Pennsylvania is managed and controlled by Iron Mountain. The North Carolina data center facility is equipped with uninterruptible power supply systems, dual diesel generators, fire protection systems, and hardware and software sufficient to operate all production systems concurrently.

For the North Carolina data center, a guard is stationed in a secure post at the entrance to the computer facilities and monitors certain security and environmental control systems from the station, including all access to exterior entrances, status of the uninterruptible power supply equipment, heat and smoke detection devices, and fire suppression equipment.

The environmental control systems at the data centers are monitored by the Security Command Center. For the Pennsylvania data center managed by Iron Mountain, Corporate Real Estate and Corporate Security reviews environmental SLA requirements on a monthly basis.

Physical security and environmental control systems for the Pennsylvania data center are managed and administered by Iron Mountain. The scope of this report does not include controls performed by Iron Mountain.

Logical access

TCH has documented Information Security policies which address requirements for information security as follows:

- Risk Assessments
- Information Security
- Organization of Information Security
- Asset Management
- Human Resource Security
- Physical and Environmental Security

- Communications and Network Operations Center Management
- Access Control
- Information Systems Acquisition Development Maintenance
- IS Incident Management
- Compliance

Access administration

TCH Access Management is a part of TCH's Chief Information Officer's organization and is responsible for reviewing access requests for all environments for completeness and authorization. An automated tool for submitting requests, Courion, is used for requesting new employee access and requesting removal of an individual's existing access. Once approved by the new employee's manager, Courion automatically routes the access request to designated department teams based on the access requested for provisioning of the request. Users are given the least amount of system privileges required to perform their responsibilities. An audit trail for each request is captured and maintained by the system.

The Courion requests for new employee access must be approved by the hiring manager. Based on an approved Courion request, the Identity and Access Management team creates or changes user accounts in Active Directory, MCP/InfoGuard and LDAP security as requested. Any changes to existing user access is requested and approved by the individual's manager through the ServiceNow ticketing system and provisioned by the Identity and Access Management team.

Courion is also used for transfers which are initiated by HR. Courion requests for transfers are then routed to the new reporting manager for approval.

TCH uses the ArcSight Enterprise Security Management System. The Security Information Event Management (SIEM) tool in ArcSight is used to facilitate information security administration. ArcSight is interfaced with all computing environments including databases, servers and networks to capture access activities including access violations. Security related activities such as user data change, file security attribute change and security violation including inappropriate user activity, unauthorized software, virus and firewall alerts are captured, logged and reported using ArcSight. ArcSight is configured to send an alert to the responsible Information Security personnel through the Information Security workstation and their mobiles when there is an event that meets the defined criteria such as a possible security violation. Each alert is reviewed and triaged by the managed security service provider, Cipher, and followed up and cleared by Information Security, as necessary.

ArcSight captures and maintains logs of access activities and provides a reporting feature for security administration. The responsible Information Security personnel and third-party vendor, Cipher, reviews access activities online as activities occur. A report from ArcSight can be generated when needed.

On a semi-annual basis, management of each employee reviews and confirms employee access or provides changes to the Identity and Access Management team. The Courion tool is used to perform the access review process. The Courion tool is updated with the user listings and then automatically generates access listings and sends e-mail notifications to management requesting their review based on reporting manager assignments provided by Human Resources. Management provides their confirmations and/or changes to the Identity and Access Management team through the Courion tool. Rejected assignments are removed and documented through a ServiceNow ticket by the Identity and Access Management team. The reporting manager can also delegate or reassign the review to another TCH employee directly through the Courion tool if deemed appropriate (e.g. if the user recently transferred to another department and reports to a different manager) but will still remain the review owner in Courion. Identity and Access Management only close the

review cycle after all review submissions have been received and they can revert incomplete delegated/reassigned reviews back to the original owner if they have not yet been completed.

Management reviews and confirms privileged access or provides changes to the Identity and Access Management team on a quarterly basis. These reviews are performed in addition to the all-inclusive semi-annual reviews described above and follow the same process via the Courion tool.

Customers must submit a request for access to EPNAccess in writing which is authorized by Client Services. Based on the customer request, the Identity and Access Management group completes the request using the ServiceNow ticketing system. ServiceNow is used for requesting a new access, deleting or changing an existing access. The ServiceNow request is routed to designated managers for approval and completion of the request. Access to EPNAccess requires a SecurID token, a valid ABA transit/routing number and associated password for file transmissions.

For SVPCOView, the customer submits a SecurID Request Form to TCH for a user ID for the customer's local security administrator account which is authorized by Client Services. The Identity and Access Management team uses ServiceNow for submitting requests for a new access, deleting an existing access or changing access. The customer's user account is setup based on the customer's transit/routing number. Access to SVPCOView requires user IDs and SecurID tokens assigned to each participant.

For CHIPSWeb, customers can request, in writing, secure tokens from Client Services, and Identity and Access Management. This department is responsible for distributing the secure key tokens and PINs to the customer. A customer accessing CHIPSWeb via VPN requires a secure token key, unique username and PIN which is issued by the Identity and Access Management department.

Requests for SecurID tokens to access the RTP Management Console are made in writing by the customers using a SecurID Request form and authorized by Client Services. The Identity and Access Management team uses ServiceNow for submitting requests for new access, deleting existing access or changing access. Access to the RTP Management Console requires a SecurID token, a valid user ID and password.

Remote access

Individuals are granted access to the TCH systems from remote locations via TCH-issued devices or Virtual Desktop Infrastructure (VDI). Remote access requires multi-factor authentication, controlled through a VDI or Virtual Private Network (VPN) using network credentials and SecurID tokens. Most employees are granted normal corporate access via the VDI with SecurID tokens. Requests for customers' users (external users) are initiated by a SecurID request form, authorized by Client Services and documented in ServiceNow. Internal user new remote access is reviewed and approved by TCH management and documented in ServiceNow.

Access to the RTP environment is also front-ended by jump servers which are accessible via the VPN. The jump servers require the use of multi-factor authentication via AD credentials and SecurID token.

Unisys mainframe environment (EPN/CHIPS/IXN)

Access to the EPN, CHIPS, and a part of the IXN production and development environments is controlled by InfoGuard, the security features of the Unisys MCP operating system. InfoGuard allows programs and users access only to defined computer resources. Access privileges are reported in the Make User report that is used by the Information Security Department and the Identity and Access Management team.

Access is controlled through usercode and password security. A valid usercode and password are required to access the system. Passwords are entered in an obfuscated field that prevents the password from being displayed on the terminal. When a usercode is shared by a group of individuals, a unique accesscode and

accesscode password are assigned to each individual. Certain usercodes are privileged and are only assigned to authorized personnel. Users are granted access based on their job responsibilities.

TCH has implemented the following security rules for the mainframe environment:

- Passwords must meet a minimum length requirement.
- Passwords must be changed at specified intervals.
- Passwords must be different from a certain number of passwords previously used.
- Usercodes (with and without accesscodes) are locked after a specified number of violations per day.
- Terminals and workstations are disabled after a number of invalid access attempts within a defined duration of time.
- Terminals and workstations are automatically logged off after a defined period of inactivity.
- Access to sensitive utility programs such as the COMS utility and the CANDE editor is restricted to authorized personnel.

Distributed environment

Access to servers in the distributed environment, where EPNAccess, CHIPSTWeb, SVPCOView and RTP's Management Console reside, is controlled by features available through Active Directory (AD) in the Windows server environment. Access to RTP servers is allowed only by first authenticating to a "jump" server where access is controlled via Active Directory credentials as well as an RSA SecurID token. Logging into the RTP production servers is then possible and is controlled via LDAP accounts managed by Identity and Access Management for non-locally authenticated accounts. TCH has implemented the following security rules for the distributed environment:

- Passwords must meet a minimum length requirement. Passwords must be changed at specified intervals.
- Passwords must be different from a certain number of passwords previously used. User IDs are locked after a specified number of violations per day.
- Inactive sessions are shut down after a defined period of inactivity.
- Access, including administrative rights, is granted to individuals based on their job responsibilities.

Incident and problem management

TCH has established procedures for incident response which address the process and controls for problem/incident response, notification, escalation, logging and resolution. Designated management members are responsible for notifying customers or other external parties, if applicable. TCH uses ServiceNow to record, escalate, report and track incidents encountered. Through ServiceNow, each incident is escalated to designated individuals based on the nature of the incident.

Systems development and maintenance

Development projects (major changes or enhancements to the functionality of the system) and changes to programs are carried out in accordance with procedures addressed in the Software Development Life-Cycle (SDLC) and Project Management Handbook. Project procedures and project management procedures are documented in the SDLC document. The procedures address requirements for software/hardware changes and system development and testing.

Project change initiation

Project changes are initiated based on business and operational needs. Project changes are monitored by the O&T Administration group. Many projects are initiated in response to the changing processing or regulatory environment. Other project changes are initiated by Network Operations Center or System Development groups in response to ideas to improve operational or processing efficiencies and to resolve incidents.

Major projects or corporate initiatives are submitted to the O&T Portfolio Steering Committee, for cost, benefit, prioritization and strategic authorization. Other smaller projects are authorized through a virtual approval process and then presented to the O&T Portfolio Steering Committee. Major projects are any projects over a certain dollar threshold that require O&T Portfolio Steering Committee approval as defined in the Project Management Handbook document. Reasons for requiring approval include: risk level, spend level, and level of resource commitment.

The O&T Administration group is responsible for monitoring project activities for timely completion of each major step including the design, development and testing of all projects. Once a project is authorized by the O&T Portfolio Steering Committee, the project is activated in the CA Project & Portfolio Management software (CA PPM). Projects are recorded and tracked in CA PPM. Projects are required to follow the requirements in the SDLC. The Project Management (PM) Sharepoint workflow approval function is used to obtain electronic signatures of approval for all critical documents. Various documents, depending on the nature of the project and guided by the PM checklist, are prepared to support the project development and implementation. These documents are maintained in the PM Sharepoint folder for each specific project. Access to the PM Sharepoint site is controlled through the security features of Active Directory. These procedures include requirements for application development and maintenance which include the following phases:

Phase 1 – Project initiation

During this phase, a Project Scope document is developed by the Sponsor to define the goals for the project. Once the scope is determined, the review/approval process is conducted.

Phase 2 – Project planning

During this phase, Business, Functional and Technical requirements are developed to meet the Sponsor's goals for the project. All changes to the business operating environment and the technical infrastructure have continuity requirements included in their development cycles, including rigid testing methodology. Technical requirements include security and availability requirements (e.g., information security review, threat modeling, security and privacy design and vulnerability evaluations). For technical projects, this may include screen layouts, expected results of user actions, database structures, technical design, testing plans, etc.

During this phase, a project plan is developed, project meetings are conducted, and the project requirements are gathered, reviewed and approved.

Phase 3 – Project execution

During this phase, the Technical Design and Functional Requirements are used to achieve the goal and objectives of the project. For technical projects, this includes application development, unit testing, functional testing, user acceptance testing (UAT) (if required), security and availability testing (e.g., fuzz and dynamic scan), and building or enhancing infrastructure environments, executing test scripts, regression testing, etc. This phase concludes with implementing the solution into the production environment or the achievement of the project's intended goal(s).

Phase 4 – Project close-out

This phase validates whether the project objectives have been met and captures any lessons learned throughout the project. This serves as an opportunity to improve TCH processes and procedures for future initiatives by developing a knowledge base for “best practices” based on the lessons learned collected from the projects.

In addition, TCH has The Clearing House Change Control Policy document that provides requirements for initiating changes to the production environment, including change initiation, approval, bi-weekly Change Advisory Board meeting and procedures for implementing and closing a change.

Development and testing

ServiceNow (SNAP) is an automated tool used to document change/incident requests, approvals, and completion dates.

Changes are developed and tested within the development environment. Programmers develop programs on a stand-alone processor or servers dedicated for program development and testing.

When the test results are satisfactory, the ServiceNow change request is submitted by the development team to request the program to be promoted to the Quality Control (QC) test environment. QC performs testing on the developed code to ensure requirements are met in a dedicated testing environment.

Vendor software is installed and “smoke tested” in the development environment prior to being installed in the QC environment.

For new programs or changes to existing programs, QC performs independent quality assurance tests, including:

- Reviewing documentation of program specifications, business and functional requirements, and code changes;
- Compiling new source and executable programs;
- Performing security and availability testing (e.g. fuzz and dynamic scan); and
- Performing functional and performance testing where applicable.

The nature of change dictates the requirement for QC testing and environment where testing takes place. The QC requirement and testing is also reviewed by the Change Advisory Board. Hardware changes do not require QC testing unless the change directly impacts the core product.

When QC testing is complete, the program is moved into the Bank Test environment, and as necessary, the business sponsor performs user acceptance testing. For projects that impact the application functionality, customers have the opportunity to further test the new application software in the Bank Test environment. Voluntary customer testing is performed for major changes. Depending on the extent and nature of the change, customers may be required to perform certification testing in the Bank Test environment to prove their systems are ready for the change. For all releases, a backout plan is documented in the project documentation in the project’s PM Sharepoint folder. The development team submits a change request in ServiceNow to migrate into the production environment. Information Security approval is required for all code deployments prior to the program being deployed to production.

Access to source code is restricted to only those persons who have a business need to access the code. As per the TCH Secure Software Development Policy, developers are to follow guidelines identified in the TCH Secure Software Best Practices document in developing secure code.

RTP source code is developed by a third-party vendor. Requirements for RTP development work is provided to the third-party developer in business requirement documentation. Source code packages are provided by the vendor and then deployed and tested within the development environment by TCH. QC performs testing on the developed code to ensure requirements are met. For in-house development for related RTP software (i.e. Billing feeds, Fedwire Interface), programmers develop programs on a stand-alone processor or servers dedicated for program development and testing.

Change approval

A Change Advisory Board meeting is conducted bi-weekly to discuss the upcoming changes that need to be approved. Changes scheduled for implementation are reviewed during the meeting. The Change Advisory Board meeting is attended by the following as needed:

- Change Control
- Database Systems or authorized delegates;
- Network Operations Center or authorized delegates;
- Identity and Access Management
- Middleware
- Security Infrastructure Systems
- Operations Services
- Corporate Real Estate Management;
- Information Security;
- Mainframe Development and Support;
- Quality Control;
- End User Support;
- Web Development;
- Business Continuity Management;
- Wintel Services;
- Network Engineering; and
- Staff members with content matter expertise, if applicable.

TCH uses ServiceNow software to support the change management process. All changes, including changes to the applications and infrastructure, are initiated using a ServiceNow Change Request Ticket which is tracked throughout the change lifecycle. The required information in the change request ticket must be completed before the ticket can be saved, submitted for approval and processed. Change requestor and change owner approvers for each department are defined in ServiceNow. Approvers can delegate their approval responsibilities to other management by establishing a delegate in the ServiceNow tool. The ServiceNow tool maintains a log of all revisions made to the ServiceNow approver assignments.

When a change request ticket is submitted, ServiceNow generates an approval alert. The approval alert is automatically sent to the immediate manager of the change requestor. The manager reviews the change ticket and can approve or reject the change request. If approved, a second approval request is automatically routed to the immediate manager of the change owner. Once approved by both managers, the change is automatically routed to the Change Advisory Board for approval. For code deployment, database and firewall changes, an Information Security approval is also required. Once all approvals have been given, the change will move to an authorized state, a member of Change Control will then review the change request for completeness and accuracy prior to approving. If any of the approvers reject the change, the change will revert to the "New" state with ServiceNow.

A change ticket can be rejected and additional information requested or rejected and marked as a permanent cancellation if the approvers deem that the change is unnecessary or considered a high risk.

Implementation of change

Implementation of the approved changes is scheduled according to risk classification: low risk, medium risk or high risk. Changes are implemented in the production environment by Platform Management or assigned implementers in the following designated groups: Network Operations Center, Operations Services, Infrastructure SMEs, and Database Administration.

For approved program changes, Platform Management representatives move the executable programs to the production environment using implementation tools. Once installation is complete, the change request is closed.

After a change has been implemented, the assigned implementer is required to update the change ticket to reflect the current status: Implemented Successfully, Implemented with Issues, or Backed Out. Any additional comments regarding the implementation are noted in the ticket. A Post Implementation Review is performed if the change did not implement successfully to capture issues encountered and lessons learned.

The final status of a change is the Closed state. The ServiceNow ticket is closed by Change Control.

Scheduling Maintenance and Downtime

Client Services sends bulletins to the customers describing upcoming system changes such as application releases and any downtime, if expected. For RTP, new release bulletins include the RTP Supplement to Functional Documentation that describes a list of client impacting defects, issues, or considerations and provides an update to the list with each major release.

Emergency changes

Emergency changes are either classified as 'Timeline Not Met' or 'Breakfix'. 'Timeline Not Met' emergency changes to resolve an issue that is negatively impacting TCH's systems are submitted for review and approval outside of the change control process (were not submitted for approval within the expected timeframes). A ServiceNow change request ticket indicating the nature of the emergency is required. These emergency changes require an additional approval from four members of the Emergency Change Approval Board (ECAB) group and cannot be verbal. 'Breakfix' emergency changes are those requiring immediate action due to failure of service and require expedition to restore service and prevent disruption and can be verbally approved. Documentation for these types of emergency changes must be completed before the end of the next business day.

Control files (EPN/CHIPS)

In the mainframe production environment, program, system software names and parameters used in processing and their corresponding compilation/creation dates are maintained in a Software Control File (Control File). QC is responsible for maintaining the Control File. Periodically throughout the day based on a schedule maintained in the workflow program, the Checkfiles program, an internally-developed program, is automatically executed to compare the names of production programs, system software and parameters and their compilation and creation dates with the information in the Control File. This procedure helps determine whether the application and system software installed on the production partition are the production versions as tested by QC and installed by Network Operations. The Checkfiles program generates a report that is reviewed for errors. Any errors are investigated and reported to management.

Access to the Control Files is limited to the Mainframe Support group and certain management. Developers and QC personnel do not have update access to the production environment. Access is controlled by the Unisys MCP operating system and the Unisys InfoGuard access control package. Access privileges are reported in the Make User report that is used by the Information Security department to monitor logical access.

Access to Production

Logical access to the supporting distributed environment is limited to selected individuals in the related support teams of the Infrastructure, Operations and Operation Services departments. Logical access in the distributed environment is controlled by features available through Active Directory (AD) in the Windows environment.

TCH employs two levels of security over access to the RTP production environment. Access to RTP servers is allowed only by first authenticating to a “jump” server where access is controlled via Active Directory credentials as well as an RSA SecurID token. Logging into the RTP production servers is then possible and is controlled via LDAP accounts for non-locally authenticated accounts managed by Identity and Access Management.

Employees are granted access to the production environment based on their job responsibilities. Programmers do not have access to the production environment.

Emergency access may be granted as part of the break-glass process to facilitate resolution of a production issue. Credentials are provisioned upon approval. If the break-glass process is invoked, a ServiceNow ticket is raised and the credentials are used. Information Security monitors the use of the break-glass credentials via ArcSight, and if used, Identity and Access Management supplies new credentials.

Documentation

Business Analysts in conjunction with Subject Matter Experts update system and/or end user documentation. The Information Security team updates all Information Security policies and procedures as each individual department does for their processes.

Operating system, infrastructure and system software change management

The process for patches, bug fixes, hardware upgrades, and software upgrades, and changes to operating system, system software and infrastructure including network configuration files, is controlled through a similar methodology used for application changes. New releases of system software from the software vendors and modifications to system software are authorized by the systems development or infrastructure departments depending on the type of system software and prioritized based on the criticality of the system components and are implemented on the development system for mainframe system software and in the test

server environment for distributed system software with the assistance of the Network Operations Center group or Platform Support deployment team. Changes are initiated, reviewed, approved and controlled throughout the cycle using ServiceNow following the process previously described.

All changes to the business operating environment and the technical infrastructure have continuity requirements included in their development cycles, including rigid testing methodology.

The same procedures and controls used for application software development are used for operating system, system software and infrastructure changes.

Software is tested on the mainframe development system or test server environment by Infrastructure Mainframe Support. Once Infrastructure's test is complete, Platform Support moves the software to either the QC environment for the mainframe development system or the QC server environment for distributed system software for QC independent testing. Upon completed testing by QC, the software is moved to the Bank Test environment, approved by the Change Advisory Board and then implemented into production by the Network Operations or Platform Management team.

Operating system software changes are tested for a period of time in the QC environment for distributed system and in the mainframe production system during a downtime window. At the conclusion of QC testing, the changes are moved into the Bank Test environment by Platform Support. This testing is performed with selected participating institutions prior to the operating system change being implemented in the production environment.

Changes discussed in the bi-weekly Change Advisory Board meetings described in the Systems Development and Maintenance section include OS changes and system software changes.

Control files (EPN/CHIPS)

As part of the Checkfiles program noted above in the Control Files section under Systems Development and Maintenance, the program checks the operating system, infrastructure and system software periodically throughout the day based on a schedule. Logical access to the servers in the distributed environment is controlled by features available through Active Directory (AD) in the Windows environment.

Computer operations

EPN/CHIPS

All processing is carried out according to a regular processing cycle, which begins with the preparation of EPN, and CHIPS for a new business day and ends with off-line report production and backup. Once daily EPN, and CHIPS cut-off processing is complete, reports and output data are distributed electronically according to customer instructions.

The Unisys MCP operating system software provides daily activity logs, hardware performance messages, and error diagnostic messages, which are reviewed by Network Operations management.

The North Carolina Network Operations Center group uses the Operator Schedule to document the completion of operations activities performed. The Operator Schedule provides audit trails for tasks performed by the operators during each shift. Each procedure has the indicated time to perform the procedure, and an area for the operator to initial that the procedure has been completed. The Operator Schedule is also used to record procedures performed with respect to monitoring environmental control systems status, processing status and output file reports and any issues that occurred during the shift, as well as timestamps for when certain processing began and completed, and the results or status of the processing.

The New York Network Operations Center group uses the Operator Schedule to document the evidence of activities performed. The Operator Schedule is completed by the operators to document the steps completed during the shift. Activities in the Operator Schedule include among other things environmental control systems status, processing status and Checkfiles processing results.

Both the New York and North Carolina Network Operations raise a ServiceNow Incident ticket in case there are any processing errors in both Unisys and distributed environments such as a mismatch result from Checkfiles processing for the mainframe.

As described above, the Checkfiles program is used to verify application and system software installed.

A number of management reports and performance statistics are monitored online by TCH's management with respect to transaction volumes, system response time, system utilization, and availability. A monthly management report (O&T KPI Executive Summary) provides among others, system availability, system downtime, analysis of problems encountered, and resolutions. This report is reviewed by management. In addition, an analysis is prepared for every shift. This analysis documents the time, length, and nature of processing problems. Hardware and system software problems are immediately brought to the attention of related vendors. Application software problems are immediately brought to the attention of Systems Development management.

As described above, TCH has established procedures for incident response which address the process and controls for problem/incident response, notification, escalation, logging and resolution.

IXN

IXN processing is performed automatically without manual intervention based on the availability of the transmittal files and cut-off times. Processing activities including file created, delivered by the virtual DTA, pulled by the gateway DTA, validated by the SDTA and rejected or completed, are logged in the system messages.

RTP

RTP processing is carried out 24 hours a day, 7 days a week. Because RTP runs 24/7, it does not have a traditional business day with "Start of Day" and "End of Day" processing. Instead, RTP employs reconciliation "windows". RTP processing runs 24/7 with a reconciliation window once a day configured to run at 11:59:59 pm with reports that are generated and made available to RTP customers via Connect:Direct Secure Plus.

Data replication

For EPN, CHIPS and RTP, records are written from the active database system to the local standby database in North Carolina and routed to the remote database system in Pennsylvania through the use of leased lines that allow file operations to occur between local and remote hosts. All files associated with a given processing cycle are updated and mirrored real time at both data centers. RTP transactions are written on the database locally and replicated to the remote stand by systems as they are committed into active database. Database transactions associated with RTP are updated simultaneously at both data centers. Online replication activities are monitored by Network Operations as documented in the Operator Schedules. Any issues are followed up and resolved.

EPN and CHIPS databases are backed up onto a virtual tape library (VTL) and databases containing IXN transaction history are backed up locally utilizing LiteSpeed for SQL Server tool based on a schedule and retained based on an approved retention period. BL Library (BL LIB), a tape management library system, is used to facilitate this process. Backup activities are monitored online by Network Operations as documented in the Operator Schedule. BL LIB records backup activities in the system log. Backup issues, if any, are followed

up and resolved and recorded in ServiceNow as necessary. For RTP, all servers are backed up by Avamar (for AIX servers) and NetWorker (for Red Hat Enterprise Linux (RHEL) servers) at both North Carolina and Pennsylvania data centers. A backup storage system is used to facilitate this process. The backup management system logs backup activities and any backup issues are followed up and resolved within a ServiceNow Incident ticket. RTP database environments are backed up daily using native DB2 shells scripts with 3 days of backups maintained locally on the file system including transaction logs. Backup images are archived using the Avamar system. The results of the backups, including any issues, are communicated to the DBA group via email notifications. ServiceNow tickets are opened to follow up and resolve backup issues.

It should be noted that TCH alternates the applications between data centers on a recurring basis each year to demonstrate a readiness stance for a disaster recovery situation.

TCH periodically tests and updates documented contingency procedures in connection with disaster recovery planning.

IXN

Databases containing IXN transaction history are backed up locally utilizing LiteSpeed for SQL Server tool based on a schedule and retained based on an approved retention period. The results of the backups, including any issues, are communicated to the DBA group via email. In addition, TCH uses Dell EMC Avamar for efficient backup and recovery of all servers, including replication across sites. The backup data is encrypted during transit across the network and at rest for added security. Backup activities are monitored online by Network Operations as documented in the Operator Schedules for the North Carolina and the New York Operations Centers. ServiceNow tickets are opened to document and track resolutions of issues noted as necessary. TCH periodically tests and updates documented contingency procedures in connection with disaster recovery planning.

Business continuity planning

TCH's management has developed a Business Continuity Plan document defining the essential components required to resume business operations for EPN, CHIPS, IXN and RTP.

To ensure continuous operation of all products, an alternate data center has been established with identical systems. All files are delivered in real-time to the alternate data center where a mirror image of all information is stored until needed for contingency situations. The telecommunications network is reconfigurable which gives TCH the ability to resume processing at its back-up center within one hour after the decision to relocate has been made. The TCH Business Continuity Plan (BCP) is maintained to help ensure continuous service to its customers during times of crisis.

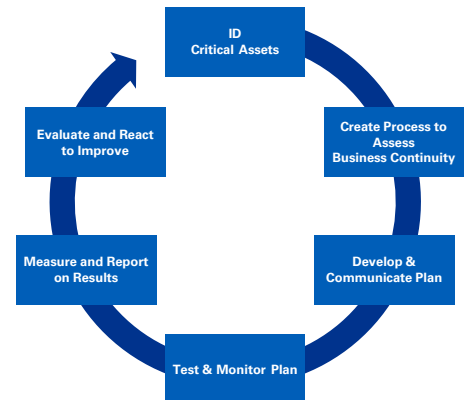
TCH's two current sites in North Carolina and New York are addressed in the existing BCP. The two Operations sites further enhance continuity effectiveness by distancing operations geographically. Geographic separation assumes that acts of terror or natural disaster are less likely to impact both sites simultaneously.

TCH business continuity preparedness cycle

The BCP planning process is constantly evolving, incorporating up to date threat contingencies and monitoring current BCP effectiveness.

During the Identification phase of Critical Business Assets and Threats, controls are developed along with test methodologies that yield measurable results.

An Enterprise Crisis and Incident Response Plan, which provides the framework for addressing major disruptions is maintained as part of the BCP. Test schedules and scripts are established for testing and examination of our contingency processes. Contingency results are reviewed by Technology and business stakeholders to eliminate or significantly reduce risks through process refinement.



Contingency plans are tested semi-annually for EPN, IXN and RTP. CHIPS contingency plans are tested quarterly. TCH Senior Management and Internal Audit review the plans annually. TCH Senior Management, TCH Audit Committee and Regulators inspect independent reports on the test results prepared by both Network Operations and Internal Audit.

BCP activation process

All operations are monitored 24x7 with regard to incident identification. Based on the type of incident encountered, information is passed to Operations Management, technology and business Executive Management and ultimately to the CEO. Once the information is processed and evaluated for urgency, a call chain to critical employees is activated. A full time open bridge line is available for conference and critical information exchange.

The type of situation and level of impact of the occurrence are taken into consideration. Assuming high severity, all TCH Managers are expected to have familiarized themselves with their Disaster Recovery Plans. Telecommunications and Operations employees should be familiar and ready to react in accordance with plans in their areas. Calls from sites can be re-routed and systems can be accessed from prearranged locations.

Employees at backup facilities are prepared to assume the responsibilities of affected counterparts. Based on the longevity of the occurrence, employees may be relocated to support the backup workforce at the discretion of TCH Management. When the disaster recovery plan is in effect, all other employees would likely be communicated with via telephone.

The emergency roles of “non critical” functions including HR, Legal, Finance and Marketing are established as part of the BCP. These functional support groups are represented at both the North Carolina and New York centers. In the event of a prolonged outage, these roles would be defined as necessary and the appropriate arrangements would be made to strengthen these support units at the working active site.

The objective of the TCH business continuity and recovery planning process is to employ the most cost-effective technologies and operational processes to support recovery goals. Recovery requirements are included in the product design process. TCH business units actively participate in the business continuity planning process. Business units and Information Technology collaborate on the best approach for recovery of each product from a system, network and business process perspective. Critical activities, specific roles that would be required after a declared event, relocation plans, and space and technology requirements are addressed and updated as required.

Disaster recovery

Primary and secondary data centers are utilized to provision a comprehensive disaster recovery arrangement. Should the primary data center be affected by a disruption, the secondary will be brought into service and communications lines are switchable from one data center to the other. To ensure the validity of this contingency plan, testing of these arrangements is conducted annually, involving a selection of clients and TCH service centers.

RTP transaction processing runs “active-active” in the North Carolina and Pennsylvania data center (which is managed and controlled by Iron Mountain). The application runs on four IBM E880 frames. Two servers are deployed in each data center. RTP services are deployed on all four, providing both intra-site and inter-site redundancy. In the event of a site outage, RTP will continue processing payments on the remaining site.

Data

TCH information must be protected and handled in a manner appropriate to its data classification and sensitivity. All information, including documents, databases and email correspondence, must be classified and handled according to its designated sensitivity level. TCH has established three levels of sensitivity for information: TCH Restricted, TCH Confidential, and Public. Appropriate procedures are implemented to ensure the protection of TCH intellectual property rights and proprietary software. To that end, non-disclosure agreements are required where appropriate. Important records are to be protected from loss, destruction, and falsification in accordance with applicable statutory, regulatory, and contractual requirements as well as the Records Retention Policy. TCH maintains procedures for the backup and retention of data. This includes legal documents and EPN, CHIPS, IXN and RTP transactional data.

EPN

TCH provides Automated Clearing House (ACH) transaction processing to customers through its Electronic Payments Network. The Automated Clearing Exchange System (ACES) is the core computerized system for EPN which processes the electronic transfer of payments between account holders at depository financial institutions.

The EPN system correlates all transaction activity and calculates credits originated, debits originated, credits received, and debits received for each settling DFI that maintains a reserve account at the Federal Reserve Bank of New York. The end of day EPN positions are transmitted to the Federal Reserve Bank of New York. The transmission identifies the settling DFI accounts to be debited or credited. A settling DFI provides data processing services and/or settles on behalf of another DFI. Advices are available at the end of each processing cycle.

TCH provides an optional feature for EPN financial institution customers, a Universal Payment Identification Code (UPIC). A UPIC represents a single customer account at a financial institution. The UPIC database contains the account holder’s Demand Deposit Account (DDA) account and the routing/transit number where the account resides. The UPIC database also contains customer name, address information and optionally customer contact information. A UPIC is a customer’s permanent electronic payment address regardless of future changes in the customer’s banking relationship. UPIC is available to all EPN financial institution customers upon completion of a UPIC registration letter.

The primary goal of UPIC is to provide a secure and scalable means for electronic payments while maintaining the anonymity of a client’s banking relationship. EPN financial institution customers can access the UPIC database through secure access over the internet or via Connect:Direct with Secure Plus. The security controls for UPIC are provided through a unique user ID and password, firewalls and VPN. All customers’ connectivity to the UPIC server is accessible through the VPN proxy (Pulse Secure Appliance). Several firewalls are in place

in various zones to filter network traffic and to separate UPIC servers from TCH's internal network. An Intrusion Detection System is implemented in different servers supporting UPIC.

Upon completion of processing for each cycle, the EPN system automatically generates output report files. When output files are available, customers can login to EPNAccess or via Connect:Direct with Secure Plus, or FTP-S to initiate a transmission job to receive their files from the EPN system.

EPN customers may elect to transmit to and receive files from TCH's data center using Connect:Direct with Secure Plus, EPNAccess, and FTP-S.

CHIPS

CHIPS is a real-time computerized system for processing and settling U.S. dollar wire payments among international and domestic banks. It is designed to facilitate payments among customers.

Customers use CHIPS to send and receive U.S. dollars for a variety of international and domestic transactions, including:

- Foreign and Domestic Trade Services – collection and reimbursement of letters of credit.
- International Loans – placement of funds and disbursement of principal and interest.
- Syndicated Loans – assembly and placement of funds and disbursement of principal and interest.
- Foreign Exchange Sales and Purchases – settlement of spot market and currency futures, and interest and currency swaps.
- Other Transactions – placement of a variety of domestic and international payment transactions such as cover payments and money market/securities related payments.

CHIPS provides real-time processing of CHIPS payment messages and controls the release of the payment messages. Throughout the business day, customers send their payments to CHIPS. A "Balance Release Algorithm" (Release Algorithm) continuously searches the transactions for unreleased payments and uses a multilateral netting scheme to match and release payments. CHIPS' ability to perform real-time netting means that very large payments can be netted earlier in the day. With real-time netting, the system continuously offsets payments between two or more customers.

Once released from CHIPS, payments are final and irrevocable, and the sending participant's obligation for the amount of the payment has been settled.

CHIPS customers' customer accounts are validated using the information in the Name and Address Database. The Name and Address Database is the database of CHIPS customers' customer accounts to which payment messages can be routed. Payment messages for which the sending customer has completed the credit party field with a valid customer account identifier are known as qualified payment messages. To help ensure efficient delivery to the ultimate receiving party (beneficiary), the vast majority of the payment messages are "qualified" where the sending participant includes one of three forms of beneficiary identification:

- Universal Identification Number (UID) – is an account identifier that is issued by CHIPS upon request of a beneficiary's bank for its customer, to eliminate the need for the beneficiary to provide its demand deposit account number to the entity sending the wire payment.
- Demand Deposit Account (DDA) – is also verifiable information if that information has been already provided to the CHIPS Name and Address Database.
- SWIFT/BIC Identifier – is issued by SWIFT and is used to identify the beneficiary's bank.

The CHIPS reporting phase is carried out according to the daily schedule. The report generation is an automated process that is executed after end-of-day processing by the CHIPS application.

During end-of-day processing, CHIPS accumulates the initial funding, supplement and final payment for each customer and calculates the final settlement amount. CHIPS balances the funding and settlement amount for accuracy and completeness of processing. This information is used for preparation of various CHIPS reports. Reports are electronically retrieved by customers on an ad-hoc basis.

IXN

Under traditional methods of check settlement, which involve the physical transportation of items between sending and receiving banks, a bank's ability to credit and debit customers' accounts is dependent on receipt of physical papers. With the Image Exchange (IXN) system, banks can view check images electronically and validate the payment information. Essential data can be processed expeditiously without concern for the limitations of paper handling.

TCH provides services governed by The Clearing House Image Exchange Network Operating Rules using the IXN system and the TCH Mainframe Settlement system. The IXN system enables banks to streamline the check settlement process by replacing the physical transport of checks with electronic check images. The IXN system is used for the electronic transfer of check images and electronic cash letters containing information about those images. The image exchange process takes place between Financial Institutions (FIs), between FIs and Third-Party Processors (acting on behalf of FIs), and between FIs and the Federal Reserve Banks (Fed) for over \$26 billion daily. IXN serves 42 participants.

The TCH Mainframe Settlement system also interfaces electronically with the Federal Reserve Bank (FRB) for transmission of settlement amounts through the National Settlement Service (NSS) provided by the Federal Reserve Banks. At the predefined cut-off time, a settlement file containing the multilateral balance of each settlement customer is transmitted from the TCH Mainframe Settlement system to the NSS at the FRB for adjustment to the customer's Federal Reserve master accounts. This completes settlement for each customer for the specified settlement time.

The IXN database is updated as processing is completed. Through SVPCOView, customers can view and generate the processing results and transaction history. Upon completion of processing, IXN and TCH Mainframe Settlement system are updated real time. Output report files are made available online and retrieved by customers through SVPCOView.

All files containing data for electronic check settlement stored on each participant's respective virtual DTA reside on TCH's EMC Symmetrix SAN which uses Advanced Encryption Standard (AES) 256 bit encryption at rest. AES is a Federal Information Processing Standard (FIPS) approved cryptographic algorithm that can be used to protect electronic data. This standard is maintained by the Department of Commerce National Institute of Standards and Technology, Information Technology Laboratory.

RTP

RTP provides consumers and businesses the ability to send and receive immediate funds transfers directly from accounts at their financial institution anytime 24 hours a day seven days a week.

RTP payments are executed through a sequence of message transmissions. A payment starts with a Payer sending a payment instruction via a channel application (such as an online or mobile banking application) provided by the Payer's FI who is a Participant in the RTP System. The Payer's FI creates an RTP Instruction Message (the payment) from the Payer's instructions which is sent to the RTP System for format validation and routing to the Payee's FI.

The RTP Instruction Message is then forwarded by the RTP system to the Payee's FI. This type of Instruction Message relays a payment instruction to the Payee's FI, which must also be an RTP Participant. The Payee's FI acknowledges receipt of the Payment and agrees to provide immediate funds availability to the Payee by creating and sending an "accept" RTP Response Message back to the RTP system which then routes the Response Message to the Payer's FI. The Payer's FI then informs the Payer of the successful completion of the Payment via their channel application.

In addition to the payment outlined above, RTP includes a number of payment-related Messages (Non-Payment Messages) that enable Payees and Payers or Payee FIs and Payer FIs to communicate data regarding a payment. A payment-related message may be a Request for Payment, a Request for Information, a Remittance Advice, a Payment Acknowledgement, or a Request for Return of Funds.

Following the end of each reconciliation window, the RTP system generates a series of standard reconciliation reports for each RTP participant. These reports include summary and detailed information on all payment activity that occurred during the applicable reconciliation window. Standard reports are electronically distributed to customers at their request. RTP provides an Internet/web-based management portal (RTP Management Console) for customers to view RTP activity, download reports, and make other configuration changes through the Internet using a secure connection.

System boundary

The boundary of the system is defined as the physical and logical perimeter of that portion of an entity's operations that is used to achieve management's specific business objectives of a system. The boundary includes all components of the system for which the entity is responsible, including those provided by vendor and other third parties.

The boundaries of the system addressed by this SOC 2® report are defined as the EPN, CHIPS, IXN, and RTP Services systems hosted by TCH in the United States on behalf of its user entities. This is limited to the system boundaries and processes covering TCH's EPN, CHIPS, IXN, and RTP infrastructure, software, people, processes, and data, as described in the sections above and includes the following layers of technology:

- The network that secures access to the system
- The hardware on which the system is housed
- The operating system used to manage the functionality of the hardware and systems installed therein
- The databases in which data is stored
- The applications in which data is processed

Relevant aspects of the control environment, risk assessment, control activities, monitoring, and information and communication

Control environment

TCH's control environment reflects the position taken by management and the Boards of Directors concerning the importance of controls and the emphasis given to controls in its policies, procedures, methods, and organizational structure.

TCH management consists of a group of Executive Vice Presidents, Senior Vice Presidents and Vice Presidents reporting to the Chief Executive Officer, who, in turn, report to the Boards of Directors of TCH.

Board of directors

Management of TCH is under the direction of two boards of directors: the Supervisory Board of Directors and the Managing Board of Directors. The Supervisory Board of Directors has overall responsibility for the business of TCH and for setting the strategic agenda, while the Managing Board of Directors, which reports to the Supervisory Board of Directors, is responsible for oversight of TCH's business and financial performance, risk management and compliance with supervisory expectations.

Members of TCH are classified into two classes, Class A and Class AA. Each Class A member is entitled to appoint one representative to the Supervisory Board and to the Managing Board of Directors. The Class AA members may collectively appoint one representative to the Managing Board of Directors only.

Human resource policies and procedures

The hiring practices of TCH are standardized and documented. All offers of employment are conditional upon the candidate successfully passing a drug screen and a background screening investigation. All employees are required to participate in the new hire orientation process. This program structures activity around general operating practices, policies and procedures. An employee performance review is conducted annually. Procedures are in place to collect company materials, deactivate card keys, and revoke physical and logical security access for terminated employees.

TCH has a formal "Code of Conduct" that must be applied in the day-to-day business at TCH. This Code of Conduct covers areas of business conduct and ethics including equal employment opportunities, outside activities, conflict of interest, confidential information, antitrust policy, ownership right, business gifts, personal finance, electronic messages, reporting questionable activity by others and conformance with laws and policies. All new employees (including vendors and contractors with access to systems) are required to sign and acknowledge that they have read and will comply with the policy and procedures. Existing employees acknowledge the Code of Conduct through annual training.

Changes in control environment

As part of ongoing operations, TCH makes changes to its operations and various support group roles and responsibilities to better align the business to service customers. This report reflects changes that have occurred during the period of this SOC 2® report.

Risk assessment

TCH has placed into operation a risk assessment process to identify and manage risks that could affect transaction processing capabilities. The TCH Managing Board of Directors, through the Enterprise Risk Management department, oversees the growth and day-to-day operations of TCH. An annual Audit Plan and Risk Assessment Evaluation process for TCH is approved by The Clearing House Audit Committee. Documentation of audit procedures and results are maintained in audit working papers and communicated through written reports to The Clearing House Audit Committee and the TCH CEO. Quarterly, The Clearing House Audit Committee reviews the status of the audit schedule, status of comments, and TCH management responses.

The Archer tool is used to document and monitor enterprise risk.

Enterprise Risk Management (ERM) department identifies, assesses, and monitors risks and reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities. These assessments include the identification and documentation of mitigating controls.

TCH holds quarterly risk assessment meetings with the Enterprise Risk Management Committee (ERMC) and Enterprise Risk Committee (ERC) to discuss potential security and availability risks including evaluating security events, environmental threats, network usage and system capacity, and risks not properly mitigated from the prior quarter. ERM is responsible for reporting risks and issues to provide transparency and escalation. Objectives are captured during these meetings and incorporated into the ongoing risk assessment process. If necessary, the change management process is initiated due to the risks discussed.

On an annual basis, assessments of external network risks are performed to identify potential impairments that could impact system security and availability. Critical, High and Medium findings are entered into Archer for tracking where criticality based on severity and likelihood as well as a remediation plan is documented. Findings are remediated based on assigned criticality and may be remediated via the change management process as applicable.

Fraud risk

Fraud risk is handled through TCH corporate policies such as the Code of Conduct that address internal fraud risk. Client level fraud risk is addressed through Operating Rules each client agrees with for each product, as well as technical controls within the applications.

For RTP, RTP Operating Rules requires a Sending Participant, when it determines that a sent RTP payment was unauthorized, to report the unauthorized payment by sending a Request for Return of Funds (RFR) message, referencing the original payment and including a FRAD (fraud) reason code. TCH RTP Operators monitor RFRs with an FRAD reason code on a daily basis and investigate select reports, which may include reaching out to both the Sending and Receiving Participants.

Control activities

TCH selects and develops control activities designed to mitigate risks to the achievement of its objectives. TCH engages in a variety of control activities as detailed throughout this section and the remainder of this

report. These control activities incorporate preventive and detective controls, including policies, procedures, systems, and people (e.g., segregation of duties, training, and communication). Supervision of activities, documented policies and procedures, peer reviews, and reconciliation of activity are examples of some of the control activities in place.

TCH selects and develops general controls over technology. TCH's mainframe and client server applications are hosted by TCH and Iron Mountain data centers on various system infrastructure platforms. Monitoring and administration of daily operations for the mainframe and applications is performed by TCH. Information security, physical and logical access controls are implemented according to established information security policies and standards. Automated technology controls are in place around physical access, environmental control systems, logical access, incident and problem management, change management, computer operations and data replication.

TCH deploys its control activities through policies and procedures.

Monitoring

TCH management and supervisory personnel monitor the quality of internal control performance as a normal part of their activities. Internal controls are evaluated and monitored on an ongoing basis by Network Operations and Payments Specialist Representatives through daily checks and validations of reports and conditions. TCH has an active security administrator and internal auditor. Departments within TCH also regularly report on their own performance to senior management. For example, Network Operations management produces monthly reports detailing computer usage and performance.

A customer satisfaction survey is conducted annually. The results of the survey are compiled and reviewed to evaluate and improve service where possible. TCH's stated goal is to receive an overall rating of at least 9.0 on a scale of 1 to 10 with 10 representing the highest rating.

The following customer service level agreement goals are also monitored by EPN management on a monthly basis, and the results are included in a performance report that is produced each month:

| Service level agreement | Goal |
|---|---------|
| ACH Processing Platform Availability (Uptime) | 99.90% |
| Output File Availability for EPN Customers | 99.50% |
| Output File Delivery to FedACH | 100.00% |
| Intra-EPN Item Investigation (within 4 hours) | 100.00% |

Note: These measurements are unique to the EPN product and are not applicable to CHIPS and IXN.

The following customer service level agreement goals are also monitored by RTP management on a monthly basis, and the results are included in a performance report that is produced each month:

| Service level agreement | Goal |
|---|--------|
| Processing Platform Availability (Uptime) | 99.90% |

Monitoring of subservice organizations

TCH uses AT&T and CenturyLink to provide transmissions services via the internet between customers and TCH.

Additionally, TCH uses a private MPLS network and transmissions services. The MPLS network is managed by AT&T. The MPLS network also utilizes CenturyLink as a second MPLS provider which AT&T manages the provider relationship for.

TCH has a dedicated AT&T account team which includes a service manager, installation manager, technical engineering specialist and sales executive. TCH and AT&T meet on a weekly basis to discuss progress on installations; planned bank site moves and changes and billing issues. The meetings are attended by Vendor Management, Network Operations Center and Client Services. TCH has an account service manager for CenturyLink and meets periodically to discuss service and any issues.

Physical security and environmental control systems for the Pennsylvania data center are managed and administered by Iron Mountain. The scope of this report does not include controls performed by Iron Mountain. TCH has contracted to receive and perform an annual review of Iron Mountain's SOC 2® report for the Iron Mountain data center services and TCH additionally performs ongoing monitoring of physical badge activity and incident management related to physical and environmental controls.

Vendor risk management

In accordance with ERM Framework, potential and existing vendor services must undergo the vendor management process which includes an onboarding risk assessment, evaluation of controls, and review over SOC reports, when available. Vendor Management performs risk assessments on specific tiered vendors on a recurring basis and is responsible for assigning a Vendor Impact Tier based on the vendor's commercial relevance and potential impact on core products and strategic initiatives. These tiers correlate to the vendor's inherent risk level, as defined by the ERM Framework.

Vendor Management assigns Vendor Relationship Owners (VROs) for each vendor to assist with performing risk assessments. Vendor Management and Information Security work with Vendor Relationship Owners (VROs) to ascertain if SLAs and performance standards are being met by vendors via scorecard and recurring risk assessments.

Regulatory review

In accordance with the Federal Financial Institutions Examination Council (FFIEC) Supervision of Significant Service Provider (SSP) program TCH is regularly examined by the Board of Governors of the Federal Reserve System ("FRB"), the Federal Deposit Insurance Corporation ("FDIC") and the Office of the Comptroller of the Currency ("OCC"). Since July 2012, TCH, as an operator of CHIPS, has been designated as a significantly important market utility under the Dodd Frank Act and, as such, the FRB has been assigned as the primary supervisor.

Internal audit

The TCH Internal Audit Group reports directly to The Clearing House Audit Committee and administratively to the CEO of TCH. The TCH Audit Group provides an independent appraisal of internal controls and management information systems to senior management. The internal audit charter provides that the auditor will not be responsible for any operational functions and authorizes the TCH Audit Group to have unrestricted access to all records, property, and personnel.

Information and communication

Information systems

The information systems relevant to the scope of this report are described in the “Software” section of this report.

TCH’s corporate network is based on Windows Active Directory. VPNs using Internet Protocol Security (IPSec) and TLS encryption, SFTP servers, and other file and data encryption methodologies are utilized to transfer data internally and between third parties. Additionally, RSA SecurID is used to authenticate users to TCH’s systems and servers.

Communication

TCH has implemented various methods of communication to ensure all TCH employees understand their individual roles and responsibilities over processing and controls, and to determine that significant events are communicated in a timely manner. Organization charts are published on the company intranet and written job descriptions have been documented for all departments. Policies and procedures are documented in The Clearing House Staff Handbook (Employee Handbook), which is distributed to all new employees and is redistributed to all existing staff if there is a revision; all department and enterprise-level policies are stored on Archer for employees to view. All Information Security policies are owned by the CISO except for the BCP policy which is owned by the Chief Risk Officer and the Physical/Environmental Security policy which is owned by Corporate Real Estate. Information Security policies are based on ISO framework. The Policy Administration Policy outlines all department and enterprise policies along with ownership and approval levels. ERM facilitates policy approvals on an annual basis.

In addition, TCH offers training and workshops to customers who purchase the NACHA rules. These workshops cover EPN fundamentals, advanced features, and new software features. These workshops are also available to all TCH personnel.

CHIPS operating rules and administrative procedures are distributed and are available on the CHIPS page of the TCH public website. Procedural guidance is available to customers and operations personnel in the CHIPS System and Operation Manual. In addition, TCH conducts a number of training workshops to assist customer institutions in the training of personnel responsible for processing entries to CHIPS. These workshops cover CHIPS fundamentals, advanced features, and new software features. These workshops are also available to all TCH personnel.

IXN membership and operating rules are available on The Clearing House’s website. Procedural guidance is available to customers and operations personnel in the IXN System and Operation Manual.

For RTP, TCH offers training and workshops to customers provided via the onboarding process, working committees, or product advocates. These workshops are also available to all TCH personnel.

TCH provides support to its customers through the Customer Services and Payment Specialist departments. In addition, personnel in the Network Operations Center are available to support customers during business hours as well as after business hours (24 x 7).

TCH prepares reports on a monthly basis to monitor and communicate the performance of operations. The reports provide performance statistics with respect to transaction volumes, system response time, system utilization, system availability, analysis of problems encountered, and resolutions. In addition, an analysis is prepared for every shift. This analysis documents the time, length, and nature of processing problems.

Hardware and system software problems are immediately brought to the attention of related vendors. Application software problems are immediately brought to the attention of Systems Development management.

TCH has established procedures for incident response as described above.

Complementary subservice organization controls

TCH uses subservice organizations to perform a range of functions. The following table describes:

- The nature of the services provided by the subservice organizations
- Each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at TCH
- The types of controls expected to be implemented at the subservice organization to meet the service commitments and system requirements based on the applicable criteria.

| Subservice organization | Services provided | Security and availability criteria intended to be met by the controls at the subservice organization | Complementary subservice organization control considerations |
|-------------------------|--|--|--|
| AT&T | TCH uses the services of AT&T for a private MPLS network and transmissions services via the internet between customers and TCH. | CC6.1, CC6.6, CC6.7, A1.2 | AT&T should have controls in place to provide reasonable assurance that the MPLS network and alternate carrier is available and secure. AT&T should have controls in place to provide reasonable assurance to provide and manage the MPLS network and services provided by AT&T and the alternate carrier. |
| CenturyLink | TCH uses the services of CenturyLink for transmissions services via the Internet between customers and TCH. | CC6.1, CC6.6, CC6.7, A1.2 | CenturyLink should have controls in place to provide reasonable assurance that the network is available and secure. |
| Iron Mountain | TCH uses the services of Iron Mountain to host and manage the Pennsylvania data center for TCH systems and applications, which has failover capabilities to and from the North Carolina data center. | CC6.4, CC6.5, A1.2 | Iron Mountain should have controls in place to provide reasonable assurance that physical access to physical assets within the data center is removed upon notification from TCH. Iron Mountain should have controls in place to provide reasonable assurance that physical access to computer equipment, storage media |

| Subservice organization | Services provided | Security and availability criteria intended to be met by the controls at the subservice organization | Complementary subservice organization control considerations |
|-------------------------|-------------------|--|--|
| | | | <p>and program documentation is authorized.</p> <p>Iron Mountain should have controls in place to provide reasonable assurance that the physical assets within the data center are protected from environmental risks.</p> |

Complementary user entity controls

TCH's system was designed with the assumption that internal controls would be placed in operation by user entities. The application of such internal controls by user entities is necessary to meet certain criteria identified in this report. There may be additional controls that would be appropriate for user entity transactions which are not identified in this report.

Throughout Section IV are descriptions of certain controls that user entities should consider to meet the criteria identified in this report. The complementary user entity controls presented throughout Section IV should not be regarded as a comprehensive list of all controls that should be employed by user entities.

Section IV Trust services criteria and The Clearing House Payments Company LLC's related controls, and KPMG LLP's test procedures and results

Completeness and accuracy of information produced by the entity

When using information produced by The Clearing House Payments Company, L.L.C., KPMG LLP evaluated whether the information was sufficiently reliable for our purposes, including, as necessary, obtaining evidence about the completeness and accuracy of the information and evaluating whether the information was sufficiently precise and detailed for our purposes. Certain controls are common to EPN, CHIPS, IXN, and RTP products and were tested as common controls.

AICPA trust services categories

This report addresses the following categories and related criteria:

- **Security (S)** – Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity’s ability to achieve its objectives.
- **Availability (A)** – Information and systems are available for operation and use to meet the entity’s objectives.

Many of the criteria used to evaluate a system are shared amongst all of the criteria; for example, the criteria related to risk management apply to the security and availability criteria. As a result, the trust services criteria consist of (1) criteria common to all five criteria (common criteria) and (2) additional principle specific criteria for the availability criteria. For the security criteria, the common criteria constitute the complete set of criteria. For the availability criteria, a complete set of criteria consists of the common criteria and the criteria applicable to the availability criteria. The common criteria are organized into the below:

- CC1.0 Control Environment
- CC2.0 Communication and Information
- CC3.0 Risk Assessment
- CC4.0 Monitoring Activities
- CC5.0 Control Activities
- CC6.0 Logical & Physical Access Controls
- CC7.0 System Operations
- CC8.0 Change Management
- CC9.0 Risk Mitigation

CC 1.0 – Common criteria related to control environment

CC1.1 – The entity demonstrates a commitment to integrity and ethical values.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|----------------------|
| CC1.1.1 | <p>Code of Conduct and Acknowledgement</p> <p>TCH has a formal “Code of Conduct” covering areas of business conduct and ethics including duty to report illegal, fraudulent, or unethical conduct. All employees are required to sign and acknowledge that they have read and will comply with the rules through an annual affidavit for the code of conduct which includes a confidentiality agreement. Existing employees acknowledge the Code of Conduct annually through online training and new employees acknowledge the Code of Conduct when they join TCH. Acknowledgement of the Code of Conduct implies conformance with all applicable laws, regulations, and TCH policies including Acceptable Use Requirements.</p> | <p>For a selection of new employees, inspected code of conduct affidavits to determine whether employees signed the code of conduct affidavit when they joined TCH.</p> <p>For a selection of existing employees, inspected the online training records that included the TCH Code of Conduct policy acknowledgement to determine whether existing employees acknowledge the Code of Conduct annually.</p> | No exceptions noted. |
| CC1.1.2 | <p>PayCo Board Code of Conduct</p> <p>The Board of Directors has a documented code of conduct via its PayCo Board Handbook (Charter, COI, Anti-Trust Compliance Policy, and Onboarding Process) and ethical standards which are reviewed annually and updated, if applicable.</p> | Inspected the PayCo Board of Directors Handbook to determine whether the PayCo Board Code of Conduct was documented and reviewed annually. | No exceptions noted. |
| CC1.1.3 | <p>Job Training and Acknowledgement of Policies</p> <p>TCH provides new employees and existing employees responsible for the design, development, implementation, operation, maintenance, and monitoring of the systems the training necessary to fulfill their responsibilities and control performance.</p> | Inspected the new personnel orientation training documentation to determine whether company-wide training as well as specific functional guidance were created to provide to new employees to give them security and availability training, and that the security awareness training included acknowledgement of all TCH policies. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| | Security awareness training includes an acknowledgement of all TCH policies including the Code of Conduct which includes duty to report illegal, fraudulent, or unethical conduct. | Inspected the existing employees training documentation to determine whether company-wide training as well as specific functional guidance were created to provide to existing employees to give them security and availability training, and that the security awareness training included acknowledgement of all TCH policies. | |
| CC1.1.4 | Background Screening Background screening is a required component of the on-boarding process for new hires and contractors. If a background check is not performed for a contractor, an attestation form is completed by the contractor/vendor's organization and retained. | Inspected the background check completion status for a selection of new employees to determine whether background checks were completed for new hires and contractors. | No exceptions noted. |
| CC1.1.5 | Employee Handbook The TCH Employee Handbook introduces and explains TCH policies, work environment, and standards in effect for all employees including personal conduct standards, company property and corrective action that will be taken due to misconduct. | Inspected the TCH Employee Handbook to determine whether the employee handbook included TCH policies, work environment, and standards in effect for all employees including personal conduct standards, company property and corrective actions that will be taken due to misconduct. | No exceptions noted. |
| CC1.1.6 | Employee Noncompliance TCH handles issues of noncompliance related to system availability and security policies as they arise. The employee is directly contacted by management and is required to take corrective action immediately. Employee noncompliance may impact performance evaluations and violations of the Code of Conduct may result in disciplinary action including termination. Reports of illegal, fraudulent, or unethical conduct can be made to management, or anonymously by mailing a written letter. | For a selection of incidents including non-compliance issues, inspected tickets and supporting documentation to determine whether the incident was escalated and resolved. Inspected the Code of Conduct to determine whether methods of reporting illegal, fraudulent, or unethical conduct and impact of violations were documented. | No exceptions noted. |

CC1.2 – The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|------------------|---|---|-------------------------|
| CC1.2.1 | <p>Board Roles, Responsibilities and Charter</p> <p>TCH sets out oversight responsibilities in its LLC Agreement, By-Laws, and in the charters for its Managing Board, Executive Committee, and other Board-level committees (Audit, Enterprise Risk, Finance, and Investment). Records are kept of the meetings of these bodies, which are provided to TCH's regulators. These bodies also engage in an annual self-assessment process to evaluate their effectiveness.</p> | <p>Inspected the LLC Agreement, By-Laws, and the Managing Board Charter, Executive Committee, and other Board-level committees (Audit, Enterprise Risk, Finance and Investment) to determine whether oversight responsibilities were outlined.</p> <p>For a selection of Board and committee meetings, inspected meeting minutes to determine whether records were kept.</p> <p>Inspected the latest self-assessment to determine whether annual self-assessments were performed.</p> | No exceptions noted. |
| CC1.2.2 | <p>Board Composition</p> <p>The Board of Directors consists solely of independent members and is comprised of one representative from each Class A Member Bank, and one representative shared amongst Class AA Member Banks. Each PayCo Board member must be a senior executive officer of a Member Bank (or an affiliate) with sufficient knowledge, authority, and influence to represent the appointing bank's multiple lines of business, and must be able to make decisions and commitments on behalf of the appointing bank.</p> | <p>Inspected the TCH PayCo Board of Directors Handbook to determine whether the composition of the PayCo Board and subcommittees was documented and the board has members who were independent from management.</p> | No exceptions noted. |
| CC1.2.3 | <p>ERMC and ERC</p> <p>The ERMC and ERC charters outline the responsibilities and information provided for the committees to ascertain risk management and status including those related to security and availability.</p> | <p>Inspected the ERMC and ERC charter to determine whether roles and responsibilities were outlined and established.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| CC1.2.4 | <p>Board Committees and Board Review of Information Security Program State</p> <p>The Board Champions of Committees (Enterprise Risk, Audit, and Finance etc.,) and the Board Champions of PayCo's Business Committees (RTP, CHIPS, EPN, and SVPCO) are allocated time during all regularly scheduled Board meetings to report on security and availability related developments relating to their respective committees that they believe rise to the level of meriting the Board's strategic attention and that are not otherwise covered in the agenda, if any. In addition, the state of TCH's information security is reviewed by the Board annually.</p> | <p>For a selection of quarters, inspected board meeting minutes to determine whether committees were allotted time on the agenda to report security and availability related developments.</p> <p>Inspected the Board of Director's Charter to determine whether the state of information security is reviewed by the board on an annual basis.</p> | No exceptions noted. |
| CC1.2.5 | <p>Board Members Background, Skills and Expertise</p> <p>The PayCo Board conducts an annual assessment of the efficacy of the Board's oversight and expertise provided.</p> <p>The Board of Directors' Charter includes the minimum background and skills required of the board (including security and availability related skills and expertise).</p> | <p>For the latest assessment, inspected the PayCo Board self-assessment documentation to determine whether an annual assessment was performed to evaluate the governance function, education and structure of the board and committees.</p> <p>Inspected the Board of Directors' Charter to determine whether minimum background and necessary expertise required was outlined.</p> | No exceptions noted. |

CC1.3 – Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| CC1.3.1 | <p>Organizational Structure and Reporting Lines</p> <p>TCH has formal organizational structures and reporting lines defined via organizational charts and organizational relationships, including an Information Security group led by the Chief Information Security Officer, and availability roles, which are available on the intranet. The organizational charts and relationships are reviewed and updated based on organizational changes. The Supervisory Board of Directors has overall responsibility for the business of TCH and for setting the strategic agenda.</p> | <p>Inspected the IT Organizational Chart on the TCH intranet, and organizational chart updates, and inquired of management to determine whether TCH has defined organizational structure and reporting lines that are updated based on organizational changes.</p> <p>Inquired of management and were informed that the Supervisory Board of Directors has the overall responsibility for the business of TCH including security and availability.</p> | No exceptions noted. |
| CC1.3.2 | <p>Policy Administration Policy</p> <p>The Policy Administration Policy outlines all department and enterprise policies along with ownership and approval levels. ERM facilitates policy approvals on an annual basis.</p> | <p>Inspected the Policy Administration Policy to determine whether procedures over the administration of policies were documented.</p> | No exceptions noted. |
| CC1.3.3 | <p>Communication of Policies and Procedures</p> <p>TCH provides personnel responsible for the design, development, implementation, operation, maintenance, and monitoring of systems the policies and procedures necessary to perform their job duties, as it relates to system security and availability. Policies and procedures are reviewed and approved annually by the Enterprise Risk Management Committee (ERMC).</p> <p>TCH employees who are responsible and accountable for system controls have the authority to ensure policies and system requirements are effectively communicated and placed into operation. All Information Security policies are owned by the CISO except for the BCP policy which is owned by the Chief Risk Officer and the Physical/Environmental</p> | <p>Inspected the posted policies and procedures to determine whether policies and procedures were available for employees responsible for the design, development, implementation, operation, maintenance, and monitoring of systems to perform their job duties, as it relates to system security and availability.</p> <p>Inspected system evidence to determine whether policies and procedures were reviewed and approved annually by the Enterprise Risk Management Committee (ERMC).</p> <p>Inquired of management and were informed that IS policies are based on the ISO framework.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|----------------------|
| | Security policy which is owned by Corporate Real Estate. Information Security policies are based on ISO framework. | | |
| CC1.3.4 | Updates to Procedures TCH has process and procedure manuals for applications, and these processes and procedures are updated in accordance with the Information Security and Availability policies. The processes and procedures documents are available to all employees on the TCH intranet. System descriptions and manuals for applications are made available to external user entities on TCH's website, permitting users to understand their role in the system. | Inspected the process and procedure manuals for EPN, CHIPS, IXN, and RTP and corresponding intranet pages to determine whether the manuals documented application processes and procedures. Inspected the revision history in the process and procedure manuals for EPN, CHIPS, IXN, and RTP to determine whether the manuals were updated in accordance with the Information Security and Availability policies. Observed TCH's website and noted system descriptions and manuals for EPN, CHIPS, IXN, and RTP were available to external user entities, permitting users to understand their role in the system. | No exceptions noted. |
| CC1.3.5 | Job Descriptions TCH has established specific job descriptions and requirements describing roles and responsibilities for all employees responsible for design, implementation, operation, maintenance, and monitoring of systems enabling TCH to meet its commitments and requirements as they relate to system security and availability. | For a selection of job titles related to security and availability, inspected job descriptions and requirements and TCH's security and availability commitments and requirements to determine whether TCH has established specific job descriptions including roles and responsibilities for employees responsible for design, development, implementation, operation, maintenance, and monitoring of systems' controls. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| CC1.3.6 | <p>Vendor Relationship Owners</p> <p>Vendor Management assigns Vendor Relationship Owners (VROs) for each vendor to assist with performing risk assessments and to assess if vendors are meeting SLAs and performance standards on a recurring basis. Vendor Management is responsible for assigning a Vendor Impact Tier based on the vendor's commercial relevance and potential impact on core products and strategic initiatives.</p> | <p>Inspected the ERM Framework to determine whether Vendor Risk Management procedures were established.</p> <p>For a selection of third-party vendors, inspected the Vendor Risk Assessments and performance scorecards to determine whether Vendor Relationship Owners were assigned to each vendor and whether risk assessments were completed on a recurring basis per specified tier and SLAs and performance standards were monitored.</p> | No exceptions noted. |
| CC1.3.7 | <p>Segregation of Duties</p> <p>TCH provides segregation of duties to effectively control the concentration of functions within the organization. The separation of Operations and Technology duties from TCH's Product Development & Management Division and other Administrative functions, which include accounting and finance, audit and human resources, provides an additional level of segregation of functions within TCH.</p> <p>Access Management training addresses segregation of duties and includes descriptions of "toxic pairs" (entitlements that should not be granted to certain roles). Management reviews and recertifies access entitlements throughout the year and reject any access entitlements that are not least privileged or segregated as appropriate. In the event that "toxic pair" entitlements are required for an individual, there is a policy exception and registration process for risk acceptance.</p> <p>Controls related to the access recertification's are documented in CC6.2.7 Periodic Access Review.</p> | <p>Inspected TCH's organizational charts and job descriptions to determine whether duties were segregated within the organization.</p> <p>Inspected TCH's Access Management Training documentation to determine whether the training addressed segregation of duties and "toxic pairs" concepts.</p> | No exceptions noted. |

CC1.4 – The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|------------------|--|---|-------------------------|
| CC1.4.1 | <p>Job Applications and Qualifications</p> <p>Job applicants complete an application and the primary HR recruiter for the region evaluates the applications and qualifications for each job applicant.</p> | For a selection of new hires, inspected applications, qualifications and job descriptions to determine whether new employees completed applications and HR evaluated applications and qualifications for each applicant. | No exceptions noted. |
| CC1.4.2 | <p>Background Screening</p> <p>Background screening is a required component of the on-boarding process for new hires and contractors. If a background check is not performed for a contractor, an attestation form is completed by the contractor/vendor's organization and retained.</p> | Inspected the background check completion status for a selection of new employees to determine whether background checks were completed for new hires and contractors. | No exceptions noted. |
| CC1.4.3 | <p>Job Training and Acknowledgement of Policies</p> <p>TCH provides new employees and existing employees responsible for the design, development, implementation, operation, maintenance, and monitoring of the systems the training necessary to fulfill their responsibilities and control performance.</p> <p>Security awareness training includes an acknowledgement of all TCH policies including the Code of Conduct which includes duty to report illegal, fraudulent, or unethical conduct.</p> | <p>Inspected the new personnel orientation training documentation to determine whether company-wide training as well as specific functional guidance were created to provide to new employees to give them security and availability training, and that the security awareness training included acknowledgement of all TCH policies.</p> <p>Inspected the existing employees training documentation to determine whether company-wide training as well as specific functional guidance were created to provide to existing employees to give them security and availability training, and that the security awareness training included acknowledgement of all TCH policies.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|----------------------|
| CC1.4.4 | Performance Reviews TCH management reviews employee performance during a formal annual review to evaluate performance of responsibilities and competency of the personnel. | Inspected the TCH Goal Setting Process document and Employee Performance Review template to determine whether it documented requirements and metrics for the review. For a selection of existing employees, inspected performance reviews to determine whether a formal annual review took place to evaluate the performance of responsibilities and competency of personnel. | No exceptions noted. |
| CC1.4.5 | Service Level Agreements and Monitoring Vendor Management and Information Security work with Vendor Relationship Owners (VROs) to monitor SLAs and performance standards via monthly performance scorecards and recurring risk assessments. | For a selection of vendors and a selection of months, inspected vendor risk assessments and performance scorecards to determine whether SLAs and performance standards were monitored for vendors. | No exceptions noted. |
| CC1.4.6 | Job Descriptions TCH has established specific job descriptions and requirements describing roles and responsibilities for all employees responsible for design, implementation, operation, maintenance, and monitoring of systems enabling TCH to meet its commitments and requirements as they relate to system security and availability. | For a selection of job titles related to security and availability, inspected job descriptions and requirements and TCH's security and availability commitments and requirements to determine whether TCH has established specific job descriptions including roles and responsibilities for employees responsible for design, development, implementation, operation, maintenance, and monitoring of systems' controls. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| CC1.4.7 | <p>Security Awareness Training</p> <p>New employees and contractors are provided individual access to the Information Security Awareness Training Program on their start date, which documents security and availability obligations. Employees are required to complete the basic awareness training within 15 days and focused training within 30 days of receiving their access to the program.</p> <p>Existing employees are required to complete the basic awareness and focused trainings annually.</p> | <p>For a selection of new employees, inspected the completed Information Security Awareness Training program documentation to determine whether the training was completed within the required timeframes.</p> <p>For a selection of existing employees, inspected completed training documentation to determine whether existing employees were required to complete training annually.</p> | No exceptions noted. |
| CC1.4.8 | <p>Succession Planning</p> <p>Succession planning for TCH is focused on senior leadership and other key roles. The plan identifies possible internal successors, or interim successors while external recruitment is completed. Training/ development notes are made for each identified successor.</p> | Inspected the Key Job Matrix and a selected critical position planning form to determine whether there was an established succession plan. | No exceptions noted. |
| CC1.4.9 | <p>Resource Management</p> <p>O&T Administration manages headcount and location of resources as well as coordinates open requisitions, roles and location, in conjunction with Corporate Real Estate Management (CREM) and HR. O&T Administration review open positions, seating, and recruitment on an ongoing basis and reconciles the active roster and open positions with HR and Finance.</p> | For a selection of months, inspected resource management documentation to determine whether O&T administration reconciled the active roster and open positions with HR and Finance. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|-----------------------------|
| CC1.4.10 | <p>Hiring Policies and Procedures</p> <p>The TCH Employee Handbook introduces and explains TCH policies, work environment, and standards in effect for all employees including personal conduct standards, company property and corrective action that will be taken due to misconduct. TCH seeks to recruit and retain a talented and diverse group of employees and ensures equal employment opportunity. TCH makes every effort to fill vacant positions with qualified employees. Employees are encouraged to explore vacant positions and career growth opportunities for retention purposes.</p> | <p>Inspected the TCH Employee Handbook to determine whether the employee handbook included TCH policies, work environment, and standards in effect for all employees including recruiting and retention efforts.</p> | <p>No exceptions noted.</p> |

CC1.5 - The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|----------------------|
| CC1.5.1 | <p>Job Descriptions</p> <p>TCH has established specific job descriptions and requirements describing roles and responsibilities for all employees responsible for design, implementation, operation, maintenance, and monitoring of systems enabling TCH to meet its commitments and requirements as they relate to system security and availability.</p> | For a selection of job titles related to security and availability, inspected job descriptions and requirements and TCH's security and availability commitments and requirements to determine whether TCH has established specific job descriptions including roles and responsibilities for employees responsible for design, development, implementation, operation, maintenance, and monitoring of systems' controls. | No exceptions noted. |
| CC1.5.2 | <p>Employee Noncompliance</p> <p>TCH handles issues of noncompliance related to system availability and security policies as they arise. The employee is directly contacted by management and is required to take corrective action immediately. Employee noncompliance may impact performance evaluations and violations of the Code of Conduct may result in disciplinary action including termination.</p> <p>Reports of illegal, fraudulent, or unethical conduct can be made to management, or anonymously by mailing a written letter.</p> | <p>For a selection of incidents including non-compliance issues, inspected tickets and supporting documentation to determine whether the incident was escalated and resolved.</p> <p>Inspected the Code of Conduct to determine whether methods of reporting illegal, fraudulent, or unethical conduct and impact of violations were documented.</p> | No exceptions noted. |
| CC1.5.3 | <p>Annual Merit and Bonus Structure</p> <p>Annual merit and bonus process aligned with the individual performance review process. Discretionary compensation is provided based on organizational performance. Successful completion of employee annual goals can influence the merit and bonus compensation decisions made by management. Merit and bonus recommendations are made annually by management, and reviewed by SVP of HR.</p> | <p>Inspected the annual compensation process outline to determine whether annual merit and bonus processes were documented.</p> <p>For the latest annual merit and bonus process, inspected an excerpt of the annual bonus process to determine whether recommendations were reviewed and approved by the SVP of HR.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| CC1.5.4 | <p>Performance Goals and Objectives</p> <p>The PayCo board reviews and approves company goals, TCH management then determines product objectives for the year and product team management incorporates into individual team goals.</p> <p>The PayCo board assesses TCH management team and reviews performance against those goals on an annual basis. This review scorecard drives annual bonus compensation for both TCH and for the product team.</p> | Inspected responsibilities within the Board charter, annual scorecard and strategic plans to determine whether the board reviewed and approved goals, objectives, and strategies as well as reviewed performance scorecards on an annual basis. | No exceptions noted. |
| CC1.5.5 | <p>Performance Reviews</p> <p>TCH management reviews employee performance during a formal annual review to evaluate performance of responsibilities and competency of the personnel.</p> | <p>Inspected the TCH Goal Setting Process document and Employee Performance Review template to determine whether it documented requirements and metrics for the review.</p> <p>For a selection of existing employees, inspected performance reviews to determine whether a formal annual review took place to evaluate the performance of responsibilities and competency of personnel.</p> | No exceptions noted. |
| CC1.5.6 | <p>Functional Department Responsibilities</p> <p>Organization charts and job descriptions exist for each function within TCH. TCH's system is supported by the key functions described in Section III of this report under Components of the System.</p> | Inspected TCH's organizational charts and job descriptions to determine whether functional department responsibilities were defined within the organization. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC1.5.7 | <p>Risk Management</p> <p>Risk Management responsibilities are outlined by the ERM Framework and supporting procedures; risks and controls are housed within Archer. The Archer platform is used to monitor, track, and log, findings, remediation plans, metrics, policies, and controls. ERM reviews and approves findings and remediation plans prior to closure in Archer to ensure the issues/risk has been addressed appropriately.</p> | <p>Inspected the ERM framework to determine whether risk management responsibilities and procedures were outlined.</p> <p>Inspected the Archer tool to determine whether it was used to monitor, track, log findings, remediation plan, risk metrics and policies and that ERM reviewed and approved findings and remediation plans prior to closure.</p> | No exceptions noted. |

CC 2.0 – Common criteria related to communication and information

CC2.1 – The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC2.1.1 | <p>Security Administration and Security Violations</p> <p>ArcSight is used to support security administration including managing security violations for both mainframe and distributed environments. Security related activities such as user data change, file security attribute change and security violations including inappropriate user activity, unauthorized software, virus and firewall alerts are captured, logged and reported using ArcSight. ArcSight is configured to capture the defined security related activities and send an alert to the Information Security responsible personnel through the Information Security workstation and to their mobile phones when there is an event that meets the defined criteria such as possible security violation. Each alert is reviewed and triaged by the managed security service provider, Cipher, and followed up and cleared by Information Security, as necessary. On an ongoing basis, the Information Security responsible personnel reviews the alerts and other activities to determine that alerts were responded to appropriately. Alerts remain pending in ArcSight until they are resolved.</p> | <p>Inspected the configuration for alert event setup in ArcSight to determine whether ArcSight was setup to capture and log the security related events such as user data change, file security attribute change and security violation including inappropriate user activity, unauthorized software, IDS, virus and firewall alerts and sends automatic alerts to Cipher, and the Information Security Analyst when an event that met the defined condition occurred.</p> <p>Observed online ArcSight alert messages on the ArcSight workstation located in a secure area of the Information Security group and noted Information Security responded to the alert in ArcSight and that alert remained pending until it was resolved.</p> <p>For a selection of months, inspected a selected ArcSight violation report to determine whether the security violations were captured and retained in ArcSight.</p> | No exceptions noted. |
| CC2.1.2 | <p>System Components Inventory</p> <p>ServiceNow is used to provide a single system of record for system components and supports management of IT Asset and Configuration Items. The Asset Management module within ServiceNow is used to manage asset information for IT Assets throughout its lifecycle from request to disposal and aids in determining criticality of the asset. Service Catalog workflows in ServiceNow are used to support the procurement, receive and retirement of IT Assets. TCH also uses the Configuration Management Database (CMDB) in</p> | <p>Inspected the CMDB configuration to determine whether IT assets were managed throughout their lifecycle.</p> <p>Inspected the ServiceNow discovery IP range list and discovery schedule list to determine whether IT servers and IT assets were tracked.</p> <p>Refer to CC7.1.9 for testing over the new IT asset discovery.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|----------------------|
| | ServiceNow to manage configuration items throughout its lifecycle from operational to out of service. Maintaining the Asset Management module allows an inventory of assets which is used in threat management. To keep configuration items up to date in the CMDB, ServiceNow Discovery is used to automate CI population into the CMDB. ServiceNow Discovery uses conventional techniques and technology to extract information from computers and other devices. | | |
| CC2.1.3 | System Availability Metrics System availability and network usage by system are tracked, summarized and reported in the monthly management report. For any breached threshold over application uptime, a ServiceNow ticket is escalated to the designated group for follow-up and resolution. Once an incident is resolved, the ticket is closed. | For a selection of months, inspected the monthly management reports to determine whether the systems and network statistics were tracked and summarized to management and for breached thresholds, if any, inspected the ServiceNow ticket to determine whether the issue was escalated to the designated group for follow-up and resolution, and ticket was closed. | No exceptions noted. |
| CC2.1.4 | Availability Monitoring TCH utilizes third-party tools to monitor performance, memory and disk space in the distributed systems environment to help ensure systems are fully functional. Automated email alerts are sent to operations management in the event of capacity and availability issues, risks are analyzed and appropriate corrective action is taken via the standard incident management process. | Inspected the monitoring tool configurations and an email notification and noted the tool was configured to distribute automated email alerts to Network Operations based on established performance rules and thresholds. Refer to CC7.4.3 Problems Reporting and Tracking for test results of incident reporting and tracking within ServiceNow. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|-----------------------------|
| CC2.1.5 | <p>Vulnerability Scans</p> <p>Weekly vulnerability scans over the network and servers are completed to identify any potential security threats that would impair system security and availability. Risks are then analyzed and appropriate corrective action is taken to address the security and availability risks identified through weekly vulnerability meetings. If necessary, the change management process is initiated as a result of any findings.</p> | <p>For a selection of weeks, inspected vulnerability scans and meeting invites and meeting minutes to determine whether the scans were completed, potential security and availability threats were identified, risks were analyzed and mitigation strategies were developed.</p> | <p>No exceptions noted.</p> |
| CC2.1.6 | <p>Intrusion Detection System</p> <p>The TCH networks include an Intrusion Detection System (IDS), CarbonBlack. This system detects and classifies suspicious events according to a library of signatures provide by the vendor. The IDS/IPS is programmed to send alerts when thresholds for particular attack signatures are exceeded. Information Security management are alerted of intrusion activities. Incidents noted are recorded in ArcSight and depending on the nature and type of problem, the incident is escalated to the designated group for follow-up and resolution. If necessary, corrective action is taken via updates to policies and/or the change management process due to the alerts.</p> <p>CarbonBlack is configured to generate alerts through ArcSight.</p> <p>Controls related incidents analysis and resolution are documented in CC7.4.4 Security Administration and Security Violations.</p> | <p>For a selection of servers, inspected the CarbonBlack management console to determine whether CarbonBlack was configured to monitor traffic.</p> <p>For a selection of incidents, inspected tickets and supporting documentation to determine whether the incident was escalated and resolved.</p> <p>Inspected configured threat intelligence library in CarbonBlack to determine whether the system was configured to detect and classify events according to the signatures.</p> <p>Inspected ArcSight management console to determine whether ArcSight was configured to alert Information Security in case of potential threats.</p> <p>Inspected the list of users with administrator access to CarbonBlack, job titles, and inquired of the management to determine whether administrative access to CarbonBlack was restricted to authorized personnel.</p> | <p>No exceptions noted.</p> |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|----------------------|
| | | <p>Inquired of Information Security management regarding policy and process updates and were informed corrective action was taken via updates to policies and/or the change management process due to the alerts.</p> <p>Refer to CC7.4.4 Security Administration and Security Violations for test results of incident analysis and resolution for ArcSight.</p> | |
| CC2.1.7 | <p>Information for Control Performance</p> <p>Information necessary for the operation of control activities is provided to TCH personnel via policies and procedures and control procedures to carry out their responsibilities.</p> | <p>Inspected the TCH intranet page and Archer for the posted policies and procedures to determine whether policies and procedures were available for employees responsible for the design, development, implementation, operation, maintenance, and monitoring of systems to perform their job duties, as it relates to system security and availability.</p> <p>Performed inspection of control descriptions and control procedures stored in Archer, observation and inquiry procedures for the controls specified by management to determine whether information necessary for the operation of control activities was provided to the control performer.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|----------------------|
| CC2.1.8 | <p>Monitoring for Vulnerabilities and Patches</p> <p>The TCH Vulnerability Management procedures include the following:</p> <p>Third-party software inspection and vulnerability management systems are used to notify TCH system administrators of the discovery of new vulnerabilities and availability of patches. Third-party and industry groups (e.g., FS-ISAC & US-CERT) broadcast notifications of new vulnerabilities on a periodic and ad-hoc basis. Notifications are actioned upon as needed by IS personnel for applicability to the current TCH environment.</p> | <p>Inspected the TCH Vulnerability Management procedures document to determine whether it included procedures to notify TCH system administrators of the discovery of new vulnerabilities and availability of patches.</p> <p>Inspected a selection of vendor notifications to determine whether TCH received third-party notifications of new vulnerabilities</p> <p>For a selection of vendor notifications, inspected documentation to determine whether corrective action was taken as needed by IS personnel.</p> | No exceptions noted. |
| CC2.1.9 | <p>Information Security Reporting</p> <p>IS metrics and known vulnerabilities, remediation plans, hardening compliance and security awareness is collated and communicated on a monthly basis to the CISO for review and in order to inform management decisions relating to the identification and assessment of IS risks, and evaluate incidents and detection/monitoring procedures.</p> | <p>For a selection of months, inspected the meeting invite and IS metrics reporting package to determine whether IS reporting was communicated to the CISO for review.</p> | No exceptions noted. |

CC2.2 – The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC2.2.1 | <p>Communication of Policies and Procedures</p> <p>TCH provides personnel responsible for the design, development, implementation, operation, maintenance, and monitoring of systems the policies and procedures necessary to perform their job duties, as it relates to system security and availability. Policies and procedures are reviewed and approved annually by the Enterprise Risk Management Committee (ERMC).</p> <p>TCH employees who are responsible and accountable for system controls have the authority to ensure policies and system requirements are effectively communicated and placed into operation. All Information Security policies are owned by the CISO except for the BCP policy which is owned by the Chief Risk Officer and the Physical/Environmental Security policy which is owned by Corporate Real Estate. Information Security policies are based on ISO framework.</p> | <p>Inspected the posted policies and procedures in Archer to determine whether policies and procedures were available for employees responsible for the design, development, implementation, operation, maintenance, and monitoring of systems to perform their job duties, as it relates to system security and availability.</p> <p>Inspected system evidence to determine whether policies and procedures were reviewed and approved annually by the Enterprise Risk Management Committee (ERMC).</p> <p>Inquired of management and were informed that IS policies are based on the ISO framework.</p> | No exceptions noted. |
| CC2.2.2 | <p>Updates to Policies</p> <p>TCH management reviews, applies updates for new threats and changes, and approves Information Security policies and related availability policies periodically. The policies are available to all employees in Archer.</p> | <p>Inspected the Information Security policies and other availability policies and Archer to determine whether they addressed the relevant security and availability attributes and included the annual revisions performed and reviewed by management.</p> <p>Inspected screenshots from Archer to determine whether policies were available to all employees.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|----------------------|
| CC2.2.3 | <p>Updates to Procedures</p> <p>TCH has process and procedure manuals for applications, and these processes and procedures are updated in accordance with the Information Security and Availability policies. The processes and procedures documents are available to all employees on the TCH intranet. System descriptions and manuals for applications are made available to external user entities on TCH's website, permitting users to understand their role in the system.</p> | <p>Inspected the process and procedure manuals for EPN, CHIPS, IXN, and RTP and corresponding intranet pages to determine whether the manuals documented application processes and procedures.</p> <p>Inspected the revision history in the process and procedure manuals for EPN, CHIPS, IXN, and RTP to determine whether the manuals were updated in accordance with the Information Security and Availability policies.</p> <p>Observed TCH's website and noted system descriptions for EPN, CHIPS, IXN, and RTP were communicated to external user entities, permitting users to understand their role in the system.</p> | No exceptions noted. |
| CC2.2.4 | <p>Communication of Job Descriptions</p> <p>TCH has established specific job descriptions and requirements describing roles and responsibilities for all employees responsible for design, implementation, operation, maintenance, and monitoring of systems enabling TCH to meet its commitments and requirements as they relate to system security and availability. Job descriptions are provided to employees during the hiring process. There are no external users with this type of responsibility.</p> | <p>For a selection of job titles relating to security and availability, inspected job descriptions and requirements and TCH's security and availability commitments and requirements to determine whether TCH has established specific job descriptions including roles and responsibilities for employees responsible for design, development, implementation, operation, maintenance, and monitoring of systems' controls.</p> <p>For a selection of new hires, inspected applications and job descriptions to determine whether job descriptions were communication during the hiring process.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| CC2.2.5 | Periodic Management Meetings TCH management and the Board of Directors meet quarterly to communicate security and availability related information that is needed to fulfill their roles with respect to the achievement of TCH's service commitments and system requirements. | For a selection of quarters, inspected board meeting minutes to determine whether TCH management and the Board of Directors meet quarterly to communicate security and availability related information. | No exceptions noted. |
| CC2.2.6 | Board of Director Meetings, Agendas and Frequency The PayCo Board meets quarterly and the Chair can call special meetings at his/her discretion. The Board Chair and the Chief Executive Officer of PayCo jointly set the agenda for each Board meeting. Any Board member may request that an item be added to the agenda. | Inspected the PayCo Board Handbook to determine whether Board meetings were scheduled on a quarterly basis. For a selection of quarters, inspected meeting agenda and minutes to determine whether necessary parties were allotted time for updates. | No exceptions noted. |
| CC2.2.7 | Board Committees and Board Review of Information Security Program State The Board Champions of Committees (Enterprise Risk, Audit, and Finance etc.,) and the Board Champions of PayCo's Business Committees (RTP, CHIPS, EPN, and SVPCO) are allocated time during all regularly scheduled Board meetings to report on security and availability related developments relating to their respective committees that they believe rise to the level of meriting the Board's strategic attention and that are not otherwise covered in the agenda, if any. In addition, the state of TCH's information security is reviewed by the Board annually. | For a selection of quarters, inspected board meeting minutes to determine whether committees were allotted time on the agenda to report security and availability related developments. Inspected the Board of Director's Charter to determine whether the state of information security is reviewed by the board on an annual basis. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| CC2.2.8 | Internal Audit Reporting Internal Audit provides periodic reports to the Audit Committee, the Board and senior management summarizing the status of the Audit Plan, results of audit activities, and details of any significant issues identified. Quarterly meetings are held with the Audit Committee. | For a selection of quarters, inspected Audit Committee meeting materials to determine whether Internal Audit reported the status, results and issues to the Audit Committee, Board and senior management. | No exceptions noted. |
| CC2.2.9 | Risk Meetings At a minimum, TCH holds quarterly risk meetings with the Enterprise Risk Management Committee (ERMC) and Enterprise Risk Committee (ERC) to discuss potential security and availability risks including evaluating security events, environmental threats, network usage and system capacity, and risks not properly mitigated from the prior quarter. ERM is responsible for reporting risks and issues to provide transparency and escalation. Objectives are captured during these meetings and incorporated into the ongoing risk assessment process. If necessary, the change management process is initiated due to the risks discussed. | For a selection of quarters, inspected risk meeting minutes to determine whether risk meetings were held with the Risk Management Committee (ERMC) and Enterprise Risk Committee (ERC), security and availability risks were discussed (including security events, environmental threats, network usage and system capacity, and risks not properly mitigated), objectives were captured, and if necessary, the change management process was initiated due to the risks. Inspected the ERM framework to determine whether ERM is responsible for reporting risks and issues. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC2.2.10 | <p>Change Advisory Board Meetings</p> <p>TCH holds a bi-weekly Change Advisory Board meeting to discuss changes, including environmental, regulatory and technological changes that affect system security and availability. Controls, policies and procedures are updated as needed based on the meeting discussions.</p> | <p>For a selection of weeks, inspected the change request report used in the bi-weekly Change Advisory Board meetings to determine whether changes, including environmental, regulatory and technological changes that affect system security and availability were discussed.</p> <p>Inquired of the VP of Information Security and VP of Operations Services and were informed that no updates were made to controls, policies, and procedures affecting security and availability during the period as a result of the Change Advisory Board meetings.</p> | No exceptions noted. |
| CC2.2.11 | <p>Network Engineering Meetings</p> <p>Network group management meets weekly to discuss needs for upgrades or changes in the network devices and configuration.</p> | <p>For a selection of weeks, inspected the network group management weekly calendar invite and meeting minutes to determine whether the group met to discuss needs for upgrades or changes in the network devices and configuration.</p> | No exceptions noted. |
| CC2.2.12 | <p>Asset Classification</p> <p>TCH has policies that document requirements on removable media and asset classifications. The policies are reviewed and updated annually by the Information Security leadership team in accordance with the Information Security policies. TCH has an asset classification and management policy which establishes three levels of data classification standards which are used to help restrict access to information:</p> <p>TCH Restricted:</p> <p>Information that, if publicly disclosed, altered or destroyed without appropriate authorization, could result in severe financial loss or reputational damage to TCH. In the case of a document or email that contains information of varying sensitivity levels, the highest sensitivity level must be applied</p> | <p>Inspected the following policy documents to determine whether they documented requirements on removable information and assets and the policy documents were updated and reviewed annually by TCH leadership.</p> <ul style="list-style-type: none"> • Asset Classification and Management Policy • Physical and Environment Security Policy <p>Inspected the asset classification and management policy to determine whether it documented the three levels of data classification standards and was updated and reviewed annually by the Information Security leadership team.</p> <p>Inspected a selection of sensitive, internal, and customer-facing documents maintained by TCH to</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| | <p>to the entire document or email. Except as otherwise set forth in the Information Classification Guidelines, no circulation is permitted outside of TCH without prior authorization of an Executive Vice President or above and the Legal department.</p> <p>TCH Confidential:</p> <p>Information that, if publicly disclosed, altered or destroyed without appropriate authorization, could result in moderate financial loss or reputational damage to TCH. Information that does not clearly fall within the TCH Restricted or Public designations should be designated TCH Confidential. Except as otherwise set forth in the Information Classification Guidelines, no circulation is permitted outside of TCH without prior authorization of Senior Vice President or above.</p> <p>Public:</p> <p>Information that is intended for public dissemination or, if publicly disclosed, altered or destroyed without authorization, would result in no financial loss or reputational damage to TCH. Data can be circulated outside of TCH.</p> | determine whether asset classification types for levels of data classification were established. | |
| CC2.2.13 | <p>Problems Reporting and Tracking</p> <p>TCH has established incident response procedures which are documented in the TCH Incident Management Process Framework. TCH uses ServiceNow tickets to record incidents.</p> <p>Depending on the nature and type of incident, the ServiceNow ticket is escalated to the designated group for follow up and resolution. Once an incident is resolved, the ticket is closed.</p> | <p>Inspected the TCH Incident Management Process Framework document to determine whether procedures for incident responses, including roles and responsibilities, were documented.</p> <p>For a selection of incidents, inspected the ServiceNow tickets to determine whether the resolution of the incidents was recorded in the ServiceNow tickets.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|--|
| CC2.2.14 | <p>Security Breaches and Response</p> <p>TCH employees are required to report breaches to management as dictated by the Information Security policies. Information Security staff will prepare a security incident report and ticket that includes the incident details and resolution. Each incident report is reviewed and resolved by the Incident Response Team in accordance with the response procedures documented in the Incident Response Plan.</p> <p>Contractors, and third-party users of information systems and services are required to note and report any observed or suspected IS incidents. These requirements are communicated during client onboarding or in third-party agreements.</p> <p>In the event that the incident involves the unauthorized access to, or use of sensitive information, the Incident Response Team is responsible for notifying the appropriate affected parties, regulatory agencies, and law enforcement a timely manner in accordance with applicable product rules and as required by applicable laws.</p> | <p>Inspected the IS Incident Management and IS Communication and Operations Management policies and Incident Response Plan to determine whether they documented requirements for employees, contractors and third-party users to report security breaches to management and response procedures for the Incident Response Team.</p> <p>Inspected the security incident reports and tickets, and inquired of management, and noted that there were no security breach incidents during the period; therefore, the operating effectiveness of this part of the control could not be tested.</p> | <p>Noted that there were no security breach incidents during the period; therefore, the operating effectiveness of this control could not be tested.</p> |
| CC2.2.15 | <p>Availability Monitoring</p> <p>TCH utilizes third-party tools to monitor performance, memory and disk space in the distributed systems environment to help ensure systems are fully functional. Automated email alerts are sent to operations management in the event of capacity and availability issues, risks are analyzed and appropriate corrective action is taken via the standard incident management process.</p> | <p>Inspected the monitoring tool configurations and an email notification and noted the tool was configured to distribute automated email alerts to Network Operations based on established performance rules and thresholds.</p> <p>Refer to CC7.4.3 Problems Reporting and Tracking for test results of incident reporting and tracking within ServiceNow.</p> | <p>No exceptions noted.</p> |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| CC2.2.16 | <p>Security Administration and Security Violations</p> <p>ArcSight is used to support security administration including managing security violations for both mainframe and distributed environments. Security related activities such as user data change, file security attribute change and security violations including inappropriate user activity, unauthorized software, virus and firewall alerts are captured, logged and reported using ArcSight. ArcSight is configured to capture the defined security related activities and send an alert to the Information Security responsible personnel through the Information Security workstation and to their mobile phones when there is an event that meets the defined criteria such as possible security violation. Each alert is reviewed and triaged by the managed security service provider, Cipher, and followed up and cleared by Information Security, as necessary. On an ongoing basis, the Information Security responsible personnel reviews the alerts and other activities to determine that alerts were responded to appropriately. Alerts remain pending in ArcSight until they are resolved.</p> | <p>Inspected the configuration for alert event setup in ArcSight to determine whether ArcSight was setup to capture and log the security related events such as user data change, file security attribute change and security violation including inappropriate user activity, unauthorized software, IDS, virus and firewall alerts and sends automatic alerts to Cipher, and the Information Security Analyst when an event that met the defined condition occurred.</p> <p>Observed online ArcSight alert messages on the ArcSight workstation located in a secure area of the Information Security group and noted Information Security responded to the alert in ArcSight and that alert remained pending until it was resolved.</p> <p>For a selection of months, inspected a selected ArcSight violation report to determine whether the security violations were captured and retained in ArcSight</p> | No exceptions noted. |
| CC2.2.17 | <p>Customer Agreements</p> <p>TCH maintains agreements established between TCH and customers that outline TCH's commitments, as well as users' responsibilities. These agreements are reviewed and approved by TCH and the customer upon onboarding.</p> | <p>For a selection of new customers added during the period, inspected the agreement to determine whether it was reviewed and approved by TCH and the customer, and documented TCH's commitments, as well as users' responsibilities.</p> <p>For a selection of existing customers, inspected the agreements to determine whether they were maintained by TCH.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC2.2.18 | <p>Subservice Organization Agreements</p> <p>TCH maintains agreements established between TCH and subservice organizations that outline security and availability commitments, as well as the subservice organizations' responsibilities. These agreements are reviewed and approved by TCH and the organizations upon establishment. Updates and modifications to contracts and commitments are assessed as part of the contract management and vendor risk assessment process.</p> <p>Controls related to vendor risk assessment are described in CC9.2.3 Vendor Risk Management.</p> | <p>Inquired of Vendor Management and were informed that there were no new subservice organization agreements during the period; therefore, the operating effectiveness of this part of the control could not be tested.</p> <p>For a selection of existing subservice organizations, inspected the agreements to determine whether they were maintained by TCH.</p> | No exceptions noted. |
| CC2.2.19 | <p>Confidentiality Agreements and Information Handling Requirements</p> <p>TCH Legal review contracts with confidentiality obligations or information handling requirements to ensure the obligations imposed are consistent with existing practices and policies.</p> | Inspected the Contract Authority Policy to determine whether legal review requirements were outlined. | No exceptions noted. |
| CC2.2.20 | <p>Communication of System Description</p> <p>TCH has provided an objective description of the system and its boundaries and communicated the description to authorized internal and external system users.</p> | <p>Inspected the system description for EPN, CHIPS, IXN, and RTP to determine whether they describe the system and its boundaries and were defined for authorized internal and external system users.</p> <p>Observed the TCH intranet page where the EPN, CHIPS, IXN, and RTP services system descriptions were stored and noted they were available to authorized internal users.</p> <p>Observed the TCH website and noted system descriptions for EPN, CHIPS, IXN, and RTP were communicated to external user entities.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC2.2.21 | <p>Communication of Changes – Security and Availability Requirements</p> <p>Changes that impact EPN, CHIPS, IXN, and RTP are communicated to and approved by business and IT personnel, as required, before they are implemented in the production environment. As part of the communication, formal documentation is prepared by O&T and Systems Development which detail the security and availability requirements. All software upgrade and install related communication is done internally by the platform support team and externally by the client services team.</p> | Inspected change documentation for a selection of application, DB and operating system changes, to determine whether the documentation included security and availability requirements and changes were approved by appropriate business and IT personnel prior to implementation. | No exceptions noted. |
| CC2.2.22 | <p>Risk Management</p> <p>Risk Management responsibilities are outlined by the ERM Framework and supporting procedures; risks and controls are housed within Archer. The Archer platform is used to monitor, track, and log, findings, remediation plans, metrics, policies, and controls. ERM reviews and approves findings and remediation plans prior to closure in Archer to ensure the issues/risk has been addressed appropriately.</p> | <p>Inspected the ERM framework to determine whether risk management responsibilities and procedures were outlined.</p> <p>Inspected the Archer tool to determine whether it was used to monitor, track, log findings, remediation plan, risk metrics and policies and that ERM reviewed and approved findings and remediation plans prior to closure.</p> | No exceptions noted. |
| CC2.2.23 | <p>Information Security Reporting</p> <p>IS metrics and known vulnerabilities, remediation plans, hardening compliance and security awareness is collated and communicated on a monthly basis to the CISO for review and in order to inform management decisions relating to the identification and assessment of IS risks, and evaluate incidents and detection/monitoring procedures.</p> | For a selection of months, inspected the meeting invite and IS metrics reporting package to determine whether IS reporting was communicated to the CISO for review. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|---|---|-------------------------|------------------|
| Complementary User Entity Control(s) | | | |
| <p>Controls should be established at user entities so that:</p> <ul style="list-style-type: none"> User entities are responsible for providing information on how to report issues, failures, incidents, etc., to TCH in the event of a security or availability issue to its users. | | | |

CC2.3 – The entity communicates with external parties regarding matters affecting the functioning of internal control.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|------------------|---|---|-----------------------------|
| CC2.3.1 | <p>External Communications Regarding Security and Availability</p> <p>TCH communicates with participants and vendors through multiple channels. This includes email distribution, document distribution, through secure website, and various committees.</p> | <p>Inspected a selection of business committee communication, and email bulletins to determine whether TCH communicated to external users and vendors regarding security and availability through multiple channels.</p> | <p>No exceptions noted.</p> |
| CC2.3.2 | <p>Customer Agreements</p> <p>TCH maintains agreements established between TCH and customers that outline TCH's commitments, as well as users' responsibilities. These agreements are reviewed and approved by TCH and the customer upon onboarding.</p> | <p>For a selection of new customers added during the period, inspected the agreement to determine whether it was reviewed and approved by TCH and the customer, and documented TCH's commitments, as well as users' responsibilities.</p> <p>For a selection of existing customers, inspected the agreements to determine whether they were maintained by TCH.</p> | <p>No exceptions noted.</p> |
| CC2.3.3 | <p>Communication of Changes, Scheduling Maintenance/Downtime</p> <p>Changes affecting system security and availability are communicated via email to management and end users. Planned outages require at least two weeks' notice.</p> <p>Client Services sends bulletins to the customers describing upcoming system changes such as application releases and any downtime, if expected. For RTP, new release bulletins include the RTP Supplement to Functional Documentation that describes a list of client impacting defects, issues, or considerations and provides an update to the list with each major release.</p> | <p>Inspected the Incident Management policy to determine whether the policy requires TCH to notify applicable parties in the event of a system change or availability event.</p> <p>For a selection of changes, inspected bulletins to determine whether customers were sent communication regarding upcoming system changes, application releases, or any downtime if expected, as applicable.</p> | <p>No exceptions noted.</p> |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|----------------------|
| CC2.3.4 | External Reporting Reporting to regulatory oversight parties occurs on a recurring basis across all products. Recurring committee reporting regarding risk are compiled by the TCH Risk Office and provided to the applicable external committees (ERC, PayCo, Audit). TCH addresses issues noted from regulatory examinations to the satisfaction of the examiners. | For a selection of months, inspected the meeting invitation, attendees and agenda to determine whether a recurring meeting with the regulators was scheduled. Inquired of management and was informed that the meetings were held as noted on the invites and issues identified by the regulators were discussed. For a selection of quarters, inspected Audit Committee meeting materials to determine whether issues noted from regulatory examinations were tracked by Internal Audit and reported to the Audit Committee. | No exceptions noted. |
| CC2.3.5 | Subservice Organization Agreements TCH maintains agreements established between TCH and subservice organizations that outline security and availability commitments, as well as the subservice organizations' responsibilities. These agreements are reviewed and approved by TCH and the organizations upon establishment. Updates and modifications to contracts and commitments are assessed as part of the contract management and vendor risk assessment process. Controls related to vendor risk assessment are described in CC9.2.3 Vendor Risk Management. | Inquired of Vendor Management and were informed that there were no new subservice organization agreements during the period; therefore, the operating effectiveness of this part of the control could not be tested. For a selection of existing subservice organizations, inspected the agreements to determine whether they were maintained by TCH. | No exceptions noted. |
| CC2.3.6 | Customer Feedback and Surveys Participants and vendors can contact TCH through multiple channels including customer service, dedicate representatives for banks and vendors. TCH business committees provide feedback that rolls up to the PayCo Board. The PayCo Board can then influence the direction of the company and senior management. In addition, other committees including the Vendor Working Group, Technology Working Group, and | Inspected the annual survey communication email and the annual survey to determine whether the annual survey was sent to customers. Inspected the TCH scorecard summary analysis to determine whether the results of the survey were prepared and analyzed by management and goals were documented. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| | ERMC report upwards. Depending on the committee, they may meet monthly, quarterly (PayCo Board), or more frequently as needed. TCH also conducts an annual customer survey that is sent to customers and results may drive annual goals. | | |
| CC2.3.7 | Communication of System Description TCH has provided an objective description of the system and its boundaries and communicated the description to authorized internal and external system users. | Inspected the system description for EPN, CHIPS, IXN, and RTP to determine whether they describe the system and its boundaries and were defined for authorized internal and external system users. Observed the TCH intranet page where the EPN, CHIPS, IXN, and RTP services system descriptions were stored and noted they were available to authorized internal users. Observed the TCH website and noted system descriptions for EPN, CHIPS, IXN, and RTP were communicated to external user entities. | No exceptions noted. |
| CC2.3.8 | Changes to Commitments – External Any changes in commitments are communicated through either technical specifications or operating rules (published annually, or as new functionality is made available or defects are resolved with a release). Any agreement changes are communicated via Legal and product to Participants for execution. Customers receive notice of changes and rules are made publicly available. For changes in commitments to vendors, any such changes would be renegotiated consistent with the controls identified. | Inspected technical specifications and operating rules on the public website to determine whether changes to commitments were communicated. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|--|--|--|----------------------|
| CC2.3.9 | Operating Rules and Participation Rules The Operating Rules and Participation Rules require participants to follow TCH procedures and technical documents. Operating rules and administrative procedures are distributed and are available on the TCH public website. Procedural guidance is available to customer and operational personnel in System and Operation manual. | Inspected TCH public website to determine whether operating rules and administrative procedures were made available on the public website. | No exceptions noted. |
| Complementary User Entity Control(s) | | | |
| Controls should be established at user entities so that: <ul style="list-style-type: none"> User entities are responsible for providing information on how to report issues, failures, incidents, etc., to TCH in the event of a security or availability issue to its users. | | | |

CC 3.0 – Common criteria related to risk assessment

CC3.1 – The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC3.1.1 | <p>Risk Control Self Assessments</p> <p>ERM performs risk control self-assessments (RCSAs) along with respective business owners on a recurring basis across the company to ascertain what is within the risk appetite and what is outside of it. Key business objectives are identified by ERM as the first step. ERM and business process owners align business objectives with security and availability processes, risks and controls. RCSAs encompass changes in TCH operations and technology. The results of an RCSA must be acknowledged by the applicable department executive. In addition, ERM is included as part of the project management process in order to provide feedback or concerns from a risk perspective.</p> | <p>Inspected the RCSA procedural document to determine whether procedures for the RCSA process including identifying key business objective, processes, risks and controls were established.</p> <p>Inspected a selected RCSA summary and results, acknowledgement email, and meeting invite to determine whether results were communicated and acknowledged by applicable department executive.</p> <p>Inspected the project management handbook to determine whether ERM is included as part of the project management process to provide risk insight.</p> | No exceptions noted. |
| CC3.1.2 | <p>Risk Meetings</p> <p>At a minimum, TCH holds quarterly risk meetings with the Enterprise Risk Management Committee (ERMC) and Enterprise Risk Committee (ERC) to discuss potential security and availability risks including evaluating security events, environmental threats, network usage and system capacity, and risks not properly mitigated from the prior quarter. ERM is responsible for reporting risks and issues to provide transparency and escalation. Objectives are captured during these meetings and incorporated into the ongoing risk assessment process. If necessary, the change management process is initiated due to the risks discussed.</p> | <p>For a selection of quarters, inspected risk meeting minutes to determine whether risk meetings were held with the Risk Management Committee (ERMC) and Enterprise Risk Committee (ERC), security and availability risks were discussed (including security events, environmental threats, network usage and system capacity, and risks not properly mitigated), objectives were captured, and if necessary, the change management process was initiated due to the risks.</p> <p>Inspected the ERM framework to determine whether ERM is responsible for reporting risks and issues.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC3.1.3 | <p>Policy Compliance with Laws and Regulation</p> <p>Enterprise-wide policies are subject to annual review by Legal to ensure compliance with applicable laws and regulations. Information Security policies are based on the ISO 27001/27002 framework.</p> <p>RTP utilizes the ISO 20022 message standards. EPN, CHIPS, IXN and RTP creates and operates under their own Operating Rules.</p> | <p>Inspected the Policy Administration Policy to determine whether enterprise-wide policies are required to be subject to an annual review by Legal. Refer to CC2.2.1 Communication of Policies and Procedures for test results related to annual review of policies by Legal.</p> <p>Inquired of management and inspected TCH internal policies and were informed that IS policies are based on the ISO 27001/27002 framework.</p> <p>Inquired of management and inspected the RTP Operating Rules to determine whether RTP utilized ISO 20022 message standards.</p> <p>Inspected EPN, CHIPS, IXN and RTP Operating Rules to determine whether each application operates under its own created rules.</p> | No exceptions noted. |
| CC3.1.4 | <p>Monitoring for Changes in Laws and Regulations</p> <p>TCH Legal closely monitors the relevant legal environment that might impact in-scope applications for the purpose of risk assessment. The Payments Law Committee provides a forum for counsel from the Company and its owners to discuss developments in payments law. Legal staff also read various newsletters and bulletins advising of trends/potential changes in the legal and business landscape.</p> | <p>Inspected the latest law committee meeting materials to determine whether TCH received updates regarding relevant legal environment changes to support the assessment of risks.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC3.1.5 | <p>Subservice Organization Agreements</p> <p>TCH maintains agreements established between TCH and subservice organizations that outline security and availability commitments, as well as the subservice organizations' responsibilities. These agreements are reviewed and approved by TCH and the organizations upon establishment. Updates and modifications to contracts and commitments are assessed as part of the contract management and vendor risk assessment process.</p> <p>Controls related to vendor risk assessment are described in CC9.2.3 Vendor Risk Management.</p> | <p>Inquired of Vendor Management and were informed that there were no new subservice organization agreements during the period; therefore, the operating effectiveness of this part of the control could not be tested.</p> <p>For a selection of existing subservice organizations, inspected the agreements to determine whether they were maintained by TCH.</p> | No exceptions noted. |
| CC3.1.6 | <p>Service Commitments and System Requirements</p> <p>Availability and security-related service commitments and system requirements are documented via the EPN, CHIPS, IXN, and RTP Operating Rules.</p> | Inspected EPN, CHIPS, IXN and RTP Operating Rules and to determine whether availability and security-related service commitments and system requirements were documented. | No exceptions noted. |

CC3.2 – The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC3.2.1 | <p>Assessing Risk</p> <p>TCH leverages a GRC tool (Archer) to record, assess, monitor and ensure appropriate remediation or risk acceptance of risks and issues. All departments have access to the tool and enter risks and issues upon identification. All risks and issues are rated at both an inherent and residual risk level. Remediation plans recorded within Archer document the required remediation effort that may include potential change management activities necessary to satisfactorily resolve identified risks and issues. ERM is responsible for monitoring risks and issues and providing transparency to the appropriate stakeholders via timely escalation and periodic reporting.</p> | <p>Inspected the GRC tool, Archer, to determine whether risks were recorded, assessed, monitored and appropriate remediation or risk acceptance of risks and issues were tracked.</p> <p>Please refer to CC3.2.2 Risk Meetings for test results related to ERM monitoring risks and periodic reporting.</p> | No exceptions noted. |
| CC3.2.2 | <p>Risk Meetings</p> <p>At a minimum, TCH holds quarterly risk meetings with the Enterprise Risk Management Committee (ERMC) and Enterprise Risk Committee (ERC) to discuss potential security and availability risks including evaluating security events, environmental threats, network usage and system capacity, and risks not properly mitigated from the prior quarter. ERM is responsible for reporting risks and issues to provide transparency and escalation. Objectives are captured during these meetings and incorporated into the ongoing risk assessment process. If necessary, the change management process is initiated due to the risks discussed.</p> | <p>For a selection of quarters, inspected risk meeting minutes to determine whether risk meetings were held with the Risk Management Committee (ERMC) and Enterprise Risk Committee (ERC), security and availability risks were discussed (including security events, environmental threats, network usage and system capacity, and risks not properly mitigated), objectives were captured, and if necessary, the change management process was initiated due to the risks.</p> <p>Inspected the ERM framework to determine whether ERM is responsible for reporting risks and issues.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| CC3.2.3 | <p>Enterprise Risk Management</p> <p>The Enterprise Risk Management department continually identifies, assesses, and monitors risks and reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities, risk assessments, Internal Audit findings, and Regulatory findings. These assessments include the identification and documentation of mitigating controls. If necessary, the change management process is initiated as a result of any findings.</p> | <p>Inspected the Enterprise Risk Management Framework document to determine whether procedures for risk identification, assessment, and monitoring, including roles and responsibilities, were documented.</p> <p>Inspected a selected RCSA assessment summary to determine whether the Enterprise Risk Management department identified, assessed, and monitored risks, reassessed the suitability of the design and implementation of control activities, and identified and documented mitigating controls as a result of any findings.</p> | No exceptions noted. |
| CC3.2.4 | <p>Vulnerability Scans</p> <p>Weekly vulnerability scans over the network and servers are completed to identify any potential security threats that would impair system security and availability. Risks are then analyzed and appropriate corrective action is taken to address the security and availability risks identified through weekly vulnerability meetings. If necessary, the change management process is initiated as a result of any findings.</p> | For a selection of weeks, inspected vulnerability scans and meeting invites and meeting minutes to determine whether the scans were completed, potential security and availability threats were identified, risks were analyzed and mitigation strategies were developed. | No exceptions noted. |
| CC3.2.5 | <p>External Network Risk Assessment</p> <p>On an annual basis, assessments of external network risks are performed to identify potential impairments that could impact system security and availability. Critical, High and Medium findings are entered into Archer for tracking where criticality based on severity and likelihood as well as a remediation plan is documented. Findings are remediated based on assigned criticality and may be remediated via the change management process as applicable.</p> | Inspected the third party external risk assessment summaries and Archer findings to determine whether identified vulnerabilities were remediated based on criticality. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|----------------------|
| | Controls related to entering, tracking and remediating findings within Archer are documented in CC3.2.1 Assessing Risk. | | |
| CC3.2.6 | Change Advisory Board Meetings TCH holds bi-weekly Change Advisory Board meeting to discuss changes, including environmental, regulatory and technological changes that affect system security and availability. Controls, policies and procedures are updated as needed based on the meeting discussions. | For a selection of weeks, inspected the change request report used in the bi-weekly Change Advisory Board meetings to determine whether changes, including environmental, regulatory and technological changes that affect system security and availability were discussed. Inquired of the VP of Information Security and VP of Operations Services and were informed that no updates were made to controls, policies, and procedures affecting security and availability during the period as a result of the Change Advisory Board meetings. | No exceptions noted. |
| CC3.2.7 | Availability Monitoring TCH utilizes third-party tools to monitor performance, memory and disk space in the distributed systems environment to help ensure systems are fully functional. Automated email alerts are sent to operations management in the event of capacity and availability issues, risks are analyzed and appropriate corrective action is taken via the standard incident management process. | Inspected the monitoring tool configurations and an email notification and noted the tool was configured to distribute automated email alerts to Network Operations based on established performance rules and thresholds. Refer to CC7.4.3 Problems Reporting and Tracking for test results of incident reporting and tracking within ServiceNow. | No exceptions noted. |
| CC3.2.8 | Risk Management Risk Management responsibilities are outlined by the ERM Framework and supporting procedures; risks and controls are housed within Archer. The Archer platform is used to monitor, track, and log, findings, remediation plans, metrics, policies, and controls. ERM reviews and approves findings and remediation plans prior to closure in Archer to ensure the issues/risk has been addressed appropriately. | Inspected the ERM framework to determine whether risk management responsibilities and procedures were outlined. Inspected the Archer tool to determine whether it was used to monitor, track, log findings, remediation plan, risk metrics and policies and that ERM reviewed and approved findings and remediation plans prior to closure. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| CC3.2.9 | <p>Internal Audit's Risk Assessment</p> <p>An audit entity universe is developed by Internal Audit and is comprised of the aggregation of several unique auditable entities. The universe that has been established is based primarily on the organizational structure of TCH. A risk assessment involves an assessment of the inherent risks, control environment and emerging risks for the auditable entity to derive a composite risk rating, which governs frequency of Internal Audit review of that entity. A risk assessment must be documented for every auditable entity within the audit universe. Once an audit of that entity is completed, an updated risk assessment will be documented as well. If changes are made to the audit universe where entities are created, merged, or deleted, risk assessments will be completed to reflect those changes.</p> | <p>Inspected TCH's current audit entity universe to determine whether an audit entity universe was established.</p> <p>Inspected the entity risk assessment and corresponding risk assessment updates to determine whether risk assessments were documented for each audit entity and risk assessments were updated once an audit of an entity was complete.</p> | No exceptions noted. |
| CC3.2.10 | <p>Risk Control Self Assessments</p> <p>ERM performs risk control self-assessments (RCSAs) along with respective business owners on a recurring basis across the company to ascertain what is within the risk appetite and what is outside of it. Key business objectives are identified by ERM as the first step. ERM and business process owners align business objectives with security and availability processes, risks and controls. RCSAs encompass changes in TCH operations and technology. The results of an RCSA must be acknowledged by the applicable department executive. In addition, ERM is included as part of the project management process in order to provide feedback or concerns from a risk perspective.</p> | <p>Inspected the RCSA procedural document to determine whether procedures for the RCSA process including identifying key business objective, processes, risks and controls were established.</p> <p>Inspected a selected RCSA summary and results, acknowledgement email, and meeting invite to determine whether results were communicated and acknowledged by applicable department executive.</p> <p>Inspected the project management handbook to determine whether ERM is included as part of the project management process to provide risk insight.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| CC3.2.11 | <p>Vendor Risk Management</p> <p>In accordance with ERM Framework, potential and existing vendor services must undergo the vendor management process which includes an onboarding risk assessment, evaluation of controls, and review over SOC reports, when available. Vendor Management performs risk assessments on specific tiered vendors on a recurring basis. Vendor Management is responsible for assigning a Vendor Impact Tier based on the vendor's commercial relevance and potential impact on core products and strategic initiatives. These tiers correlate to the vendor's inherent risk level, as defined by the Enterprise Risk Management Framework. Impact Tiers and risk assessment frequency include:</p> <ol style="list-style-type: none"> 1. Critical – On-boarding and Annually 2. Very High – On-boarding and Annually 3. High – On-boarding and 18 months 4. Medium – On-boarding and Biennial 5. Low – On-boarding or Service Change and Biennial if categorized as SaaS | <p>Inspected the ERM Framework to determine whether Vendor Risk Management procedures were established.</p> <p>For a selection of third-party vendors, inspected the Vendor Risk Assessments to determine whether risk assessments were completed on a recurring basis per specified tier and included evaluation of controls and review over SOC reports when available.</p> | No exceptions noted. |
| CC3.2.12 | <p>Asset Classification – Risk Classifications</p> <p>TCH has an asset classification and management policy which establishes three levels of data classification standards based on risk; TCH restricted - severe risk, TCH confidential - moderate risk, and TCH public - no risk.</p> | <p>Inspected the asset classification and management policy to determine whether it documented the three levels of data classification standards based on risks and was updated and reviewed annually by the Information Security leadership team.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| CC3.2.13 | <p>System Components Inventory</p> <p>ServiceNow is used to provide a single system of record for system components and supports management of IT Asset and Configuration Items. The Asset Management module within ServiceNow is used to manage asset information for IT Assets throughout its lifecycle from request to disposal and aids in determining criticality of the asset. Service Catalog workflows in ServiceNow are used to support the procurement, receive and retirement of IT Assets. TCH also uses the Configuration Management Database (CMDB) in ServiceNow to manage configuration items throughout its lifecycle from operational to out of service. Maintaining the Asset Management module allows an inventory of assets which is used in threat management. To keep configuration items up to date in the CMDB, ServiceNow Discovery is used to automate CI population into the CMDB. ServiceNow Discovery uses conventional techniques and technology to extract information from computers and other devices.</p> | <p>Inspected the CMDB configuration to determine whether IT assets were managed throughout their lifecycle.</p> <p>Inspected the ServiceNow discovery IP range list and discovery schedule list to determine whether IT servers and IT assets were tracked.</p> <p>Refer to CC7.1.9 for testing over the new IT asset discovery.</p> | No exceptions noted. |
| CC3.2.14 | <p>Disaster Recovery Plan</p> <p>Disaster Recovery plans are maintained and updated at least annually by all respective business unit managers/application owners, who are also responsible for providing the Disaster Recovery training to their team members, in order to address disaster risk. All Disaster Recovery plans must address strategies to achieve recovery time objective (RTO) and recovery point objective (RPO).</p> <p>IT Service Continuity Management performs Disaster Recovery testing at least once per year. Testing follows the Disaster Recovery plan and includes a failover to the alternate hosting sites. Results are documented and risks are assessed to improve/update the Disaster Recovery plan.</p> | <p>Inspected the plans to determine whether a review and approval process was established.</p> <p>Inspected the Business Continuity Management policy to determine whether it documented roles and requirements for maintenance and review of the Disaster Recovery plans, training, and addressing RTO and RPO strategies were established to address disaster risk.</p> <p>Inspected the annual Disaster Recovery testing results and Disaster Recovery Plan to determine whether the testing followed the Disaster Recovery Plan, results were officially documented and the Disaster Recovery Plan was updated to address identified risks.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|----------------------|
| CC3.2.15 | <p>Business Continuity Plan</p> <p>TCH has established a Business Continuity Program to provide capabilities, information, and training to ensure that employees are prepared for any interruption and know what to do in the event of an interruption incident at any of the TCH sites. The TCH Enterprise Risk Management Framework document and Business Continuity Management policy define roles and responsibilities for business continuity and disaster recovery plan development and maintenance, identify procedures to facilitate plan development, establish a review and approval process for business continuity plans, specify requirements for plan ownership, and provide requirements and frequency for plan test.</p> | <p>Inspected the TCH Enterprise Risk Management Framework and Business Continuity Management Policy documents, and recent business continuity plan tests to determine whether roles and responsibilities for business continuity and disaster recovery plan development and maintenance were defined, procedures to facilitate plan development were identified, a review and approval process for business continuity plans was established, requirements for plan ownership were specified, and requirements and frequency for plan test were provided.</p> <p>Inspected the business continuity plans to determine whether a review and approval process was established.</p> | No exceptions noted. |

CC3.3 – The entity considers the potential for fraud in assessing risks to the achievement of objectives.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| CC3.3.1 | <p>Code of Conduct and Acknowledgement</p> <p>TCH has a formal “Code of Conduct” covering areas of business conduct and ethics including duty to report illegal, fraudulent, or unethical conduct. All employees are required to sign and acknowledge that they have read and will comply with the rules through an annual affidavit for the code of conduct which includes a confidentiality agreement. Existing employees acknowledge the Code of Conduct annually through online training and new employees acknowledge the Code of Conduct when they join TCH. Acknowledgement of the Code of Conduct implies conformance with all applicable laws, regulations, and TCH policies including Acceptable Use Requirements.</p> | <p>For a selection of new employees, inspected code of conduct affidavits to determine whether employees signed the code of conduct affidavit when they joined TCH.</p> <p>For a selection of existing employees, inspected the online training records that included the TCH Code of Conduct policy acknowledgement to determine whether existing employees acknowledge the Code of Conduct annually.</p> | No exceptions noted. |
| CC3.3.2 | <p>Asset Classification</p> <p>TCH has policies that document requirements on removable media and asset classifications. The policies are reviewed and updated annually by the Information Security leadership team in accordance with the Information Security policies. TCH has an asset classification and management policy which establishes three levels of data classification standards which are used to help restrict access to information:</p> <p>TCH Restricted:</p> <p>Information that, if publicly disclosed, altered or destroyed without appropriate authorization, could result in severe financial loss or reputational damage to TCH. In the case of a document or email that contains information of varying sensitivity levels, the highest sensitivity level must be applied to the entire document or email. Except as otherwise set forth in the Information Classification Guidelines, no circulation is permitted outside of TCH without prior</p> | <p>Inspected the following policy documents to determine whether they documented requirements on removable information and assets and the policy documents were updated and reviewed annually by TCH leadership.</p> <ul style="list-style-type: none"> • Asset Classification and Management Policy • Physical and Environment Security Policy <p>Inspected the asset classification and management policy to determine whether it documented the three levels of data classification standards and was updated and reviewed annually by the Information Security leadership team.</p> <p>Inspected a selection of sensitive, internal, and customer-facing documents maintained by TCH to determine whether asset classification types for levels of data classification were established.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| | <p>authorization of an Executive Vice President or above and the Legal department.</p> <p>TCH Confidential:</p> <p>Information that, if publicly disclosed, altered or destroyed without appropriate authorization, could result in moderate financial loss or reputational damage to TCH. Information that does not clearly fall within the TCH Restricted or Public designations should be designated TCH Confidential. Except as otherwise set forth in the Information Classification Guidelines, no circulation is permitted outside of TCH without prior authorization of Senior Vice President or above.</p> <p>Public:</p> <p>Information that is intended for public dissemination or, if publicly disclosed, altered or destroyed without authorization, would result in no financial loss or reputational damage to TCH. Data can be circulated outside of TCH.</p> | | |
| CC3.3.3 | <p>Fraud Risk</p> <p>Fraud risk is handled through TCH corporate policies such as the Code of Conduct that address internal fraud risk. Client level fraud risk is addressed through Operating Rules each client agrees with for each product, as well as technical controls within the applications.</p> | <p>Inspected the TCH Code of Conduct to determine whether the policy addressed reporting fraud risk.</p> <p>Inspected the EPN, CHIPS IXN, and RTP Operating Rules to determine whether they addressed fraud risk.</p> | No exceptions noted. |
| CC3.3.4 | <p>Security Administration and Security Violations</p> <p>ArcSight is used to support security administration including managing security violations for both mainframe and distributed environments. Security related activities such as user data change, file security attribute change and security violations including inappropriate user activity, unauthorized software, virus and firewall alerts are captured, logged and reported using ArcSight. ArcSight is configured to capture the defined security related activities and send an alert to the</p> | <p>Inspected the configuration for alert event setup in ArcSight to determine whether ArcSight was setup to capture and log the security related events such as user data change, file security attribute change and security violation including inappropriate user activity, unauthorized software, IDS, virus and firewall alerts and sends automatic alerts to Cipher, and the Information Security Analyst when an event that met the defined condition occurred.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| | Information Security responsible personnel through the Information Security workstation and to their mobile phones when there is an event that meets the defined criteria such as possible security violation. Each alert is reviewed and triaged by the managed security service provider, Cipher, and followed up and cleared by Information Security, as necessary. On an ongoing basis, the Information Security responsible personnel reviews the alerts and other activities to determine that alerts were responded to appropriately. Alerts remain pending in ArcSight until they are resolved. | Observed online ArcSight alert messages on the ArcSight workstation located in a secure area of the Information Security group and noted Information Security responded to the alert in ArcSight and that alert remained pending until it was resolved. For a selection of months, inspected a selected ArcSight violation report to determine whether the security violations were captured and retained in ArcSight. | |
| CC3.3.5 | Fraud Detection – RTP RTP Operating Rules requires a Sending Participant, when it determines that a sent RTP payment was unauthorized, to report the unauthorized payment by sending a Request for Return of Funds (RFR) message, referencing the original payment and including a FRAD (fraud) reason code. TCH RTP Operators monitor RFRs with an FRAD reason code on a daily basis and investigate select reports, which may include reaching out to both the Sending and Receiving Participants. | For a selection of dates, inspected evidence of daily report received by the RTP Operators to determine RFRs with a 'FRAD' reason code were investigated and resolved as necessary. | No exceptions noted. |

CC3.4 – The entity identifies and assesses changes that could significantly impact the system of internal control.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|-----------------------------|
| CC3.4.1 | <p>Monitoring for Changes in Laws and Regulations</p> <p>TCH Legal closely monitors the relevant legal environment that might impact in-scope applications for the purpose of risk assessment. The Payments Law Committee provides a forum for counsel from the Company and its owners to discuss developments in payments law. Legal staff also read various newsletters and bulletins advising of trends/potential changes in the legal and business landscape.</p> | <p>Inspected the latest law committee meeting materials to determine whether TCH received updates regarding relevant legal environment changes to support the assessment of risks.</p> | <p>No exceptions noted.</p> |
| CC3.4.2 | <p>Enterprise Risk Management</p> <p>The Enterprise Risk Management department continually identifies, assesses, and monitors risks and reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities, risk assessments, Internal Audit findings, and Regulatory findings. These assessments include the identification and documentation of mitigating controls. If necessary, the change management process is initiated as a result of any findings.</p> | <p>Inspected the Enterprise Risk Management Framework document to determine whether procedures for risk identification, assessment, and monitoring, including roles and responsibilities, were documented.</p> <p>Inspected a selected RCSA assessment summary to determine whether the Enterprise Risk Management department identified, assessed, and monitored risks, reassessed the suitability of the design and implementation of control activities, and identified and documented mitigating controls as a result of any findings.</p> | <p>No exceptions noted.</p> |
| CC3.4.3 | <p>Risk Control Self Assessments</p> <p>ERM performs risk control self-assessments (RCSAs) along with respective business owners on a recurring basis across the company to ascertain what is within the risk appetite and what is outside of it. Key business objectives are identified by ERM as the first step. ERM and business process owners align business objectives with security and availability processes, risks and controls. RCSAs encompass changes in TCH operations and technology. The results of an RCSA must be acknowledged by the applicable department executive. In</p> | <p>Inspected the RCSA procedural document to determine whether procedures for the RCSA process including identifying key business objective, processes, risks and controls were established.</p> <p>Inspected a selected RCSA summary and results, acknowledgement email, and meeting invite to determine whether results were communicated and acknowledged by applicable department executive.</p> | <p>No exceptions noted.</p> |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| | addition, ERM is included as part of the project management process in order to provide feedback or concerns from a risk perspective. | Inspected the project management handbook to determine whether ERM is included as part of the project management process to provide risk insight. | |
| CC3.4.4 | <p>Internal Audit's Risk Assessment</p> <p>An audit entity universe is developed by Internal Audit and is comprised of the aggregation of several unique auditable entities. The universe that has been established is based primarily on the organizational structure of TCH. A risk assessment involves an assessment of the inherent risks, control environment and emerging risks for the auditable entity to derive a composite risk rating, which governs frequency of Internal Audit review of that entity. A risk assessment must be documented for every auditable entity within the audit universe. Once an audit of that entity is completed, an updated risk assessment will be documented as well. If changes are made to the audit universe where entities are created, merged, or deleted, risk assessments will be completed to reflect those changes.</p> | <p>Inspected TCH's current audit entity universe to determine whether an audit entity universe was established.</p> <p>Inspected the entity risk assessment and corresponding risk assessment updates to determine whether risk assessments were documented for each audit entity and risk assessments were updated once an audit of an entity was complete.</p> | No exceptions noted. |
| CC3.4.5 | <p>Vendor Risk Management</p> <p>In accordance with ERM Framework, potential and existing vendor services must undergo the vendor management process which includes an onboarding risk assessment, evaluation of controls, and review over SOC reports, when available. Vendor Management performs risk assessments on specific tiered vendors on a recurring basis. Vendor Management is responsible for assigning a Vendor Impact Tier based on the vendor's commercial relevance and potential impact on core products and strategic initiatives. These tiers correlate to the vendor's inherent risk level, as defined by the Enterprise Risk Management Framework.</p> | <p>Inspected the ERM Framework to determine whether Vendor Risk Management procedures were established.</p> <p>For a selection of third-party vendors, inspected the Vendor Risk Assessments to determine whether risk assessments were completed on a recurring basis per specified tier and included evaluation of controls and review over SOC reports when available.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|-----------------------------|
| | Impact Tiers and risk assessment frequency include: 1. Critical – On-boarding and Annually 2. Very High – On-boarding and Annually 3. High – On-boarding and 18 months 4. Medium – On-boarding and Biennial 5. Low – On-boarding or Service Change and Biennial if categorized as SaaS | | |
| CC3.4.6 | Vulnerability Scans Weekly vulnerability scans over the network and servers are completed to identify any potential security threats that would impair system security and availability. Risks are then analyzed and appropriate corrective action is taken to address the security and availability risks identified through weekly vulnerability meetings. If necessary, the change management process is initiated as a result of any findings. | For a selection of weeks, inspected vulnerability scans and meeting invites and meeting minutes to determine whether the scans were completed, potential security and availability threats were identified, risks were analyzed and mitigation strategies were developed. | No exceptions noted. |
| CC3.4.7 | Risk Assessment for Changes A bi-weekly Change Advisory Board meeting, which is attended by designated members of Change Control, Application Development, Infrastructure, Quality Control, Information Security and other Technology and Network Operations Center representatives as needed, is conducted to review and approve each change that is scheduled for migration into the production environment. Changes are scheduled according to risk classifications; low, moderate, high, and emergency. During the SDLC project initiation process, ERM is included in order to provide feedback or concerns from a risk perspective. | Inspected the Change Control Policy to determine whether bi-weekly Change Advisory Board meetings are conducted and changes are scheduled according to risk classification. Inspected the project management handbook to determine whether ERM is included as part of the project management process to provide risk insight. | No exceptions noted. |

CC 4.0 – Common criteria related to monitoring activities

CC4.1 – The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC4.1.1 | <p>Risk Control Self Assessments</p> <p>ERM performs risk control self-assessments (RCSAs) along with respective business owners on a recurring basis across the company to ascertain what is within the risk appetite and what is outside of it. Key business objectives are identified by ERM as the first step. ERM and business process owners align business objectives with security and availability processes, risks and controls. RCSAs encompass changes in TCH operations and technology. The results of an RCSA must be acknowledged by the applicable department executive. In addition, ERM is included as part of the project management process in order to provide feedback or concerns from a risk perspective.</p> | <p>Inspected the RCSA procedural document to determine whether procedures for the RCSA process including identifying key business objective, processes, risks and controls were established.</p> <p>Inspected a selected RCSA summary and results, acknowledgement email, and meeting invite to determine whether results were communicated and acknowledged by applicable department executive.</p> <p>Inspected the project management handbook to determine whether ERM is included as part of the project management process to provide risk insight.</p> | No exceptions noted. |
| CC4.1.2 | <p>Internal Audit</p> <p>Internal Audit provides independent, objective and timely assurance to the Managing Board of Directors, the Audit Committee, senior management and regulators on the design and operating effectiveness of controls that mitigate current and emerging risks. The Chief Auditor manages the Internal Audit function and reports directly to the Audit Committee and administratively to the CEO of TCH.</p> <p>Internal Audit performs audits on data center operations and client services on a cyclical basis based on the entity risk ratings. Results and periodic reports are communicated to the Audit Committee, the Board and senior management summarizing the status of the Audit Plan, results of audit activities including issues and corrective actions, and details</p> | <p>Inspected TCH's Internal Audit Organizational Chart and TCH's Organizational Chart to determine whether Internal Audit was independent from TCH management.</p> <p>For a selection of quarters, inspected Audit Committee meeting materials and internal audit results to determine whether Internal Audit periodically reports to the Audit Committee, Board and senior management.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|----------------------|
| | of any significant issues identified. Quarterly meetings are held with the Audit Committee. | | |
| CC4.1.3 | <p>Vendor Risk Management</p> <p>In accordance with ERM Framework, potential and existing vendor services must undergo the vendor management process which includes an onboarding risk assessment, evaluation of controls, and review over SOC reports, when available. Vendor Management performs risk assessments on specific tiered vendors on a recurring basis. Vendor Management is responsible for assigning a Vendor Impact Tier based on the vendor's commercial relevance and potential impact on core products and strategic initiatives. These tiers correlate to the vendor's inherent risk level, as defined by the Enterprise Risk Management Framework. Impact Tiers and risk assessment frequency include:</p> <ol style="list-style-type: none"> 1. Critical – On-boarding and Annually 2. Very High – On-boarding and Annually 3. High – On-boarding and 18 months 4. Medium – On-boarding and Biennial 5. Low – On-boarding or Service Change and Biennial if categorized as SaaS | <p>Inspected the ERM Framework to determine whether Vendor Risk Management procedures were established.</p> <p>For a selection of third-party vendors, inspected the Vendor Risk Assessments to determine whether risk assessments were completed on a recurring basis per specified tier.</p> | No exceptions noted. |
| CC4.1.4 | <p>Internal Audit Competencies and Specialized Skills</p> <p>Internal Audit has the appropriate experience and expertise to conduct their work with proficiency and due professional care. Internal audit staff engage in continuing professional education including forty allocated training hours each fiscal year. In the event that the requisite skills are not available in Internal Audit for a specific engagement, the Chief Auditor will seek approval from the Audit Committee and the CEO for external assistance.</p> | <p>Inspected the Audit Manual to determine whether continuous education requirements were outlined.</p> <p>Inspected the Internal Audit Training schedule to determine whether the completion of professional education training courses was tracked.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| CC4.1.5 | <p>Audit Entity Universe</p> <p>An audit entity universe is developed by Internal Audit and is comprised of the aggregation of several unique auditable entities. The universe that has been established is based primarily on the organizational structure of TCH. A risk assessment must be documented for every auditable entity within the audit universe. Once an audit of that entity is completed, an updated risk assessment will be documented as well. If changes are made to the audit universe where entities are created, merged, or deleted, risk assessments will be completed to reflect those changes.</p> | <p>Inspected TCH's current audit entity universe to determine whether an audit entity universe was established.</p> <p>Inspected the entity risk assessment and corresponding risk assessment updates to determine whether risk assessments were documented for each audit entity and risk assessments were updated once an audit of an entity was complete.</p> | No exceptions noted. |
| CC4.1.6 | <p>Audit Plan</p> <p>The annual audit plan is developed by Internal Audit management and approved by the TCH Chief Auditor. The Audit Committee will review and approve, on an annual basis, the audit plan as stated within the responsibilities and duties of the TCH Audit Committee Charter. Any changes to the plan will be presented to the Audit Committee during the quarterly meetings.</p> <p>The TCH Chief Auditor monitors progress against plan and provides updates to the following on a scheduled basis during the year; TCH CEO, PayCo Board and TCH Audit Committee.</p> | <p>Inspected the annual audit plan to determine whether the audit plan was developed by internal audit management and approved by the TCH Chief Auditor.</p> <p>Inspected Audit Committee meeting materials to determine whether audit plan progress was monitored.</p> | No exceptions noted. |
| CC4.1.7 | <p>Internal Audit Objectivity</p> <p>Internal Audit is independent and has no authority or operating responsibility for the activities it audits. The Chief Auditor manages the Internal Audit function and reports directly to the Audit Committee and administratively to the CEO of TCH. Internal Audit activities are carried out independently under the oversight of the Audit Committee.</p> | <p>Inspected TCH's Internal Audit Organizational Chart TCH's Organizational Chart to determine whether Internal Audit was independent from TCH management.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| CC4.1.8 | Vulnerability Scans Weekly vulnerability scans over the network and servers are completed to identify any potential security threats that would impair system security and availability. Risks are then analyzed and appropriate corrective action is taken to address the security and availability risks identified through weekly vulnerability meetings. If necessary, the change management process is initiated as a result of any findings. | For a selection of weeks, inspected vulnerability scans and meeting invites and meeting minutes to determine whether the scans were completed, potential security and availability threats were identified, risks were analyzed and mitigation strategies were developed. | No exceptions noted. |
| CC4.1.9 | External Network Risk Assessment On an annual basis, assessments of external network risks are performed to identify potential impairments that could impact system security and availability. Critical, High and Medium findings are entered into Archer for tracking where a criticality based on severity and likelihood as well as a remediation plan is documented. Findings are remediated based on assigned criticality and may be remediated via the change management process as applicable. Controls related to entering, tracking and remediating findings within Archer are documented in CC3.2.1 Assessing Risk. | Inspected the third party external risk assessment summaries and Archer findings to determine whether identified vulnerabilities were remediated based on criticality. | No exceptions noted. |
| CC4.1.10 | Regulatory and Association Requirements TCH falls under the Significant Service Provider program and are subject to supervision by the FFIEC with the Federal Reserve as the lead regulator. As a result, multiple examinations by the regulators may occur in a given year. TCH addresses issues noted from these examinations to the satisfaction of the examiners. | Inspected evidence from the US Treasury to determine whether TCH falls under the Significant Service Provider program and were subject to supervision to the FFIEC. For a selection of quarters, inspected Audit Committee meeting materials to determine whether Internal Audit tracks open regulatory examination findings through closure. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| CC4.1.11 | <p>Disaster Recovery Plan</p> <p>Disaster Recovery plans are maintained and updated at least annually by all respective business unit managers/application owners, who are also responsible for providing the Disaster Recovery training to their team members, in order to address disaster risk. All Disaster Recovery plans must address strategies to achieve recovery time objective (RTO) and recovery point objective (RPO).</p> <p>IT Service Continuity Management performs Disaster Recovery testing at least once per year. Testing follows the Disaster Recovery plan and includes a failover to the alternate hosting sites. Results are documented and risks are assessed to improve/update the Disaster Recovery plan.</p> | <p>Inspected the plans to determine whether a review and approval process was established.</p> <p>Inspected the Business Continuity Management policy to determine whether it documented roles and requirements for maintenance and review of the Disaster Recovery plans, training, and addressing RTO and RPO strategies were established to address disaster risk.</p> <p>Inspected the annual Disaster Recovery testing results and Disaster Recovery Plan to determine whether the testing followed the Disaster Recovery Plan, results were officially documented and the Disaster Recovery Plan was updated to address identified risks.</p> | No exceptions noted. |
| CC4.1.12 | <p>Business Continuity Plan</p> <p>TCH has established a Business Continuity Program to provide capabilities, information, and training to ensure that employees are prepared for any interruption and know what to do in the event of an interruption incident at any of the TCH sites. The TCH Enterprise Risk Management Framework document and Business Continuity Management policy define roles and responsibilities for business continuity and disaster recovery plan development and maintenance, identify procedures to facilitate plan development, establish a review and approval process for business continuity plans, specify requirements for plan ownership, and provide requirements and frequency for plan test.</p> | <p>Inspected the TCH Enterprise Risk Management Framework and Business Continuity Management Policy documents, and recent business continuity plan tests to determine whether roles and responsibilities for business continuity and disaster recovery plan development and maintenance were defined, procedures to facilitate plan development were identified, a review and approval process for business continuity plans was established, requirements for plan ownership were specified, and requirements and frequency for plan test were provided.</p> <p>Inspected the business continuity plans to determine whether a review and approval process was established.</p> | No exceptions noted. |

CC4.2 – The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| CC4.2.1 | <p>Archer - Deficiencies</p> <p>TCH leverages a GRC tool (Archer) to record, assess, monitor and ensure appropriate remediation or risk acceptance of risks and issues. Findings are documented and tracked within the tool and remediation plans recorded document the required remediation effort that may include potential change management activities necessary to satisfactorily resolve identified risks and issues. ERM is responsible for monitoring risks and issues and providing transparency to the appropriate stakeholders via timely escalation and periodic reporting via risk assessment meetings.</p> <p>Controls related to ERM reporting is described in CC3.2.2 Risk Assessment Meetings.</p> | <p>Inspected the GRC tool, Archer, to determine whether risks were recorded, assessed, monitored and appropriate remediation or risk acceptance of risks and issues were tracked.</p> <p>Please refer to CC3.2.2 Risk Meetings for test results related to Risk Meetings.</p> | No exceptions noted. |
| CC4.2.2 | <p>Risk Meetings</p> <p>At a minimum, TCH holds quarterly risk meetings with the Enterprise Risk Management Committee (ERMC) and Enterprise Risk Committee (ERC) to discuss potential security and availability risks including evaluating security events, environmental threats, network usage and system capacity, and risks not properly mitigated from the prior quarter. ERM is responsible for reporting risks and issues to provide transparency and escalation. Objectives are captured during these meetings and incorporated into the ongoing risk assessment process. If necessary, the change management process is initiated due to the risks discussed.</p> | <p>For a selection of quarters, inspected risk meeting minutes to determine whether risk meetings were held with the Risk Management Committee (ERMC) and Enterprise Risk Committee (ERC), security and availability risks were discussed (including security events, environmental threats, network usage and system capacity, and risks not properly mitigated), objectives were captured, and if necessary, the change management process was initiated due to the risks.</p> <p>Inspected the ERM framework to determine whether ERM is responsible for reporting risks and issues.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC4.2.3 | Vulnerability Scans Weekly vulnerability scans over the network and servers are completed to identify any potential security threats that would impair system security and availability. Risks are then analyzed and appropriate corrective action is taken to address the security and availability risks identified through weekly vulnerability meetings. If necessary, the change management process is initiated as a result of any findings. | For a selection of weeks, inspected vulnerability scans and meeting invites and meeting minutes to determine whether the scans were completed, potential security and availability threats were identified, risks were analyzed and mitigation strategies were developed. | No exceptions noted. |
| CC4.2.4 | External Network Risk Assessment On an annual basis, assessments of external network risks are performed to identify potential impairments that could impact system security and availability. Critical, High and Medium findings are entered into Archer for tracking where a criticality based on severity and likelihood as well as a remediation plan is documented. Findings are remediated based on assigned criticality and may be remediated via the change management process as applicable. Controls related to entering, tracking and remediating findings within Archer are documented in CC3.2.1 Assessing Risk. | Inspected the third party external risk assessment summaries and Archer findings to determine whether identified vulnerabilities were remediated based on criticality. | No exceptions noted. |
| CC4.2.5 | Intrusion Detection System The TCH networks include an Intrusion Detection System (IDS), CarbonBlack. This system detects and classifies suspicious events according to a library of signatures provide by the vendor. The IDS/IPS is programmed to send alerts when thresholds for particular attack signatures are exceeded. Information Security management are alerted of intrusion activities. Incidents noted are recorded in ArcSight and depending on the nature and type of problem, the incident is escalated to the designated group for follow-up and resolution. If necessary, corrective action is taken via updates | For a selection of servers, inspected the CarbonBlack management console to determine whether CarbonBlack was configured to monitor traffic. For a selection of incidents, inspected tickets and supporting documentation to determine whether the incident was escalated and resolved. Inspected configured threat intelligence library in CarbonBlack to determine whether the system was configured to detect and classify events according to the signatures. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| | <p>to policies and/or the change management process due to the alerts.</p> <p>CarbonBlack is configured to generate alerts through ArcSight.</p> <p>Controls related incidents analysis and resolution are documented in CC7.4.4 Security Administration and Security Violations.</p> | <p>Inspected ArcSight management console to determine whether ArcSight was configured to alert Information Security in case of potential threats.</p> <p>Inspected the list of users with administrator access to CarbonBlack, job titles, and inquired of the management to determine whether administrative access to CarbonBlack was restricted to authorized personnel.</p> <p>Inquired of Information Security management regarding policy and process updates and were informed corrective action was taken via updates to policies and/or the change management process due to the alerts.</p> <p>Refer to CC7.4.4 Security Administration and Security Violations for test results of incident analysis and resolution for ArcSight.</p> | |
| CC4.2.6 | <p>Security Administration and Security Violations</p> <p>ArcSight is used to support security administration including managing security violations for both mainframe and distributed environments. Security related activities such as user data change, file security attribute change and security violations including inappropriate user activity, unauthorized software, virus and firewall alerts are captured, logged and reported using ArcSight. ArcSight is configured to capture the defined security related activities and send an alert to the Information Security responsible personnel through the Information Security workstation and to their mobile phones when there is an event that meets the defined criteria such as possible security violation. Each alert is reviewed and triaged by the managed security service provider, Cipher, and followed up and cleared by Information Security, as necessary. On an ongoing basis, the Information Security responsible personnel reviews the alerts and other activities</p> | <p>Inspected the configuration for alert event setup in ArcSight to determine whether ArcSight was setup to capture and log the security related events such as user data change, file security attribute change and security violation including inappropriate user activity, unauthorized software, IDS, virus and firewall alerts and sends automatic alerts to Cipher, and the Information Security Analyst when an event that met the defined condition occurred.</p> <p>Observed online ArcSight alert messages on the ArcSight workstation located in a secure area of the Information Security group and noted Information Security responded to the alert in ArcSight and that alert remained pending until it was resolved.</p> <p>For a selection of months, inspected a selected ArcSight violation report to determine whether the</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| | to determine that alerts were responded to appropriately. Alerts remain pending in ArcSight until they are resolved. | security violations were captured and retained in ArcSight. | |
| CC4.2.7 | <p>Board Committees and Board Review of Information Security Program State</p> <p>The Board Champions of Committees (Enterprise Risk, Audit, and Finance etc.) and the Board Champions of PayCo's Business Committees (RTP, CHIPS, EPN, and SVPCO) are allocated time during all regularly scheduled Board meetings to report on security and availability related developments relating to their respective committees that they believe rise to the level of meriting the Board's strategic attention and that are not otherwise covered in the agenda, if any. In addition, the state of TCH's information security is reviewed by the Board annually.</p> | <p>For a selection of quarters, inspected board meeting minutes to determine whether committees were allotted time on the agenda to report security and availability related developments.</p> <p>Inspected the Board of Director's Charter to determine whether the state of information security is reviewed by the board on an annual basis.</p> | No exceptions noted. |
| CC4.2.8 | <p>Internal Audit Reporting</p> <p>Internal Audit provides periodic reports to the Audit Committee, the Board and senior management summarizing the status of the Audit Plan, results of audit activities, and details of any significant issues identified. Quarterly meetings are held with the Audit Committee.</p> | For a selection of quarters, inspected Audit Committee meeting materials to determine whether Internal Audit reported the status, results and issues to the Audit Committee, Board and senior management. | No exceptions noted. |

CC 5.0 – Common criteria related to control activities

CC5.1 – The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| CC5.1.1 | <p>Control Activities</p> <p>Along with assessing risks, management has identified and put into effect actions to address those risks. A mixture of preventative, detective, automated and manual control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently for security and availability commitments and system requirements.</p> | Observed control activities stored in Archer to determine whether a mixture of preventative, detective, automated and manual control activities were established. | No exceptions noted. |
| CC5.1.2 | <p>Enterprise Risk Management</p> <p>The Enterprise Risk Management department continually identifies, assesses, and monitors risks and reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities, risk assessments, Internal Audit findings, and Regulatory findings. These assessments include the identification and documentation of mitigating controls. If necessary, the change management process is initiated as a result of any findings.</p> | <p>Inspected the Enterprise Risk Management Framework document to determine whether procedures for risk identification, assessment, and monitoring, including roles and responsibilities, were documented.</p> <p>Inspected a selected RCSA assessment summary to determine whether the Enterprise Risk Management department identified, assessed, and monitored risks, reassessed the suitability of the design and implementation of control activities, and identified and documented mitigating controls as a result of any findings.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC5.1.3 | <p>Vendor Risk Management</p> <p>In accordance with ERM Framework, potential and existing vendor services must undergo the vendor management process which includes an onboarding risk assessment, evaluation of controls, and review over SOC reports, when available. Vendor Management performs risk assessments on specific tiered vendors on a recurring basis. Vendor Management is responsible for assigning a Vendor Impact Tier based on the vendor's commercial relevance and potential impact on core products and strategic initiatives. These tiers correlate to the vendor's inherent risk level, as defined by the Enterprise Risk Management Framework.</p> <p>Impact Tiers and risk assessment frequency include:</p> <ol style="list-style-type: none"> 1. Critical – On-boarding and Annually 2. Very High – On-boarding and Annually 3. High – On-boarding and 18 months 4. Medium – On-boarding and Biennial 5. Low – On-boarding or Service Change and Biennial if categorized as SaaS | <p>Inspected the ERM Framework to determine whether Vendor Risk Management procedures were established.</p> <p>For a selection of third-party vendors, inspected the Vendor Risk Assessments to determine whether risk assessments were completed on a recurring basis per specified tier and included evaluation of controls and review over SOC reports when available.</p> | No exceptions noted. |
| CC5.1.4 | <p>Risk Management</p> <p>Risk Management responsibilities are outlined by the ERM Framework and supporting procedures; risks and controls are housed within Archer. The Archer platform is used to monitor, track, and log, findings, remediation plans, metrics, policies, and controls. ERM reviews and approves findings and remediation plans prior to closure in Archer to ensure the issues/risk has been addressed appropriately.</p> | <p>Inspected the ERM framework to determine whether risk management responsibilities and procedures were outlined.</p> <p>Inspected the Archer tool to determine whether it was used to monitor, track, log findings, remediation plan, risk metrics and policies and that ERM reviewed and approved findings and remediation plans prior to closure.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|----------------------|
| CC5.1.5 | <p>Segregation of Duties</p> <p>TCH provides segregation of duties to effectively control the concentration of functions within the organization. The separation of Operations and Technology duties from TCH's Product Development & Management Division and other Administrative functions, which include accounting and finance, audit and human resources, provides an additional level of segregation of functions within TCH.</p> <p>Access Management training addresses segregation of duties and includes descriptions of "toxic pairs" (entitlements that should not be granted to certain roles). Management reviews and recertifies access entitlements throughout the year and reject any access entitlements that are not least privileged or segregated as appropriate. In the event that "toxic pair" entitlements are required for an individual, there is a policy exception and registration process for risk acceptance.</p> <p>Controls related to the access recertification's are documented in CC6.2.7 Periodic Access Review.</p> | <p>Inspected TCH's organizational charts and job descriptions to determine whether duties were segregated within the organization.</p> <p>Inspected TCH's Access Management Training documentation to determine whether the training addressed segregation of duties and "toxic pairs" concepts.</p> | No exceptions noted. |

CC5.2 – The entity also selects and develops general control activities over technology to support the achievement of objectives.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|-----------------------------|
| CC5.2.1 | <p>Security and Availability Related Policies</p> <p>As governed by the policy administration policy, TCH has developed and documented policies and procedures over key IT and IS operations that address information security and availability requirements. The policies include requirements over risk management, information security, asset classification, asset disposal, access control, SDLC, change management, capacity management, removable media, physical access, incident management and are updated periodically. Policies and procedures are communicated in Archer.</p> | <p>Inspected the policies and procedures to determine whether information security and availability policies were documented, maintained, and updated periodically and made available to TCH employees in Archer.</p> | <p>No exceptions noted.</p> |
| CC5.2.2 | <p>Updates to Policies</p> <p>TCH management reviews, applies updates for new threats and changes, and approves Information Security policies and related availability policies periodically. The policies are available to all employees in Archer.</p> | <p>Inspected the Information Security policies and availability policies to determine whether they addressed the relevant security and availability attributes and included the annual revisions performed and reviewed by management.</p> <p>Inspected screenshots from Archer to determine whether policies were available to all employees.</p> | <p>No exceptions noted.</p> |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| CC5.2.3 | <p>Updates to Procedures</p> <p>TCH has process and procedure manuals for applications, and these processes and procedures are updated in accordance with the Information Security and Availability policies. The processes and procedures documents are available to all employees on the TCH intranet. System descriptions and manuals for applications are made available to external user entities on TCH's website, permitting users to understand their role in the system.</p> | <p>Inspected the process and procedure manuals for EPN, CHIPS, IXN, and RTP to determine whether the manuals documented application processes and procedures.</p> <p>Inspected the revision history in the process and procedure manuals for EPN, CHIPS, IXN, and RTP to determine whether the manuals were updated in accordance with the Information Security and Availability policies.</p> <p>Observed TCH's website and noted system descriptions for EPN, CHIPS, IXN and RTP were communicated to external user entities, permitting users to understand their role in the system.</p> | No exceptions noted. |
| CC5.2.4 | <p>Server Hardening</p> <p>TCH provides hardening standards for system administrators in order to implement secure server configurations within the company's infrastructure. The guidelines are reviewed and updated when changes occur by the Information Security team.</p> <p>Monthly validation of compliance to hardening standards occurs through the use of BigFix. Weekly meetings are held to discuss compliance results, and if necessary, tickets are created for remediation or a policy exception is documented in Archer.</p> | <p>Inspected the hardening guidelines to determine whether they document approved hardening standards for server configurations.</p> <p>For a selection of months, inspected monthly compliance report to determine whether compliance checks were performed to ensure devices were hardened per defined standards.</p> <p>For a selection of weeks, inspected the compliance meeting invite and notes to determine whether compliance results were discussed, and if necessary, tickets were created for remediation of any noted issues or a policy exception was documented in Archer.</p> | No exceptions noted. |

CC5.3 – The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|-----------------------------|
| CC5.3.1 | <p>Security and Availability Related Policies</p> <p>As governed by the policy administration policy, TCH has developed and documented policies and procedures over key IT and IS operations that address information security and availability requirements. The policies include requirements over risk management, information security, asset classification, asset disposal, access control, SDLC, change management, systems acquisition, development and maintenance, capacity management, removable media, physical access, incident management and are updated periodically. Policies and procedures are communicated in Archer.</p> | <p>Inspected the policies and procedures to determine whether information security and availability policies were documented, maintained, and updated periodically and made available to TCH employees in Archer.</p> | <p>No exceptions noted.</p> |
| CC5.3.2 | <p>Communication of Policies and Procedures</p> <p>TCH provides personnel responsible for the design, development, implementation, operation, maintenance, and monitoring of systems the policies and procedures necessary to perform their job duties, as it relates to system security and availability. Policies and procedures are reviewed and approved annually by the Enterprise Risk Management Committee (ERMC).</p> <p>TCH employees who are responsible and accountable for system controls have the authority to ensure policies and system requirements are effectively communicated and placed into operation. All Information Security policies are owned by the CISO except for the BCP policy which is owned by the Chief Risk Officer and the Physical/Environmental Security policy which is owned by Corporate Real Estate. Information Security policies are based on ISO framework.</p> | <p>Inspected the posted policies and procedures in Archer to determine whether policies and procedures were available for employees responsible for the design, development, implementation, operation, maintenance, and monitoring of systems to perform their job duties, as it relates to system security and availability</p> <p>Inspected system evidence to determine whether policies and procedures were reviewed and approved annually by the Enterprise Risk Management Committee (ERMC).</p> <p>Inquired of management and were informed that IS policies are based on the ISO framework.</p> | <p>No exceptions noted.</p> |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| CC5.3.3 | Policy Administration Policy The Policy Administration Policy outlines all department and enterprise policies along with ownership and approval levels. ERM facilitates policy approvals on an annual basis. | Inspected the Policy Administration Policy to determine whether all department and enterprise policies were outlined. | No exceptions noted. |
| CC5.3.4 | Updates to Policies TCH management reviews, applies updates for new threats and changes, and approves Information Security policies and availability policies periodically. The policies are available to all employees in Archer. | Inspected the Information Security policies and availability policies to determine whether they addressed the relevant security and availability attributes and included the annual revisions performed and reviewed by management. Inspected screenshots from Archer to determine whether policies were available to all employees. | No exceptions noted. |
| CC5.3.5 | Updates to Procedures TCH has process and procedure manuals for applications, and these processes and procedures are updated in accordance with the Information Security and Availability policies. The processes and procedures documents are available to all employees on the TCH intranet. System descriptions and manuals for applications are made available to external user entities on TCH's website, permitting users to understand their role in the system. | Inspected the process and procedure manuals for EPN, CHIPS, IXN, and RTP and corresponding intranet pages to determine whether the manuals documented application processes and procedures Inspected the revision history in the process and procedure manuals for EPN, CHIPS, IXN, and RTP to determine whether the manuals were updated in accordance with the Information Security and Availability policies. Observed TCH's website and noted system descriptions and manuals for EPN, CHIPS, IXN, and RTP were available to external user entities, permitting users to understand their role in the system. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|-----------------------------|
| CC5.3.6 | <p>Hiring Policies and Procedures</p> <p>The TCH Employee Handbook introduces and explains TCH policies, work environment, and standards in effect for all employees including personal conduct standards, company property and corrective action that will be taken due to misconduct. TCH seeks to recruit and retain a talented and diverse group of employees and ensures equal employment opportunity. TCH makes every effort to fill vacant positions with qualified employees. Employees are encouraged to explore vacant positions and career growth opportunities for retention purposes.</p> | <p>Inspected the TCH Employee Handbook to determine whether the employee handbook included TCH policies, work environment, and standards in effect for all employees including recruiting and retention efforts.</p> | <p>No exceptions noted.</p> |

CC 6.0 – Common criteria related to logical and physical access

CC6.1 – The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| CC6.1.1 | <p>Asset Classification</p> <p>TCH has policies that document requirements on removable media and asset classifications. The policies are reviewed and updated annually by the Information Security leadership team in accordance with the Information Security policies. TCH has an asset classification and management policy which establishes three levels of data classification standards which are used to help restrict access to information:</p> <p>TCH Restricted:</p> <p>Information that, if publicly disclosed, altered or destroyed without appropriate authorization, could result in severe financial loss or reputational damage to TCH. In the case of a document or email that contains information of varying sensitivity levels, the highest sensitivity level must be applied to the entire document or email. Except as otherwise set forth in the Information Classification Guidelines, no circulation is permitted outside of TCH without prior authorization of an Executive Vice President or above and the Legal department.</p> <p>TCH Confidential:</p> <p>Information that, if publicly disclosed, altered or destroyed without appropriate authorization, could result in moderate financial loss or reputational damage to TCH. Information that does not clearly fall within the TCH Restricted or Public designations should be designated TCH Confidential. Except as otherwise set forth in the Information Classification Guidelines, no circulation is permitted outside of TCH without prior authorization of Senior Vice President or above.</p> | <p>Inspected the following policy documents to determine whether they documented requirements on removable information and assets and the policy documents were updated and reviewed annually by TCH leadership.</p> <ul style="list-style-type: none"> Asset Classification and Management Policy Physical and Environment Security Policy <p>Inspected the asset classification and management policy to determine whether it documented the three levels of data classification standards and was updated and reviewed annually by the Information Security leadership team.</p> <p>Inspected a selection of sensitive, internal, and customer-facing documents maintained by TCH to determine whether asset classification types for levels of data classification were established.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|------------------------------|
| | <p>Public:</p> <p>Information that is intended for public dissemination or, if publicly disclosed, altered or destroyed without authorization, would result in no financial loss or reputational damage to TCH. Data can be circulated outside of TCH.</p> | | |
| CC6.1.2 | <p>Network Inventory</p> <p>The network tools manage the network devices and maintain an inventory. In addition, ServiceNow system scans all network subnets which also builds a device database.</p> | <p>Inspected the CMDB configuration to determine whether new IT assets were identified.</p> <p>Inspected the discovery IP range list and the discovery schedule list produced through ServiceNow to determine whether new servers and IT assets were inventoried as they come online.</p> | No exceptions noted. |
| CC6.1.3 | <p>Security Configuration – Mainframe</p> <p>Access to the Unisys production environment and development environment is controlled by the Unisys MCP operating system and the Unisys InfoGuard access control package. MCP allows programs and users access only to defined computer resources. InfoGuard is a software package which provides logical security options beyond that provided by the MCP operating system. Hardening guidelines for the security configuration of the Unisys MCP operating systems are documented and implemented within the system.</p> <p>TCH has implemented the following security rules in the production environments per the Unisys MCP hardening standard:</p> <ul style="list-style-type: none"> • Employee individual accesscode and group usercode passwords must meet a minimum length requirement. • Employee individual accesscode and group usercode passwords must be changed at specified intervals. | <p>For a selection of mainframe servers, inspected the MCP/InfoGuard logical security options to determine whether they were configured based on TCH's Information Security policy and procedures.</p> <p>For a selection of mainframe servers, individual accesscodes, and group usercodes, inspected the accesscode and usercode parameters and the Unisys configuration to determine whether the security rules were setup according to TCH's requirements.</p> | Exceptions noted, see below: |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|---|---|-------------------------|------------------|
| | <ul style="list-style-type: none"> Employee individual accesscode and group usercode passwords must be different from a certain number of passwords previously used (password history). Employee individual usercodes (with and without accesscodes) are suspended after a specified number of violations per day. Terminals are disabled after a number of invalid access attempts within certain duration of time. | | |
| <p>Exceptions Noted:</p> <p>Individual accesscodes</p> <ul style="list-style-type: none"> For 2 out of 120 individual accesscodes selected, the minimum password length was not set. For 25 of 120 individual accesscodes selected, the password was not set to expire. For 25 of 120 individual accesscodes selected, the password history was not set. For 116 of 120 individual accesscodes selected, the password lockout setting was set; however, it was not in accordance with TCH policy requirements. For 4 of 120 individual accesscodes selected, the password lockout setting was not set. <p>Group usercodes</p> <ul style="list-style-type: none"> For 1 of 40 group usercodes selected, the minimum password length was set; however, it was not in accordance with TCH policy requirements. For 13 of 40 group usercodes selected, the password was not set to expire. For 19 of 40 group usercodes selected, the password history was not set. For 39 of 40 group usercodes selected, the password lockout setting was set; however, it was not in accordance with TCH policy requirements. For 1 of 40 group usercodes selected, the password lockout setting was not set. | | | |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|--|--|---|-------------------------------------|
| CC6.1.4 | <p>Security Rules - Distributed</p> <p>TCH has implemented the following security rules for the servers, applications and databases in the distributed environment:</p> <ul style="list-style-type: none"> • A user ID and password are required. Passwords must be changed at specified interval. • Passwords must meet a minimum length requirement. • New passwords must be different from a certain number of passwords previously used. • User IDs are disabled after a number of invalid access attempts within certain duration of time. | <p>For the production systems network domains, and for a selection of Windows servers, applications and databases in the distributed environment, inspected the password parameters to determine whether the security rules were setup in accordance with TCH's requirements.</p> <p>Observed a TCH employee log on to the TCH network and noted that a username and password are required.</p> | <p>Exceptions noted, see below:</p> |
| <p>Exceptions Noted:</p> <p>Windows Databases:</p> <p>Noted that management had identified local database accounts where password rules were not enforced per TCH policy.</p> <p>Linux Servers:</p> <p>Password parameter settings for local server accounts were configured, however, not established in accordance with TCH policy; per TCH policy minimum password length required is 15 characters, however, configuration was set to 8 characters.</p> | | | |
| CC6.1.5 | <p>Individual Accesscodes</p> <p>Logical access is controlled through group usercodes and individual accesscode, requiring two different passwords. A valid group usercode, individual accesscode and passwords are required to access the system. Passwords are entered in an obfuscated field that prevents the password from being displayed on the terminal.</p> <p>Users are granted the level of access based on their job responsibilities.</p> | <p>For a selection of mainframe servers, inspected logon screens to determine whether an accesscode and password were required to login and the password was not displayed on the screen.</p> <p>Please refer to CC6.2.7 Periodic Access Review for test results of user access being granted based on job responsibility.</p> | <p>No exceptions noted.</p> |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC6.1.6 | <p>Group Usercodes – Mainframe</p> <p>Each individual with access to a group usercode, which is a shared password, is assigned a unique individual accesscode and password. Users are granted the level of access based on their job responsibilities.</p> | For a selection of mainframe servers and group usercodes, inspected usercodes' parameters and the individuals assigned to the selected group usercodes, and inspected the organization chart and inquired of management regarding users' responsibilities to determine whether users were granted access privileges based on their job responsibilities and that individual accesscode and accesscode password were assigned to each usercode per TCH information policy. | No exceptions noted. |
| CC6.1.7 | <p>Privileged Usercodes – Mainframe</p> <p>Certain usercodes are privileged and are only assigned to authorized personnel. Access to sensitive utility programs such as the COMS utility and the CANDE editor is restricted to authorized personnel based on job responsibilities.</p> | For a selection of mainframe servers, inspected the list of users that were granted privileged usercodes and/or granted access to sensitive utility programs such as the COMS utility and the CANDE editor, inspected usercodes' parameters and inquired of management regarding users' responsibilities to determine whether users were granted access privileges based on their job responsibilities. | No exceptions noted. |
| CC6.1.8 | <p>Administrator Access – Distributed Environment</p> <p>Logical access for the distributed environment is controlled by the security features of Active Directory. A valid user ID and password are required. Users are granted a level of access based on their job responsibilities. Administrative rights are restricted to authorized personnel based on their job responsibilities.</p> <p><i>RTP</i></p> <p>TCH employs two levels of security over access to the RTP production environment. Server access is restricted by Windows Jump Server and for non-locally authenticated accounts, IBM Security Directory Server via LDAP. A valid</p> | <p>For the production systems network domains, inspected the permission granted to general users to determine that users were granted access to the shared directory folders and were not granted full controls to the directory.</p> <p>For a selection of Windows servers, applications and databases in the distributed environment, inspected a list of users with administrative rights and the TCH organization chart to determine whether access was restricted based on job responsibilities.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| | user ID and password are required. Users are granted a level of access based on their job responsibilities. | Observed management log into the RTP server environment and noted that access was restricted by Windows Jump Server and IBM LDAP. | |
| CC6.1.9 | Security Violations Logon and access activities for both successful and failed attempts are captured through ArcSight. The logs are maintained in ArcSight for reference when needed. | Inspected the active channels configured within ArcSight to determine whether parameters were set to capture logon and access activities. Observed a successful and failed logon attempt and inspected the corresponding logon and logoff activity logs to determine whether logon and access activities for both successful and failed attempts were captured through ArcSight. Inspected the list of users with administrator access to ArcSight, job titles, and inquired of the management to determine whether administrative access to ArcSight was restricted to authorized personnel. | No exceptions noted. |
| CC6.1.10 | Security Administration and Security Violations ArcSight is used to support security administration including managing security violations for both mainframe and distributed environments. Security related activities such as user data change, file security attribute change and security violations including inappropriate user activity, unauthorized software, virus and firewall alerts are captured, logged and reported using ArcSight. ArcSight is configured to capture the defined security related activities and send an alert to the Information Security responsible personnel through the Information Security workstation and to their mobile phones when there is an event that meets the defined criteria such as possible security violation. Each alert is reviewed and triaged by the managed security service provider, Cipher, and followed up and cleared by Information Security, as necessary. On an ongoing basis, the Information Security | Inspected the configuration for alert event setup in ArcSight to determine whether ArcSight was setup to capture and log the security related events such as user data change, file security attribute change and security violation including inappropriate user activity, unauthorized software, IDS, virus and firewall alerts and sends automatic alerts to Cipher, and the Information Security Analyst when an event that met the defined condition occurred. Observed online ArcSight alert messages on the ArcSight workstation located in a secure area of the Information Security group and noted Information Security responded to the alert in ArcSight and that alert remained pending until it was resolved. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| | responsible personnel reviews the alerts and other activities to determine that alerts were responded to appropriately. Alerts remain pending in ArcSight until they are resolved. | For a selection of months, inspected a selected ArcSight violation report to determine whether the security violations were captured and retained in ArcSight. | |
| CC6.1.11 | Access to ServiceNow TCH uses ServiceNow to support systems development, program changes and incident reporting. Access to ServiceNow is controlled through unique username and password credentials. | Observed the login process for ServiceNow to determine users were authenticated using a username and password. Inspected access levels of all ServiceNow approval groups and inquired of management regarding users' responsibilities to determine whether users were granted access based on their job responsibilities. Compared the list of employees with access to the ServiceNow approval group against a list of terminated users to determine whether any terminated users had retained access to the ServiceNow approval groups. | No exceptions noted. |
| CC6.1.12 | Access Control Policy TCH has an access control policy that ensures access privileges are appropriately restricted, authorized and removed when no longer needed, assignments provides adequate segregation of duties and prohibits users from sharing login credentials. The policy is reviewed and updated annually by the Information Security leadership team in accordance with the Information Security policies. | Inspected the access control policy to determine whether access control topics were documented and the policy was updated and reviewed annually by the Information Security leadership team. | No exceptions noted. |
| CC6.1.13 | Unique User IDs Unique user ids are created for access to the network, applications, and databases. | For a selection of servers, applications, and databases, inspected the user listing and determined that unique user ids were created for access. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| CC6.1.14 | <p>Virus and Unauthorized Software Monitoring</p> <p>TCH utilizes Symantec Endpoint Protection to protect against viruses, malware, malicious code and unauthorized software. Virus definitions are kept current and infected files are quarantined. Security alerts are logged, reported and analyzed via ArcSight.</p> <p>Controls related security alerts being logged, reported and analyzed are described in CC7.4.4 Security Administration and Security Violations.</p> | <p>Inspected the TCH Incident Response Plan to determine whether procedures for virus definitions being kept current and infected files quarantine were documented.</p> <p>Inspected the Symantec Endpoint Protection Manager configuration to determine whether TCH workstations were protected and virus definitions were updated on a recurring basis.</p> <p>For a selection of servers, inspected the Symantec Endpoint Protection Manager configuration to determine whether TCH servers were protected.</p> <p>Observed ArcSight and noted security alerts from Symantec Endpoint Protection were configured to be logged via ArcSight.</p> | No exceptions noted. |
| CC6.1.15 | <p>Network Design</p> <p>The TCH networks are segregated from TCH's corporate network and are separate from other applications and include provisioning for redundancies.</p> <p>The EPN network design includes:</p> <ul style="list-style-type: none"> • Connect:Direct with Secure Plus, and MPLS; and • The internet using EPNAccess via the PSA VPN Appliance application security gateway or File Transfer Protocol (FTP-S). <p>The TCH CHIPS networks are segregated from TCH's corporate network and are separate from other applications and include provisioning for redundancies. The network design for each customer site includes an MPLS and ISDN backup connection. All connections are encrypted router to router using IPSec 256 AES.</p> | <p>Inspected network diagrams to determine whether the design of the TCH's EPN network was segregated from TCH's internal network and the networks for the other services and that network design included redundancy, routers, firewalls and an intrusion detection system.</p> <p>Inspected network diagrams to determine whether the design of the EPN network included Connect:Direct with Secure Plus, MPLS, EPNAccess with the VPN appliance and FTP-S.</p> <p>Inspected network diagrams to determine whether the design of the TCH's CHIPS network was segregated from TCH's internal network and networks for the other services and whether the network design included redundancy, routers, firewalls and an intrusion detection system.</p> <p>Inspected the IXN network diagrams to determine whether the design of the IXN network included an</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|------------------|
| | <p>The IXN network is segregated from TCH's internal network and networks used for the other services. The IXN network design includes redundancy, routers and firewalls. Routers and firewalls are placed at various points of the network to provide security for data transmission.</p> <p>External Network - IXN customers transmit payloads to receiving banks and transmit transmittal files to TCH over the private IXN network provided and managed by AT&T (FTP-S over the internet is available as a non-managed connectivity option). Two network hubs are maintained to provide redundancy between MPLS providers.</p> <p>The RTP network is segregated from TCH's corporate network and is separate from other applications and includes provisioning for redundancies. The RTP network design includes:</p> <ul style="list-style-type: none"> • MPLS; and • VPN network systems that provide a secure transport between TCH and its customers <p>Connect:Direct with Secure Plus is used to send reconciliation and standard reports and IBM MQ is used to send RTP messages, both methods are sent over the MPLS network or secure VPN. The endpoint routers between the customer site and TCH create an encrypted tunnel. The encryption between the customer router and the TCH data centers ensure all traffic between the sites is encrypted.</p> <p>Routers, firewalls and an intrusion detection system are used to provide network security. Router configurations include ACLs, NAT and IPSec to provide end to end network security.</p> | <p>external network provided by third parties and TCH's IXN network which was segregated from TCH's internal network and networks used for the other services and whether network design included redundancy, routers and firewalls.</p> <p>Inspected network diagrams to determine whether the design of the TCH's RTP network was segregated from TCH's corporate network and the networks for the other services and that network design included redundancy, routers, firewalls and an intrusion detection system.</p> <p>Inspected network diagrams to determine whether the design of the RTP network included MPLS, and VPN access.</p> <p>Please refer to CC6.1.16 Router Configuration for test results of router configurations.</p> <p>Please refer to CC8.1.15 Network Management Procedures for test results of network changes to TCH network.</p> | |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| CC6.1.16 | Router Configuration Routers are configured to only accept transmissions from defined IP addresses. Access to the router console requires a user ID and password via an RSA token. | For a selection of routers, inspected router configurations to determine whether the routers were configured to allow only transmissions from defined IP addresses. Observed a user login to the router configurations to determine whether a user ID and password from RSA token were required to access the routers. | No exceptions noted. |
| CC6.1.17 | Firewall Rules Firewalls are configured to allow only defined services into the TCH networks and firewall address translation is used to prevent the actual IP address from being disclosed to external parties. | For a selection of firewalls, inspected firewall rules to determine whether incoming traffic was restricted to specific logical communication ports and whether the rules were established to audit the incoming traffic and determine the source address. For a selection of firewalls, inspected the firewall configuration to determine whether address translation rules were applied to the transmissions to prevent the actual IP address from being disclosed to external parties. | No exceptions noted. |
| CC6.1.18 | Intrusion Detection System The TCH networks include an Intrusion Detection System (IDS), CarbonBlack. This system detects and classifies suspicious events according to a library of signatures provide by the vendor. The IDS/IPS is programmed to send alerts when thresholds for particular attack signatures are exceeded. Information Security management are alerted of intrusion activities. Incidents noted are recorded in ArcSight and depending on the nature and type of problem, the incident is escalated to the designated group for follow-up and resolution. If necessary, corrective action is taken via updates to policies and/or the change management process due to the alerts. | For a selection of servers, inspected the CarbonBlack management console to determine whether CarbonBlack was configured to monitor traffic. For a selection of incidents, inspected tickets and supporting documentation to determine whether the incident was escalated and resolved. Inspected configured threat intelligence library in CarbonBlack to determine whether the system was configured to detect and classify events according to the signatures. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| | <p>CarbonBlack is configured to generate alerts through ArcSight.</p> <p>Controls related incidents analysis and resolution are documented in CC7.4.4 Security Administration and Security Violations.</p> | <p>Inspected ArcSight management console to determine whether ArcSight was configured to alert Information Security in case of potential threats.</p> <p>Inspected the list of users with administrator access to CarbonBlack, job titles, and inquired of the management to determine whether administrative access to CarbonBlack was restricted to authorized personnel.</p> <p>Inquired of Information Security management regarding policy and process updates and were informed corrective action was taken via updates to policies and/or the change management process due to the alerts.</p> <p>Refer to CC7.4.4 Security Administration and Security Violations for test results of incident analysis and resolution for ArcSight.</p> | |
| CC6.1.19 | <p>Encryption – EPNAccess</p> <p>Customers use EPNAccess, a web based front-end system to transmit files to TCH. Access to EPNAccess requires a SecurID token, a valid ABA transit/routing number and associated password for file transmissions.</p> <p>EPNAccess utilizes a PSA VPN Appliance to provide security through the internet. The PSA integrates standards-based security and session encryption support is based on TLS. All files transmitted to and from EPN utilize encrypted links to ensure that the files are sent from an authorized source and are not altered or visible during transmission.</p> | <p>Inspected the EPNAccess logon screen to determine whether EPNAccess required a Secure ID token, a valid user ID or ABA transit/routing number and associated password.</p> <p>Inspected the EPNAccess logon screen and PSA VPN Appliance configuration to determine whether EPNAccess transmissions were encrypted using TLS protocol.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| CC6.1.20 | <p>Encryption – RTP Management Console</p> <p>The RTP Management Console is accessed through a third-party application security gateway, a PSA VPN Appliance, to enhance the security through the Internet. Access through the PSA is controlled through a series of authentications including RSA SecurID tokens, user groups and ACLs. The PSA provides extended secure access to corporate application resources to authorized users via standard web browsers. The PSA integrates standards-based security and session encryption is based on TLS.</p> | <p>Inspected the RTP Management Console logon screen to determine whether it was accessed via the PSA VPN appliance, and required a Secure ID token, a valid user ID and associated password.</p> <p>Inspected the PSA VPN Appliance configuration to determine whether RTP Management Console transmissions were encrypted using TLS protocol.</p> | No exceptions noted. |
| CC6.1.21 | <p>Encryption – FTP-S (EPN)</p> <p>FTP-S transmissions are routed through firewalls that allow only authorized customers to send and receive files based on IP address. Data transmissions via the internet are validated for authorized sending points by firewalls. All customer connectivity to the FTP-S system is controlled by allowing only customer host IP address and required port numbers. The EPN FTP-S transmissions are secured using TLS and PGP encryption. PGP encrypts and digitally signs files before sending them via the internet. EPN generates a pair of keys – a public key and a private key. TCH sends the public key to the EPN FTP-S customer. The customers are required to import the public key into its key files. The customer follows a required process to generate the public key and private key. New FTP-S customers are required to complete an FTP-S New Client Data Sheet with bank information and FTP-S transmission details.</p> | <p>For a selection of customer using FTP-S, inspected system generated connection log and configuration to determine whether the transmissions via FTP-S were encrypted using PGP and TLS encryption.</p> <p>Inspected firewall rules on a selection of firewalls to determine whether incoming traffic was restricted to specific number of logical communication and whether the rules were established to audit the incoming traffic and determine the source address.</p> <p>For a selection of new FTP-S customers, inspected the Client Data Sheet and connection log details to determine whether the Client Data Sheet was completed for new FTP connections and EPN/FTP-S transmissions were encrypted using PGP encryption. Refer to CC6.1.17 Firewall Rules for testing over Firewall Rules.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| CC6.1.22 | <p>Encryption – MPLS and IBM MQ (CHIPS and RTP)</p> <p>CHIPS messages utilize IBM MQ and are encrypted using TLS protocol, and digital certificate for authentication. All RTP messages are encrypted twice during transmission – at the router level using AES 256 encryption and between the customers’ MQ managers and the TCH MQ managers using IBM MQ. IBM MQ encrypts RTP messages using TLS 1.2 protocol. The sending customer’s user ID is verified through standard MQ channel initiation procedures with x509 public certificates. MQCHLAUTH records validate at runtime for each MQ channel to ensure a match otherwise the connection is rejected. In addition, RTP messages are digitally signed to ensure they have not been altered during transmission.</p> <p>Transmissions over the MPLS network are encrypted using router configurations which use IP Security (IPSec) policy and an AES 256 encryption algorithm.</p> | <p>For a selection of CHIPS customers, inspected IBM MQ TLS configuration to determine whether CHIPS messages were encrypted using TLS, digital certificate and channel verifications was enabled.</p> <p>For a selection of RTP customers, inspected IBM MQ TLS configuration and selected channel log to determine whether RTP messages were encrypted using TLS, and channel verifications was enabled.</p> <p>For a selection of MPLS customers, inspected router configurations to determine whether the transmissions used IPSec and were AES 256 encrypted.</p> <p>For a selection of routers, inspected router configurations to determine whether the transmissions used IPSec and were AES 256 encrypted.</p> <p>Please refer to CC6.1.35 RTP Messages and Authentication for results of testing digitally signed messages.</p> | No exceptions noted. |
| CC6.1.23 | <p>Encryption – MPLS and Connect:Direct with Secure Plus (EPN)</p> <p>EPN messages transmitted via Connect:Direct with Secure Plus are encrypted to protect the messages from alteration of data while in transit.</p> <p>In addition, transmissions over the MPLS network are encrypted using router configurations which use IP Security (IPSec) policy and an AES 256 encryption algorithm.</p> | <p>For a selection of customers using Connect:Direct with Secure Plus, inspected the node configurations to determine whether the data transmissions between customer and EPN were encrypted.</p> <p>For a selection of MPLS customers, inspected router configurations to determine whether the data transmissions used IPSec and were AES 256 encrypted.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| CC6.1.24 | <p>Data Encryption – Connect:Direct with Secure Plus and FTP-S (IXN)</p> <p>IXN messages transmitted via Connect:Direct with Secure Plus are encrypted to protect the messages from alteration of data while in transit.</p> <p>FTP-S transmissions are routed through firewalls that allow only authorized customers to send and receive files based on IP address. Data transmissions via the internet are validated for authorized sending points by firewalls. All customer connectivity to the FTP-S system is controlled by allowing only customer host IP address and required port numbers. The IXN FTP-S transmissions are secured using TLS and PGP encryption. PGP encrypts and digitally signs files before sending them via the internet using a pair of keys – a public key and a private key.</p> | <p>For a selection of customers using Connect:Direct with Secure Plus, inspected the node configuration to determine data transmissions between customer and IXN were encrypted.</p> <p>For a selection of customer using FTP-S, inspected system generated connection log and configuration to determine whether the transmissions via FTP-S were encrypted using PGP encryption and TLS.</p> <p>Inspected the system generated list of new IXN customers and noted there were no new FTP installs for new customers during the period; therefore, the operating effectiveness of this control for new client FTP installs could not be tested.</p> <p>Refer to CC6.1.17 Firewall Rules for testing over Firewall Rules.</p> | No exceptions noted. |
| CC6.1.25 | <p>Encryption - Connect:Direct with Secure Plus (RTP)</p> <p>Clients may elect to receive standard reconciliation reports via Connect:Direct with Secure Plus which uses Transport Layer Security (TLS) providing a secure layer on top of TCP/IP over the MPLS network or secure VPN.</p> <p>In addition, transmissions over the MPLS network are encrypted via router configurations which use IP Security (IPsec) and an AES 256 encryption algorithm.</p> | <p>For a selection of nodes using Connect:Direct with Secure Plus, inspected the node configurations to determine whether the data transmissions between customer and RTP were encrypted.</p> <p>For a selection of MPLS routers, inspected router configurations to determine whether the data transmissions used IPsec and were AES 256 encrypted.</p> | No exceptions noted. |
| CC6.1.26 | <p>Remote Access</p> <p>TCH's employees and contractors are granted access to the TCH network from remote locations to support operations. An approval from designated management is required for remote access.</p> | <p>For a selection of employees and contractors from the RSA SecurID token report inquired of Information Security Director regarding their job responsibilities to determine whether they were current employees and contractors and required remote access to carry out their job responsibilities.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| | Remote access requires multi-factor authentication, controlled through VPN or VDI using network credentials and SecurID tokens. Controls related to new remote access requests are described in CC6.3.2. | <p>Compared the list of employees with access to RSA tokens against a list of terminated users to determine whether any terminated users had retained access to RSA tokens.</p> <p>Please refer to CC6.3.2 Access Authorization - SecurID for test results of approval of new remote access requests.</p> <p>Observed a TCH employee access TCH's network via remote access via VPN and VDI, and noted that a password and SecurID were required.</p> | |
| CC6.1.27 | <p>Server Hardening</p> <p>TCH provides hardening standards for system administrators in order to implement secure server configurations within the company's infrastructure. The guidelines are reviewed and updated when changes occur by the Information Security team.</p> <p>Monthly validation of compliance to hardening standards occurs through the use of BigFix. Weekly meetings are held to discuss compliance results, and if necessary, tickets are created for remediation or a policy exception is documented in Archer.</p> | <p>Inspected the hardening guidelines to determine whether they document approved hardening standards for server configurations.</p> <p>For a selection of months, inspected monthly compliance report to determine whether compliance checks were performed to ensure devices were hardened per defined standards.</p> <p>For a selection of weeks, inspected the compliance meeting invite and notes to determine whether compliance results were discussed, and if necessary, tickets were created for remediation of any noted issues or a policy exception was documented in Archer.</p> | No exceptions noted. |
| CC6.1.28 | <p>Connect:Direct with Secure Plus EPN Users</p> <p>Profiles are established for customers using Connect:Direct with Secure Plus and users are restricted to specific directories assigned for file transmission.</p> | For a selection of customers using Connect:Direct with Secure Plus, inspected the configurations for customer profiles on the Connect:Direct with Secure Plus server to determine whether users were restricted to specific directories. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| CC6.1.29 | <p>EPN FTP-S Users</p> <p>Each customer using FTP-S requires a valid user ID and password for transmitting files to TCH through the FTP-S server. FTP-S profiles are established for customers using FTP-S and users are restricted to specific directories on the FTP-S server assigned for file transmission.</p> | <p>For a selection of customers using FTP-S, inspected the configuration of customer profiles on the FTP-S server to determine whether user IDs and passwords were required and users were restricted to specific directories.</p> <p>Observed a TCH employee's attempt to access EPN via FTP-S and noted that user ID and password were required.</p> | No exceptions noted. |
| CC6.1.30 | <p>UPIC Option</p> <p>Customers may elect to use UPIC, an optional feature of the EPN system. EPN customers who register for UPIC can access the UPIC database through a secure connection over the internet or using Connect:Direct with Secure Plus. Access to UPIC is controlled through a unique user ID and password, firewalls and VPN.</p> <p>UPIC is available to all EPN customers upon completion of a UPIC registration letter. Each customer is provided a minimum of two SecurID tokens and two passwords. Customers must change the password upon initial login.</p> | <p>Inspected the UPIC logon screen to determine whether it required a SecurID, a valid user ID and associated password.</p> <p>For a selection of new UPIC customers, inspected the registration letter to determine it was completed.</p> | No exceptions noted. |
| CC6.1.31 | <p>Laptop and Mobile Device Encryption</p> <p>TCH laptops have hard drive encryption technology installed and activated. By default, Universal Serial Bus (USB) access is set to read only. TCH mobile devices used to access emails are encrypted.</p> | <p>Inspected the global encryption configuration to determine whether encryption mechanisms were enforced.</p> <p>Inspected the USB group policy to determine whether USB ports are globally set to read-only.</p> <p>For a selection of employees, inspected mobile device encryption settings to determine whether mobile devices were encrypted.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC6.1.32 | <p>Separate Environments</p> <p>Programmers develop programs on a stand-alone processor or servers dedicated for program development and testing.</p> <p><i>RTP</i></p> <p>RTP source code is developed by a third-party vendor. Requirements for RTP development work is provided to the third-party developer in business requirement documentation. Source code packages are provided and then deployed and tested within the development environment by TCH.</p> | <p>Inspected the system configuration for both the Unisys and distributed environments to determine whether test and development environments were separated from the production environments.</p> <p>Refer to CC8.1.4 Application, Program and Configuration Program Development and Test Environment for evidence of RTP development and testing.</p> | No exceptions noted. |
| CC6.1.33 | <p>Source Code Repository</p> <p>Team Foundation Server (TFS) is utilized for source code management. Application functionality regardless of data center location is identical and shares the same application code.</p> | Observed TFS and noted the tool was utilized for EPN, CHIPS, IXN and RTP source code management. | No exceptions noted. |
| CC6.1.34 | <p>RTP Management Console Authentication</p> <p>Users accessing the RTP Management Console are required to authenticate via two factor authentication using a token and then an additional set of credentials.</p> <p>The RTP Management Console is configured to lock out user accounts after three (3) unsuccessful login attempts. In the event a user attempts to log into the RTP Management Console after three failed login attempts, the user will be notified that the account has been locked, and the user will be instructed to contact their system administrator.</p> | <p>Inspected the RTP Management Console logon screen to determine whether it required a Secure ID token, a valid user ID and associated password.</p> <p>Inspected RTP application password configurations to determine whether the RTP Management Console was configured to lockout user accounts after three (3) unsuccessful login attempts.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|---|---|--|----------------------|
| CC6.1.35 | RTP Messages and Authentication RTP participants must digitally sign their messages to ensure authenticity. Each participant provides a trusted certificate upon onboarding to be used to validate their digital signatures. The RTP system will reject any message that fails this validation. | Inspected the RTP interface guide to determine whether participants were required to digitally sign their messages to ensure authenticity. For a selection of onboarded RTP participants, inspected digital signature configurations to determine whether participants were configured to digitally sign their messages. Observed a QC specialist send a test RTP message and noted the system rejected messages that failed digital signature validation. Observed the test environment and production environment and noted test mirrored production. | No exceptions noted. |
| Complementary User Entity Control(s) | | | |
| Controls should be established at user entities so that: <ul style="list-style-type: none"> • Users manage security for their Connect:Direct with Secure Plus software for encryption used for transmissions. • Users send acknowledgement of receipt of the Privacy-Enhanced Mail (PEM) to TCH. • Users store the Privacy-Enhanced Mail (PEM) containing public keys in a secure location and provide the public keys to TCH. | | | |

CC6.2 – Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC6.2.1 | <p>Access Authorization – Logical Access</p> <p>New employee and transfer access requests are processed and approved through the Courion tool via an automated access request form. Courion is used for requesting a new user account in Active Directory and the related usercode in the Unisys, and deleting existing user accounts/usercodes. Upon approval by the individual's manager, Courion automatically routes the access request to designated departments based on the access requested for provisioning of the request. Courion is also used to approve/recertify access levels for transferred employees. The Courion tool provides an automatic notification, electronic approval and audit trails of all activities.</p> <p>Access to the Courion system is controlled through the security features of Active Directory.</p> <p>Changes to existing user access is requested and approved by the department manager through a ServiceNow ticket with appropriate approval.</p> <p>Changes to the security files including additions, deletions and changes to the user profiles are captured by the systems. Through ArcSight, Information Security reviews the results of user account setup and privileged user activity. Controls related to security administration using ArcSight are described in CC7.4.4 Security Administration and Security Violations.</p> | <p>For a selection of new hires and existing user access modifications, inspected the related Courion forms or the related ServiceNow ticket to determine whether the requests and access level to be granted were reviewed and approved by the individual's manager.</p> <p>For a selection of new hires, inspected the ArcSight reports for User Accounts Created to determine whether new user accounts created were captured in ArcSight.</p> <p>For a selection of transfers, inspected the related Courion forms to determine whether access modifications (if required) were approved by the individual's manager.</p> <p>Observed the automatic routing within Courion to determine that access requests are automatically routed to designated departments based on access types requested for provisioning of the request.</p> <p>Inspected the list of users with administrator access to Courion, job titles, and inquired of the management to determine whether administrative access to Courion was restricted to authorized personnel.</p> <p>Observed the login process for Courion and noted that user IDs and passwords were required to access the LAN and that access to Courion was authenticated through Windows Active Directory.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| | | Please refer to CC7.4.4 Security Administration and Security Violations for results of testing security administration. | |
| CC6.2.2 | <p>Access Authorization – SecurID</p> <p>Requests for granting new remote access via SecurID tokens for TCH employees (internal users) are initiated in ServiceNow. These requests are then processed through ServiceNow by Identity and Access Management. Internal user new token requests are reviewed and approved by appropriate TCH management. Token renewals for internal users do not require further approval.</p> <p>Requests for new customers’ user (external users) tokens are initiated by a SecurID request form, authorized by Client Services and documented in ServiceNow. External user token renewals also require authorization via a Token Holder List.</p> | For a selection of new and renewed tokens for customers (customer banks) and internal users, inspected the ServiceNow tickets and supporting documentation to determine whether customers and internal users were granted remote access based on approved requests or SecurID request forms/Token Holder Lists where applicable. | No exceptions noted. |
| CC6.2.3 | <p>Remote Access</p> <p>TCH’s employees and contractors are granted access to the TCH network from remote locations to support operations. An approval from designated management is required for remote access.</p> <p>Remote access requires multi-factor authentication, controlled through VPN or VDI using network credentials and SecurID tokens.</p> <p>Controls related to new remote access requests are described in CC6.3.2.</p> | <p>For a selection of employees and contractors from the RSA SecurID token report inquired of Information Security Director regarding their job responsibilities to determine whether they were current employees and contractors and required remote access to carry out their job responsibilities.</p> <p>Compared the list of employees with access to RSA tokens against a list of terminated users to determine whether any terminated users had retained access to RSA tokens.</p> <p>Please refer to CC6.3.2 Access Authorization - SecurID for test results of approval of new remote access requests.</p> <p>Observed a TCH employee access TCH’s network via remote access via VPN and VDI, and noted that a password and SecurID were required.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| CC6.2.4 | Account Sharing TCH has an access control policy that prohibits users from sharing login credentials. The policy is reviewed and updated annually by the Information Security leadership team in accordance with the Information Security policies | Inspected the access control policy to determine whether it prohibits users from sharing login credentials and was updated and reviewed annually by the Information Security leadership team. | No exceptions noted. |
| CC6.2.5 | Unique User IDs Unique user ids are created for access to the network, applications, and databases. | For a selection of servers, applications, and databases, inspected the user listing and determined that unique user ids were created for access. | No exceptions noted. |
| CC6.2.6 | Access Revocation and Adjustment - Logical Notifications for employee terminations are processed through the Courion tool. The requests are automatically routed to the Identity and Access management group and designated departments based on the individual's access for access revocation. | For a selection of employee terminations from the lists provided by HR, inspected the related Courion forms and system generated access removal logs to determine whether access for terminated employees was removed from the network in a timely manner. Compared terminated users against the active list of users with access to in-scope systems to determine whether terminated users' access was revoked. Observed the automatic routing within Courion to determine that access removal requests are automatically routed to designated departments based on access types for the deprovisioning of the access. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|----------------------|
| CC6.2.7 | <p>Periodic Access Review</p> <p>On a semi-annual basis, the management of each employee reviews and confirms the employee access or provides changes to Identity and Access Management. All access modification requests are processed by Identity and Access Management.</p> <p>On a quarterly basis, management reviews and confirms privileged access or provides changes to Identity and Access Management team. All access modification requests are processed by Identity and Access Management Team.</p> | <p>Inspected the Entitlement Review Policy to determine whether the TCH's user entitlement review process was documented and maintained.</p> <p>Inspected the latest user entitlement review for the all-inclusive semi-annual review to determine whether access was reviewed as required.</p> <p>For a selection of access modifications identified during the all-inclusive user entitlement review, inspected system generated listings to determine whether modifications noted by the reviewer were completed.</p> <p>Inspected the latest user entitlement review for privileged access review to determine whether access was reviewed as required.</p> <p>For a selection of access modifications identified during the privileged user entitlement reviews, inspected system generated listings to determine whether modifications noted by the reviewer were completed.</p> <p>Inspected TCH's Access Management Training documentation to determine whether the training addressed segregation of duties and "toxic pairs" examples.</p> | No exceptions noted. |
| CC6.2.8 | <p>Break-glass Access</p> <p>Emergency access may be granted as part of the break-glass process to facilitate resolution of a production issue. Credentials are provisioned upon approval. If the break-glass process is invoked, a ServiceNow ticket is raised and the credentials are used. Information Security monitors the use of the break-glass credentials via ArcSight, and if used, Identity and Access Management supplies new credentials.</p> | <p>Inquired of management regarding the break-glass access process.</p> <p>For the break-glass access occurrence during the period, inspected corresponding ticket and system log to determine whether break-glass access was documented, approved, and the use of break-glass credentials was logged and new credentials were supplied.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|----------------------|
| CC6.2.9 | <p>EPNAccess Users</p> <p>Requests for access to EPNAccess are made in writing by customers using a SecurID Request Form, and authorized by Client Services. The Identity and Access Management team uses ServiceNow for submitting requests for a new access, deleting an existing access or changing access. Access to EPNAccess requires a SecurID token, a valid user ID or ABA transit/routing number and associated password.</p> | <p>Inspected the EPNAccess logon screen to determine whether files transmitted via EPNAccess required a SecurID token, a valid user ID or ABA transit/routing number and associated password.</p> <p>Inspected a listing of client EPNAccess user removal requests and noted there were none during the period; therefore, the operating effectiveness of the control for requested client EPNAccess user removals could not be tested.</p> <p>Please refer to CC6.3.2 Access Authorization - SecurID for test results of access authorization to SecurID.</p> | No exceptions noted. |
| CC6.2.10 | <p>UPIC Option</p> <p>Customers may elect to use UPIC, an optional feature of the EPN system. EPN customers who register for UPIC can access the UPIC database through a secure connection over the internet or using Connect:Direct with Secure Plus. Access to UPIC is controlled through a unique user ID and password, firewalls and VPN.</p> <p>UPIC is available to all EPN customers upon completion of a UPIC registration letter. Each customer is provided a minimum of two SecurID tokens and two passwords. Customers must change the password upon initial login.</p> | <p>Inspected the UPIC logon screen to determine whether it required a SecurID, a valid user ID and associated password.</p> <p>For a selection of new UPIC customers, inspected the registration letter to determine it was completed.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC6.2.11 | <p>Access to CHIPSWeb</p> <p>Customers access CHIPSWeb through a secure VPN using TLS authentication. All connections are encrypted using TLS protocol. A secure token is used for dual factor authentication for accessing the VPN. A customer accessing VPN requires a secure token key, unique username and PIN which is issued by the Identity and Access Management department.</p> <p>Customers must request, in writing, the secure token from the Identity and Access Management department. This department is responsible for distributing the secure key token and PIN to the customer.</p> | <p>Observed TCH management access the CHIPSWeb and noted that a user ID, secure token key and PIN were required to gain access to the tool.</p> <p>Please refer to CC6.3.2 Access Authorization - SecurID for test results of access authorization to SecurID.</p> | No exceptions noted. |
| CC6.2.12 | <p>Customer User Access (IXN)</p> <p>Customers access IXN using SVPCOView, a web based system management tool provided by TCH. As part of customer setup, the customer is provided access to SVPCOView for file transmission and other IXN related processing. The customer submits a SecurID Request Form to TCH for a user ID for the customer's local security administrator account which is authorized by Client Services. The Identity and Access Management team uses ServiceNow for submitting requests for a new access, deleting an existing access or changing access. The customer's user account is setup based on the customer's transit/routing number. Access to SVPCOView requires user IDs and SecurID tokens assigned to each participant.</p> | <p>Inquired of the VP of Operations, Client Services regarding the access controls for SVPCOView.</p> <p>Observed a Payments Specialist Representative logon to SVPCOView and noted that user ID, PIN and SecurID token key were required to access SVPCOView.</p> <p>Please refer to CC6.3.2 Access Authorization - SecurID for test results of access authorization to SecurID.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| CC6.2.13 | RTP Management Console Access Requests for SecurID tokens to access the RTP Management Console are made in writing by the customers using a SecurID Request form and authorized by Client Services. The Identity and Access Management team uses ServiceNow for submitting requests for new access, deleting existing access or changing access. Access to the RTP Management Console requires a SecurID token, a valid user ID and password. | Inspected the RTP Management Console logon screen to determine whether a SecurID token, a valid user ID and associated password were required. Please refer to CC6.3.2 Access Authorization – SecurID for test results relating to access authorization to SecurID. | No exceptions noted. |
| CC6.2.14 | RTP Onboarding/ Customer Setup The RTP Client Services Handbook provides requirements for adding, maintaining and removing RTP customers. New customers are added based on an executed SecurID Form, Security Officer & Application Admin Form, Contact Information Form, MPLS Router Configuration Form, and VPN Configuration Form (if VPN is used instead of MPLS), MQ Configuration Form, MQ Digital Certificate Form, Application Digital Signature Certificates Form, Connect:Direct Configuration Form, Connect:Direct TLS Digital Certificates Form, and Connect:Direct Report Selection Form, as applicable to the setup. | Inspected the RTP Client Services Handbook to determine whether it provided requirements for adding, maintaining and removing RTP customers. For a selection of onboarded RTP participants, inspected associated forms and setup documentation to determine whether the required onboarding and customer setup documentation was executed, as applicable. | No exceptions noted. |

Complementary User Entity Control(s)

Controls should be established at user entities so that:

- Only properly authorized user personnel have access to terminals or other equipment used for transaction entry and control procedures over the use of RTP Management Console username, password, and PIN are in place.
- SecurID tokens are distributed to authorized personnel.
- Access to RTP Management Console is controlled and only authorized personnel can withdraw funds.

CC6.3 – The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity’s objectives.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC6.3.1 | <p>Access Authorization – Logical Access</p> <p>New employee and transfer access requests are processed and approved through the Courion tool via an automated access request form. Courion is used for requesting a new user account in Active Directory and the related usercode in the Unisys, and deleting existing user accounts/usercodes. Upon approval by the individual’s manager, Courion automatically routes the access request to designated departments based on the access requested for provisioning of the request. Courion is also used to approve/recertify access levels for transferred employees. The Courion tool provides an automatic notification, electronic approval and audit trails of all activities.</p> <p>Access to the Courion system is controlled through the security features of Active Directory.</p> <p>Changes to existing user access is requested and approved by the department manager through a ServiceNow ticket with appropriate approval.</p> <p>Changes to the security files including additions, deletions and changes to the user profiles are captured by the systems. Through ArcSight, Information Security reviews the results of user account setup and privileged user Controls related to security administration using ArcSight are described in CC7.4.4 Security Administration and Security Violations.</p> | <p>For a selection of new hires and existing user access modifications, inspected the related Courion forms or the related ServiceNow ticket to determine whether the requests and access level to be granted were reviewed and approved by the individual’s manager.</p> <p>For a selection of new hires, inspected the ArcSight reports for User Accounts Created to determine whether new user accounts created were captured in ArcSight.</p> <p>For a selection of transfers, inspected the related Courion forms to determine whether access modifications (if required) were approved by the individual’s manager.</p> <p>Observed the automatic routing within Courion to determine that access requests are automatically routed to designated departments based on access types requested for provisioning of the request.</p> <p>Inspected the list of users with administrator access to Courion, job titles, and inquired of the management to determine whether administrative access to Courion was restricted to authorized personnel.</p> <p>Observed the login process for Courion and noted that user IDs and passwords were required to access the LAN and that access to Courion was authenticated through Windows Active Directory. Please refer to CC7.4.4 Security Administration and</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| | | Security Violations for results of testing security administration. | |
| CC6.3.2 | <p>Access Authorization – SecurID</p> <p>Requests for granting new remote access via SecurID tokens for TCH employees (internal users) are initiated in ServiceNow. These requests are then processed through ServiceNow by Identity and Access Management. Internal user new token requests are reviewed and approved by appropriate TCH management. Token renewals for internal users do not require further approval.</p> <p>Requests for new customers’ user (external users) tokens are initiated by a SecurID request form, authorized by Client Services and documented in ServiceNow. External user token renewals also require authorization via a Token Holder List.</p> | For a selection of new and renewed tokens for customers (customer banks) and internal users, inspected the ServiceNow tickets and supporting documentation to determine whether customers and internal users were granted remote access based on approved requests or SecurID request forms/Token Holder Lists where applicable. | No exceptions noted. |
| CC6.3.3 | <p>Remote Access</p> <p>TCH’s employees and contractors are granted access to the TCH network from remote locations to support operations. An approval from designated management is required for remote access.</p> <p>Remote access requires multi-factor authentication, controlled through VPN or VDI using network credentials and SecurID tokens. Controls related to new remote access requests are described in CC6.3.2.</p> | <p>For a selection of employees and contractors from the RSA SecurID token report inquired of Information Security Director regarding their job responsibilities to determine whether they were current employees and contractors and required remote access to carry out their job responsibilities.</p> <p>Compared the list of employees with access to RSA tokens against a list of terminated users to determine whether any terminated users had retained access to RSA tokens.</p> <p>Please refer to CC6.3.2 Access Authorization - SecurID for test results of approval of new remote access requests.</p> <p>Observed a TCH employee access TCH’s network via remote access via VPN and VDI, and noted that a password and SecurID were required.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|----------------------|
| CC6.3.4 | <p>Break-glass Access</p> <p>Emergency access may be granted as part of the break-glass process to facilitate resolution of a production issue. Credentials are provisioned upon approval. If the break-glass process is invoked, a ServiceNow ticket is raised and the credentials are used. Information Security monitors the use of the break-glass credentials via ArcSight, and if used, Identity and Access Management supplies new credentials.</p> | <p>Inquired of management regarding the break-glass access process.</p> <p>For the break-glass access occurrence during the period, inspected corresponding ticket and system log to determine whether break-glass access was documented, approved, and the use of break-glass credentials was logged and new credentials were supplied.</p> | No exceptions noted. |
| CC6.3.5 | <p>EPNAccess Users</p> <p>Requests for access to EPNAccess are made in writing by customers using a SecurID Request Form, and authorized by Client Services. The Identity and Access Management team uses ServiceNow for submitting requests for a new access, deleting an existing access or changing access. Access to EPNAccess requires a SecurID token, a valid user ID or ABA transit/routing number and associated password.</p> | <p>Inspected the EPNAccess logon screen to determine whether files transmitted via EPNAccess required a SecurID token, a valid user ID or ABA transit/routing number and associated password.</p> <p>Inspected a listing of client EPNAccess user removal requests and noted there were none during the period; therefore, the operating effectiveness of the control for requested client EPNAccess user removals could not be tested.</p> <p>Please refer to CC6.3.2 Access Authorization - SecurID for test results of access authorization to SecurID.</p> | No exceptions noted. |
| CC6.3.6 | <p>UPIC Option</p> <p>Customers may elect to use UPIC, an optional feature of the EPN system. EPN customers who register for UPIC can access the UPIC database through a secure connection over the internet or using Connect:Direct with Secure Plus. Access to UPIC is controlled through a unique user ID and password, firewalls and VPN.</p> <p>UPIC is available to all EPN customers upon completion of a UPIC registration letter. Each customer is provided a</p> | <p>Inspected the UPIC logon screen to determine whether it required a SecurID, a valid user ID and associated password.</p> <p>For a selection of new UPIC customers, inspected the registration letter to determine it was completed.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| | minimum of two SecurID tokens and two passwords. Customers must change the password upon initial login. | | |
| CC6.3.7 | <p>Access to CHIPSWeb</p> <p>Customers access CHIPSWeb through a secure VPN using TLS authentication. All connections are encrypted using TLS protocol. A secure token is used for dual factor authentication for accessing the VPN. A customer accessing VPN requires a secure token key, unique username and PIN which is issued by the Identity and Access Management department.</p> <p>Customers must request, in writing, the secure token from the Identity and Access Management department. This department is responsible for distributing the secure key token and PIN to the customer.</p> | <p>Observed TCH management access the CHIPSWeb and noted that a user ID, secure token key and PIN were required to gain access to the tool.</p> <p>Please refer to CC6.3.2 Access Authorization - SecurID for test results of access authorization to SecurID.</p> | No exceptions noted. |
| CC6.3.8 | <p>Customer User Access (IXN)</p> <p>Customers access IXN using SVPCOView, a web based system management tool provided by TCH. As part of customer setup, the customer is provided access to SVPCOView for file transmission and other IXN related processing. The customer submits a SecurID Request Form to TCH for a user ID for the customer's local security administrator account which is authorized by Client Services. The Identity and Access Management team uses ServiceNow for submitting requests for a new access, deleting an existing access or changing access. The customer's user account is setup based on the customer's transit/routing number. Access to SVPCOView requires user IDs and SecurID tokens assigned to each participant.</p> | <p>Observed a Payments Specialist Representative logon to SVPCOView and noted that user ID, PIN and SecurID token key were required to access SVPCOView.</p> <p>Please refer to CC6.3.2 Access Authorization - SecurID for test results of access authorization to SecurID.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| CC6.3.9 | <p>RTP Management Console Access</p> <p>Requests for SecurID tokens to access the RTP Management Console are made in writing by the customers using a SecurID Request form and authorized by Client Services. The Identity and Access Management team uses ServiceNow for submitting requests for new access, deleting existing access or changing access. Access to the RTP Management Console requires a SecurID token, a valid user ID and password.</p> | <p>Inspected the RTP Management Console logon screen to determine whether a SecurID token, a valid user ID and associated password were required.</p> <p>Please refer to CC6.3.2 Access Authorization – SecurID for test results relating to access authorization to SecurID.</p> | No exceptions noted. |
| CC6.3.10 | <p>Periodic Access Review</p> <p>On a semi-annual basis, the management of each employee reviews and confirms the employee access or provides changes to Identity and Access Management. All access modification requests are processed by Identity and Access Management.</p> <p>On a quarterly basis, management reviews and confirms privileged access or provides changes to Identity and Access Management team. All access modification requests are processed by Identity and Access Management Team.</p> | <p>Inspected the Entitlement Review Policy to determine whether the TCH’s user entitlement review process was documented and maintained.</p> <p>Inspected the latest user entitlement review for the all-inclusive semi-annual review to determine whether access was reviewed as required.</p> <p>For a selection of access modifications identified during the all-inclusive user entitlement review, inspected system generated listings to determine whether modifications noted by the reviewer were completed.</p> <p>Inspected the latest user entitlement review for privileged access review to determine whether access was reviewed as required.</p> <p>For a selection of access modifications identified during the privileged user entitlement reviews, inspected system generated listings to determine whether modifications noted by the reviewer were completed. Inspected TCH’s Access Management Training documentation to determine whether the training addressed segregation of duties and “toxic pairs” examples.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| CC6.3.11 | <p>Access Revocation and Adjustment - Logical</p> <p>Notifications for employee terminations are processed through the Courion tool. The requests are automatically routed to the Identity and Access management group and designated departments based on the individual's access for access revocation.</p> | <p>For a selection of employee terminations from the lists provided by HR, inspected the related Courion forms and system generated access removal logs to determine whether access for terminated employees was removed from the network in a timely manner.</p> <p>Compared terminated users against the active list of users with access to in-scope systems to determine whether terminated users' access was revoked.</p> <p>Observed the automatic routing within Courion to determine that access removal requests are automatically routed to designated departments based on access types for the deprovisioning of the access.</p> | No exceptions noted. |
| CC6.3.12 | <p>Privileged Usercodes - Mainframe</p> <p>Certain usercodes are privileged and are only assigned to authorized personnel. Access to sensitive utility programs such as the COMS utility and the CANDE editor is restricted to authorized personnel based on job responsibilities.</p> | <p>For a selection of mainframe servers, inspected the list of users that were granted privileged usercodes and/or granted access to sensitive utility programs such as the COMS utility and the CANDE editor, inspected usercodes' parameters and inquired of management regarding users' responsibilities to determine whether users were granted access privileges based on their job responsibilities.</p> | No exceptions noted. |
| CC6.3.13 | <p>Administrative Access to Tools</p> <p>Administrator access to tools is granted to employees based on their job responsibilities.</p> | <p>For a selection of tools, inspected the list of users with administrator access, job titles, and inquired of management to determine whether administrative access was restricted to authorized personnel based on job responsibilities.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| CC6.3.14 | <p>Segregation of Duties</p> <p>TCH provides segregation of duties to effectively control the concentration of functions within the organization. The separation of Operations and Technology duties from TCH's Product Development & Management Division and other Administrative functions, which include accounting and finance, audit and human resources, provides an additional level of segregation of functions within TCH.</p> <p>Access Management training addresses segregation of duties and includes descriptions of "toxic pairs" (entitlements that should not be granted to certain roles). Management reviews and recertifies access entitlements throughout the year and reject any access entitlements that are not least privileged or segregated as appropriate. In the event that "toxic pair" entitlements are required for an individual, there is a policy exception and registration process for risk acceptance.</p> <p>Controls related to the access recertifications are documented in CC6.2.7 Periodic Access Review.</p> | <p>Inspected TCH's organizational charts and job descriptions to determine whether duties were segregated within the organization.</p> <p>Inspected TCH's Access Management Training documentation to determine whether the training addressed segregation of duties and "toxic pairs" concepts.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| CC6.3.15 | <p>Access to the Production Environment</p> <p>Employees are granted access to the production environment and Control File based on their job responsibilities. Programmers do not have access to the production environment.</p> <p>Employees are granted access to the system files based on their job responsibilities. Logical access for the distributed environment is controlled by the security features of Active Directory. A valid user ID and password are required. Users are granted a level of access based on their job responsibilities. Administrative rights are restricted to authorized personnel based on their job responsibilities.</p> <p>TCH employs two levels of security over access to the RTP production environment. Server access is restricted by Windows Jump Server and for non-locally authenticated accounts, IBM Security Directory Server via LDAP. A valid user ID and password are required. Users are granted a level of access based on their job responsibilities.</p> | <p>For a selection of mainframe servers and usercodes, inspected the Make User reports, a system generated security report for Unisys, and system-generated HR termination listings and inquired of management of the individuals' job responsibilities to determine whether programmers did not have access to the production environment and access to the Control File (Unisys) was limited to support teams and authorized management based on their job responsibilities.</p> <p>For a selection of servers, applications and databases in the distributed environment, inspected the users who were granted update access to the production environment (system administration capabilities), and system-generated HR termination listings and inquired of management of the individuals' job responsibilities to determine whether programmers did not have access to the production environment and access was limited to support teams and authorized management based on their job responsibilities.</p> <p>Observed personnel log into the RTP server environment and noted that access was restricted by Windows Jump Server and IBM LDAP, and for locally authenticated accounts that a valid user ID and password were required.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|--|--|--|----------------------|
| CC6.3.16 | <p>Administrator Access - Distributed Environment</p> <p>Logical access for the distributed environment is controlled by the security features of Active Directory. A valid user ID and password are required. Users are granted a level of access based on their job responsibilities. Administrative rights are restricted to authorized personnel based on their job responsibilities.</p> <p>TCH employs two levels of security over access to the RTP production environment. Server access is restricted by Windows Jump Server and for non-locally authenticated accounts, IBM Security Directory Server via LDAP. A valid user ID and password are required. Users are granted a level of access based on their job responsibilities.</p> | <p>For the production systems network domains, inspected the permission granted to general users to determine that users were granted access to the shared directory folders and were not granted full controls to the directory.</p> <p>For a selection of Windows servers, applications and databases in the distributed environment, inspected a list of users with administrative rights and the TCH organization chart to determine whether access was restricted based on job responsibilities.</p> <p>Observed management log into the RTP server environment and noted that access was restricted by Windows Jump Server and IBM LDAP.</p> | No exceptions noted. |
| Complementary User Entity Control(s) | | | |
| <p>Controls should be established at user entities so that:</p> <ul style="list-style-type: none"> Only properly authorized user personnel have access to terminals or other equipment used for transaction entry, and control procedures over the use of RTP Management Console username, password, and PIN are in place. SecurID tokens are distributed to authorized personnel. Access to RTP Management Console is controlled and only authorized personnel can withdraw funds. | | | |

CC6.4 – The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity’s objectives.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|----------------------|
| CC6.4.1 | <p>Physical Access Control Policy</p> <p>TCH has documented policies and procedures for physical access including procedures over the security of company premises (external doors, emergency exits, surveillance etc.), protections over systems and equipment, and security of data-bearing assets.</p> | <p>Inspected the Physical Security Policy manual to determine whether the policies and procedures for physical security were documented and maintained. Toured the North Carolina and New York processing facilities and North Carolina data center and observed the following:</p> <ul style="list-style-type: none"> • Access was controlled by multi-zoned biometric access systems located in separate secure areas of the New York and North Carolina facilities. • In the “man trap”, the second entrance could not be opened if the first entrance was not closed. • The data center and telecommunication area at each facility were in separate access zones. • The security guards monitored the facilities through closed circuit televisions. • The security guards toured the facilities several times throughout the day. | No exceptions noted. |
| CC6.4.2 | <p>Access Authorization – Physical Access</p> <p>The Corporate Real Estate group is responsible for administering access to facilities and the data centers.</p> <p>New employee access requests are processed and approved through the Courion Tool, a third party software package.</p> <p>An automated access request form using the Courion Tool is used for requesting access to the facilities and data centers. The tool provides for automatic notification and electronic</p> | <p>For a selection of new hires from a list provided by HR, inspected the Courion notification and facility access level report to determine whether the request forms were approved by the new employee’s manager and access was granted based on approved requests.</p> <p>For the TCH employee granted permanent access to the Pennsylvania data center during the period, inspected approval documentation to determine</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| | <p>approval and audit trails of activities. The requests are initiated by HR and are approved by the new employee's manager before being routed to the Corporate Real Estate group for provisioning. Final assignment of access is assigned by Corporate Security Management in compliance with the Corporate Security Clearance Matrix and Procedures.</p> <p>Access to the Pennsylvania data center as a facility is granted by Iron Mountain upon approval from TCH management.</p> | <p>whether access was granted based on approved requests.</p> <p>Inspected the list of users with administrator access to badge access system (C-Cure), job titles, and inquired of the management to determine whether administrative access to badge access system was restricted to authorized personnel.</p> | |
| CC6.4.3 | <p>Physical Access System Administration</p> <p>Administrative access to C-Cure is restricted to appropriate personnel.</p> | <p>Inspected a list of users with administrative rights to determine whether users rights were appropriate based on their job responsibilities.</p> | No exceptions noted. |
| CC6.4.4 | <p>Visitor/Vendor Access</p> <p>Visitors/vendors are required to present identification cards, sign in, wear a visitor's badge, and be escorted by a TCH employee to their destination.</p> <p>Visitor and vendor access controls for the Pennsylvania data center as a facility are managed and performed by Iron Mountain and are not in scope of this report.</p> | <p>Observed that visitors at the New York and North Carolina processing facilities and North Carolina data center presented identification cards, signed in, wore visitor's badges and were escorted by TCH employees.</p> <p>For a selection of dates, inspected visitor logs to determine visitors/vendors were required to sign in.</p> | No exceptions noted. |
| CC6.4.5 | <p>Access to Facilities</p> <p>The primary data center for EPN, CHIPS, and IXN is located in North Carolina and the secondary data center is located in Pennsylvania (which is managed and controlled by Iron Mountain). RTP runs "active-active" in the North Carolina and Pennsylvania data center.</p> <p>TCH has documented policies and procedures for physical access. Access to the New York Network Operations Center and processing facility, and North Carolina data center, Network Operations Center and processing facilities are controlled by a biometric access control system.</p> | <p>Inspected the Physical Security Policy manual to determine whether the policies and procedures for physical security were documented and maintained.</p> <p>Toured the North Carolina and New York processing facilities and North Carolina data center and observed the following:</p> <ul style="list-style-type: none"> • Access was controlled by multi zoned biometric access systems. • In the "man trap", the second entrance could not be opened if the first entrance was not closed. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|----------------------|
| | <p>Entrance to the facilities is controlled through two successive doorways and the corridor between these doors serves as a "man trap". Strategic locations such as the entrance to the computer and telecommunications room, are monitored by closed circuit television. A guard is on duty 24 hours a day and seven days a week and is required to tour the facility several times during each shift.</p> <p>The data center and telecommunication area in North Carolina is in separate access zones.</p> <p>Program documentation is maintained online and access to the documentation manuals is restricted to authorized individuals.</p> <p>Physical access lists and badge activity for the Pennsylvania data center are sent from Iron Mountain and reviewed on a monthly basis.</p> <p>Physical security controls for the Pennsylvania data center as a facility are managed and performed by Iron Mountain and are not in scope of this report.</p> | <ul style="list-style-type: none"> • The data center and telecommunication area at each facility were in separate access zones. • The security guards monitored the facilities through closed circuit televisions. • The security guards toured the facilities several times throughout the day. <p>For a selection of months, inspected physical access lists and badge activity sign off for the Pennsylvania data center to determine access was reviewed on a monthly basis.</p> | |
| CC6.4.6 | <p>Access Revocation and Adjustment - Physical</p> <p>Terminations and transfers are notified and processed through the Courion Tool.</p> <p>An automated access form using the Courion Tool is used for notifying the Identity and Access Management team and Corporate Real Estate of employee terminations and transfers. The tool provides for automatic notification and electronic approval and audit trails of activities. The physical control system retains date and time that access was removed or modified.</p> <p>Changes to existing access (that are not HR transfers) are approved by designated individuals based on access requested through email to Corporate Security Management.</p> | <p>For a selection of employee terminations from a list provided by HR, inspected the Courion notification and physical control system generated audit trails to determine whether access for terminated employees was removed from the system in a timely manner.</p> <p>Inspected a listing of transferred employees during the period and noted no transferred employees requiring a change in physical access; therefore, the operating effectiveness of this control for transfers could not be tested.</p> <p>For a selection of access modifications, inspected the email evidence to determine whether changes</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|--|--|--|----------------------|
| | Management sends requests to Iron Mountain to revoke access to the Pennsylvania data center as necessary. | <p>were requested and authorized and access was granted based on approved requests.</p> <p>Inspected the list of terminated users, and the active list of users with access to Facilities and data centers to determine whether terminated users had access to the facilities or data centers.</p> <p>Inspected the list of terminated users and Pennsylvania data center access listings and determined that there were no terminated users with access to the Pennsylvania data center during the period; therefore, the operating effectiveness of this control for the Pennsylvania data center could not be tested.</p> | |
| CC6.4.7 | <p>Periodic Access Review - Physical</p> <p>At a minimum an annual facilities access recertification process is performed by Corporate Real Estate. Access is reviewed by individual's managers. This recertification process includes all clearances identified by management which could affect production. General access is not included in this review. Any changes are documented in the Physical Security Access Profile Review and modifications performed as required.</p> | Inspected the periodic access review and user listings to determine whether physical access identified by management as affecting production was reviewed and any changes were documented and performed as required. | No exceptions noted. |
| Complementary User Entity Control(s) | | | |
| <p>Controls should be established at user entities so that:</p> <ul style="list-style-type: none"> • Users manage physical security at locations where TCH routers are located. • Physical access to routers at the user entity site is limited. | | | |

CC6.5 – The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity’s objectives.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|-----------------------------|
| CC6.5.1 | <p>Asset Disposal Policies and Procedures</p> <p>The Physical and Environmental Security Policy includes procedures relating to data-bearing assets and their disposal. All staff members are responsible for turning over data-bearing assets to Corporate Security for destruction. Corporate Security is responsible for disposing of, securing, and/or destroying data-bearing assets that will no longer be active in accordance with TCH’s asset classifications.</p> | <p>Inspected the Physical and Environmental Security policy and Data Bearing Asset Destruction procedural document to determine whether procedures for the disposal of data-bearing assets were established.</p> | <p>No exceptions noted.</p> |
| CC6.5.2 | <p>Discontinued System Components Inventory</p> <p>The Asset Management module within ServiceNow is used to manage asset information for IT Assets throughout its lifecycle from request to disposal. Obsolete hardware is physically secured and tracked until it is disposed of per documented data-bearing procedures. Service Catalog workflows in ServiceNow are used to support the procurement, receive and retirement of IT Assets. TCH also uses the Configuration Management Database (CMDB) in ServiceNow to manage configuration items throughout its lifecycle from operational to out of service.</p> | <p>Inspected the ServiceNow configuration to determine whether IT assets were managed from request to disposal.</p> <p>Inspected the ServiceNow discovery IP range list and discovery schedule list to determine whether IT servers and IT assets were tracked from operational use to out of service.</p> <p>For a selection of obsolete hardware requiring disposal, inspected associated ServiceNow tickets and ticket tasks to determine whether the asset was tracked through disposal as per documented data-bearing procedures.</p> | <p>No exceptions noted.</p> |

CC6.6 – The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|-------------------------------------|
| CC6.6.1 | <p>Security Configuration - Mainframe</p> <p>Access to the Unisys production environment and development environment is controlled by the Unisys MCP operating system and the Unisys InfoGuard access control package. MCP allows programs and users access only to defined computer resources. InfoGuard is a software package which provides logical security options beyond that provided by the MCP operating system. Hardening guidelines for the security configuration of the Unisys MCP operating systems are documented and implemented within the system.</p> <p>TCH has implemented the following security rules in the production environments per the Unisys MCP hardening standard:</p> <ul style="list-style-type: none"> • Employee individual accesscode and group usercode passwords must meet a minimum length requirement. • Employee individual accesscode and group usercode passwords must be changed at specified intervals. • Employee individual accesscode and group usercode passwords must be different from a certain number of passwords previously used (password history). • Employee individual usercodes (with and without accesscodes) are suspended after a specified number of violations per day. • Terminals are disabled after a number of invalid access attempts within certain duration of time. | <p>For a selection of mainframe servers, inspected the MCP/InfoGuard logical security options to determine whether they were configured based on TCH's Information Security policy and procedures.</p> <p>For a selection of mainframe servers, individual accesscodes, and group usercodes, inspected the accesscode and usercode parameters and the Unisys configuration to determine whether the security rules were setup according to TCH's requirements.</p> | <p>Exceptions noted, see below:</p> |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|---|---|--|------------------------------|
| Exceptions Noted: Individual accesscodes <ul style="list-style-type: none"> For 2 out of 120 individual accesscodes selected, the minimum password length was not set. For 25 of 120 individual accesscodes selected, the password was not set to expire. For 25 of 120 individual accesscodes selected, the password history was not set. For 116 of 120 individual accesscodes selected, the password lockout setting was set; however, it was not in accordance with TCH policy requirements. For 4 of 120 individual accesscodes selected, the password lockout setting was not set. Group usercodes <ul style="list-style-type: none"> For 1 of 40 group usercodes selected, the minimum password length was set; however, it was not in accordance with TCH policy requirements. For 13 of 40 group usercodes selected, the password was not set to expire. For 19 of 40 group usercodes selected, the password history was not set. For 39 of 40 group usercodes selected, the password lockout setting was set; however, it was not in accordance with TCH policy requirements. For 1 of 40 group usercodes selected, the password lockout setting was not set. | | | |
| CC6.6.2 | Security Rules - Distributed TCH has implemented the following security rules for the servers, applications and databases in the distributed environment: <ul style="list-style-type: none"> A user ID and password are required. Passwords must be changed at specified interval. Passwords must meet a minimum length requirement. New passwords must be different from a certain number of passwords previously used. User IDs are disabled after a number of invalid access attempts within certain duration of time. | For the production systems network domains, and for a selection of Windows servers, applications and databases in the distributed environment, inspected the password parameters to determine whether the security rules were setup in accordance with TCH's requirements. Observed a TCH employee log on to the TCH network and noted that a username and password are required. | Exceptions noted, see below: |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|---|---|--|----------------------|
| Exceptions Noted: Windows Databases: Noted that management had identified local database accounts where password rules were not enforced per TCH policy. Linux Servers: Password parameter settings for local server accounts were configured, however, not established in accordance with TCH policy; per TCH policy minimum password length required is 15 characters, however, configuration was set to 8 characters. | | | |
| CC6.6.3 | Security Administration and Security Violations ArcSight is used to support security administration including managing security violations for both mainframe and distributed environments. Security related activities such as user data change, file security attribute change and security violations including inappropriate user activity, unauthorized software, virus and firewall alerts are captured, logged and reported using ArcSight. ArcSight is configured to capture the defined security related activities and send an alert to the Information Security responsible personnel through the Information Security workstation and to their mobile phones when there is an event that meets the defined criteria such as possible security violation. Each alert is reviewed and triaged by the managed security service provider, Cipher, and followed up and cleared by Information Security, as necessary. On an ongoing basis, the Information Security responsible personnel reviews the alerts and other activities to determine that alerts were responded to appropriately. Alerts remain pending in ArcSight until they are resolved. | Inspected the configuration for alert event setup in ArcSight to determine whether ArcSight was setup to capture and log the security related events such as user data change, file security attribute change and security violation including inappropriate user activity, unauthorized software, IDS, virus and firewall alerts and sends automatic alerts to Cipher, and the Information Security Analyst when an event that met the defined condition occurred. Observed online ArcSight alert messages on the ArcSight workstation located in a secure area of the Information Security group and noted Information Security responded to the alert in ArcSight and that alert remained pending until it was resolved. For a selection of months, inspected a selected ArcSight violation report to determine whether the security violations were captured and retained in ArcSight. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|----------------------|
| CC6.6.4 | <p>Firewall Rules</p> <p>Firewalls are configured to allow only defined services into the TCH networks and firewall address translation is used to prevent the actual IP address from being disclosed to external parties.</p> | <p>For a selection of firewalls, inspected firewall rules to determine whether incoming traffic was restricted to specific logical communication ports and whether the rules were established to audit the incoming traffic and determine the source address.</p> <p>For a selection of firewalls, inspected the firewall configuration to determine whether address translation rules were applied to the transmissions to prevent the actual IP address from being disclosed to external parties.</p> | No exceptions noted. |
| CC6.6.5 | <p>Network Design</p> <p>The TCH networks are segregated from TCH's corporate network and are separate from other applications and include provisioning for redundancies.</p> <p>The EPN network design includes:</p> <ul style="list-style-type: none"> • Connect:Direct with Secure Plus, and MPLS; and • The internet using EPNAccess via the PSA VPN Appliance application security gateway or File Transfer Protocol (FTP-S). <p>The TCH CHIPS networks are segregated from TCH's corporate network and are separate from other applications and include provisioning for redundancies. The network design for each customer site includes an MPLS and ISDN backup connection. All connections are encrypted router to router using IPSec 256 AES.</p> <p>The IXN network is segregated from TCH's internal network and networks used for the other services. The IXN network design includes redundancy, routers and firewalls. Routers and firewalls are placed at various points of the network to provide security for data transmission.</p> | <p>Inspected network diagrams to determine whether the design of the TCH's EPN network was segregated from TCH's internal network and the networks for the other services and that network design included redundancy, routers, firewalls and an intrusion detection system.</p> <p>Inspected network diagrams to determine whether the design of the EPN network included Connect:Direct with Secure Plus, MPLS, EPNAccess with the VPN appliance and FTP-S.</p> <p>Inspected network diagrams to determine whether the design of the TCH's CHIPS network was segregated from TCH's internal network and networks for the other services and whether the network design included redundancy, routers, firewalls and an intrusion detection system.</p> <p>Inspected the IXN network diagrams to determine whether the design of the IXN network included an external network provided by third parties and TCH's IXN network which was segregated from TCH's internal network and networks used for the</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| | <p>External Network - IXN customers transmit payloads to receiving banks and transmit transmittal files to TCH over the private IXN network provided and managed by AT&T (FTP-S over the internet is available as a non-managed connectivity option). Two network hubs are maintained to provide redundancy between MPLS providers.</p> <p>The RTP network is segregated from TCH's corporate network and is separate from other applications and includes provisioning for redundancies. The RTP network design includes:</p> <ul style="list-style-type: none"> • MPLS; and • VPN network systems that provide a secure transport between TCH and its customers <p>Connect:Direct with Secure Plus is used to send reconciliation and standard reports and IBM MQ is used to send RTP messages, both methods are sent over the MPLS network or secure VPN. The endpoint routers between the customer site and TCH create an encrypted tunnel. The encryption between the customer router and the TCH data centers ensure all traffic between the sites is encrypted.</p> <p>Routers, firewalls and an intrusion detection system are used to provide network security. Router configurations include ACLs, NAT and IPSec to provide end to end network security.</p> | <p>other services and whether network design included redundancy, routers and firewalls.</p> <p>Inspected network diagrams to determine whether the design of the TCH's RTP network was segregated from TCH's corporate network and the networks for the other services and that network design included redundancy, routers, firewalls and an intrusion detection system.</p> <p>Inspected network diagrams to determine whether the design of the RTP network included MPLS, and VPN access.</p> <p>Please refer to CC6.1.16 Router Configuration for test results of router configurations.</p> <p>Please refer to CC8.1.15 Network Management Procedures for test results of network changes to TCH network.</p> | |
| CC6.6.6 | <p>Remote Access</p> <p>TCH's employees and contractors are granted access to the TCH network from remote locations to support operations. An approval from designated management is required for remote access.</p> <p>Remote access requires multi-factor authentication, controlled through VPN or VDI using network credentials and SecurID</p> | <p>For a selection of employees and contractors from the RSA SecurID token report inquired of Information Security Director regarding their job responsibilities to determine whether they were current employees and contractors and required remote access to carry out their job responsibilities.</p> <p>Compared the list of employees with access to RSA tokens against a list of terminated users to</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| | tokens. Controls related to new remote access requests are described in CC6.3.2. | <p>determine whether any terminated users had retained access to RSA tokens.</p> <p>Please refer to CC6.3.2 Access Authorization - SecurID for test results of approval of new remote access requests.</p> <p>Observed a TCH employee access TCH's network via remote access via VPN and VDI, and noted that a password and SecurID were required.</p> | |
| CC6.6.7 | <p>Encryption – MPLS and Connect:Direct with Secure Plus (EPN)</p> <p>EPN messages transmitted via Connect:Direct with Secure Plus are encrypted to protect the messages from alteration of data while in transit.</p> <p>In addition, transmissions over the MPLS network are encrypted using router configurations which use IP Security (IPSec) policy and an AES 256 encryption algorithm.</p> | <p>For a selection of customers using Connect:Direct with Secure Plus, inspected the node configurations to determine whether the data transmissions between customer and EPN were encrypted.</p> <p>For a selection of MPLS customers, inspected router configurations to determine whether the data transmissions used IPSec and were AES 256 encrypted.</p> | No exceptions noted. |
| CC6.6.8 | <p>Encryption – EPNAccess</p> <p>Customers use EPNAccess, a web based front-end system to transmit files to TCH. Access to EPNAccess requires a SecurID token, a valid ABA transit/routing number and associated password for file transmissions.</p> <p>EPNAccess utilizes a PSA VPN Appliance to provide security through the internet. The PSA integrates standards-based security and session encryption support is based on TLS. All files transmitted to and from EPN utilize encrypted links to ensure that the files are sent from an authorized source and are not altered or visible during transmission.</p> | <p>Inspected the EPNAccess logon screen to determine whether EPNAccess required a Secure ID token, a valid user ID or ABA transit/routing number and associated password.</p> <p>Inspected the EPNAccess logon screen and PSA VPN Appliance configuration to determine whether EPNAccess transmissions were encrypted using TLS protocol.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|----------------------|
| CC6.6.9 | <p>Encryption – FTP-S (EPN)</p> <p>FTP-S transmissions are routed through firewalls that allow only authorized customers to send and receive files based on IP address. Data transmissions via the internet are validated for authorized sending points by firewalls. All customer connectivity to the FTP-S system is controlled by allowing only customer host IP address and required port numbers. The EPN FTP-S transmissions are secured using TLS and PGP encryption. PGP encrypts and digitally signs files before sending them via the internet. EPN generates a pair of keys – a public key and a private key. TCH sends the public key to the EPN FTP-S customer. The customers are required to import the public key into its key files. The customer follows a required process to generate the public key and private key. New FTP-S customers are required to complete an FTP-S New Client Data Sheet with bank information and FTP-S transmission details.</p> | <p>For a selection of customer using FTP-S, inspected system generated connection log and configuration to determine whether the transmissions via FTP-S were encrypted using PGP and TLS encryption.</p> <p>Inspected firewall rules on a selection of firewalls to determine whether incoming traffic was restricted to specific number of logical communication and whether the rules were established to audit the incoming traffic and determine the source address.</p> <p>For a selection of new FTP-S customers, inspected the Client Data Sheet and connection log details to determine whether the Client Data Sheet was completed for new FTP connections and EPN/FTP-S transmissions were encrypted using PGP encryption.</p> <p>Refer to CC6.1.17 Firewall Rules for testing over Firewall Rules.</p> | No exceptions noted. |
| CC6.6.10 | <p>Data Encryption – Connect:Direct with Secure Plus and FTP-S (IXN)</p> <p>IXN messages transmitted via Connect:Direct with Secure Plus are encrypted to protect the messages from alteration of data while in transit.</p> <p>FTP-S transmissions are routed through firewalls that allow only authorized customers to send and receive files based on IP address. Data transmissions via the internet are validated for authorized sending points by firewalls. All customer connectivity to the FTP-S system is controlled by allowing only customer host IP address and required port numbers. The IXN FTP-S transmissions are secured using TLS and PGP encryption. PGP encrypts and digitally signs files before sending them via the internet using a pair of keys – a public key and a private key.</p> | <p>For a selection of customers using Connect:Direct with Secure Plus, inspected the node configuration to determine data transmissions between customer and IXN were encrypted.</p> <p>For a selection of customer using FTP-S, inspected system generated connection log and configuration to determine whether the transmissions via FTP-S were encrypted using PGP encryption and TLS.</p> <p>Inspected the system generated list of new IXN customers and noted there were no new FTP installs for new customers during the period; therefore, the operating effectiveness of this control for new client FTP installs could not be tested.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| | | Refer to CC6.1.17 Firewall Rules for testing over Firewall Rules. | |
| CC6.6.11 | <p>Encryption – MPLS and IBM MQ (CHIPS and RTP)</p> <p>CHIPS messages utilize IBM MQ and are encrypted using TLS protocol, and digital certificate for authentication. All RTP messages are encrypted twice during transmission – at the router level using AES 256 encryption and between the customers’ MQ managers and the TCH MQ managers using IBM MQ. IBM MQ encrypts RTP messages using TLS 1.2 protocol. The sending customer’s user ID is verified through standard MQ channel initiation procedures with x509 public certificates. MQCHLAUTH records validate at runtime for each MQ channel to ensure a match otherwise the connection is rejected. In addition, RTP messages are digitally signed to ensure they have not been altered during transmission.</p> <p>Transmissions over the MPLS network are encrypted using router configurations which use IP Security (IPSec) policy and an AES 256 encryption algorithm.</p> | <p>For a selection of CHIPS customers, inspected IBM MQ TLS configuration to determine whether CHIPS messages were encrypted using TLS, digital certificate and channel verifications was enabled.</p> <p>For a selection of RTP customers, inspected IBM MQ TLS configuration and selected channel log to determine whether RTP messages were encrypted using TLS, and channel verifications was enabled.</p> <p>For a selection of MPLS customers, inspected router configurations to determine whether the transmissions used IPSec and were AES 256 encrypted.</p> <p>For a selection of routers, inspected router configurations to determine whether the transmissions used IPSec and were AES 256 encrypted.</p> <p>Please refer to CC6.1.35 RTP Messages and Authentication for results of testing digitally signed messages.</p> | No exceptions noted. |
| CC6.6.12 | <p>Encryption - Connect:Direct with Secure Plus (RTP)</p> <p>Clients may elect to receive standard reconciliation reports via Connect:Direct with Secure Plus which uses Transport Layer Security (TLS) providing a secure layer on top of TCP/IP over the MPLS network or secure VPN.</p> <p>In addition, transmissions over the MPLS network are encrypted via router configurations which use IP Security (IPsec) and an AES 256 encryption algorithm.</p> | <p>For a selection of nodes using Connect:Direct with Secure Plus, inspected the node configurations to determine whether the data transmissions between customer and RTP were encrypted.</p> <p>For a selection of MPLS routers, inspected router configurations to determine whether the data transmissions used IPSec and were AES 256 encrypted.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC6.6.13 | <p>Encryption – RTP Management Console</p> <p>The RTP Management Console is accessed through a third-party application security gateway, a PSA VPN Appliance, to enhance the security through the Internet. Access through the PSA is controlled through a series of authentications including RSA SecurID tokens, user groups and ACLs. The PSA provides extended secure access to corporate application resources to authorized users via standard web browsers. The PSA integrates standards-based security and session encryption is based on TLS.</p> | <p>Inspected the RTP Management Console logon screen to determine whether it was accessed via the PSA VPN appliance, and required a Secure ID token, a valid user ID and associated password.</p> <p>Inspected the PSA VPN Appliance configuration to determine whether RTP Management Console transmissions were encrypted using TLS protocol.</p> | No exceptions noted. |
| CC6.6.14 | <p>Intrusion Detection System</p> <p>The TCH networks include an Intrusion Detection System (IDS), CarbonBlack. This system detects and classifies suspicious events according to a library of signatures provide by the vendor. The IDS/IPS is programmed to send alerts when thresholds for particular attack signatures are exceeded. Information Security management are alerted of intrusion activities. Incidents noted are recorded in ArcSight and depending on the nature and type of problem, the incident is escalated to the designated group for follow-up and resolution. If necessary, corrective action is taken via updates to policies and/or the change management process due to the alerts.</p> <p>CarbonBlack is configured to generate alerts through ArcSight.</p> <p>Controls related incidents analysis and resolution are documented in CC7.4.4 Security Administration and Security Violations.</p> | <p>For a selection of servers, inspected the CarbonBlack management console to determine whether CarbonBlack was configured to monitor traffic.</p> <p>For a selection of incidents, inspected tickets and supporting documentation to determine whether the incident was escalated and resolved.</p> <p>Inspected configured threat intelligence library in CarbonBlack to determine whether the system was configured to detect and classify events according to the signatures.</p> <p>Inspected ArcSight management console to determine whether ArcSight was configured to alert Information Security in case of potential threats.</p> <p>Inspected the list of users with administrator access to CarbonBlack, job titles, and inquired of the management to determine whether administrative access to CarbonBlack was restricted to authorized personnel.</p> <p>Inquired of Information Security management regarding policy and process updates and were informed corrective action was taken via updates to</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|--|---|---|----------------------|
| | | <p>policies and/or the change management process due to the alerts.</p> <p>Refer to CC7.4.4 Security Administration and Security Violations for test results of incident analysis and resolution for ArcSight.</p> | |
| CC6.6.15 | <p>Server Hardening</p> <p>TCH provides hardening standards for system administrators in order to implement secure server configurations within the company's infrastructure. The guidelines are reviewed and updated when changes occur by the Information Security team.</p> <p>Monthly validation of compliance to hardening standards occurs through the use of BigFix. Weekly meetings are held to discuss compliance results, and if necessary, tickets are created for remediation or a policy exception is documented in Archer.</p> | <p>Inspected the hardening guidelines to determine whether they document approved hardening standards for server configurations.</p> <p>For a selection of months, inspected monthly compliance report to determine whether compliance checks were performed to ensure devices were hardened per defined standards.</p> <p>For a selection of weeks, inspected the compliance meeting invite and notes to determine whether compliance results were discussed, and if necessary, tickets were created for remediation of any noted issues or a policy exception was documented in Archer.</p> | No exceptions noted. |
| Complementary User Entity Control(s) | | | |
| <p>Controls should be established at user entities so that:</p> <ul style="list-style-type: none"> • Users manage security for their Connect:Direct with Secure Plus software for encryption used for transmissions. • Users send acknowledgement of receipt of the Privacy-Enhanced Mail (PEM) to TCH. • Users store the Privacy-Enhanced Mail (PEM) containing public keys in a secure location and provide the public keys to TCH. | | | |

CC6.7 – The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity’s objectives.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC6.7.1 | Removable Media Policies TCH has policies that document requirements on removable information and assets. The policies are reviewed and updated annually by the Information Security leadership team in accordance with the Information Security policies. | Inspected the following policy documents to determine whether they documented requirements on removable information and assets and the policy documents were updated and reviewed annually by TCH leadership. <ul style="list-style-type: none"> Asset Classification and Management Policy Physical and Environment Security Policy | No exceptions noted. |
| CC6.7.2 | Laptop and Mobile Device Encryption TCH laptops have hard drive encryption technology installed and activated. By default, Universal Serial Bus (USB) access is set to read only. TCH mobile devices used to access emails are encrypted. | Inspected the global encryption configuration to determine whether encryption mechanisms were enforced. Inspected the USB group policy to determine whether USB ports are globally set to read-only. For a selection of employees, inspected mobile device encryption settings to determine whether mobile devices were encrypted. | No exceptions noted. |
| CC6.7.3 | Data Loss Prevention Detecting and preventing data exfiltration, potential DLP events will normally be identified by a toolset based on specific criteria and classes of criteria that have been selected and designated to identify details surrounding data at rest and in transit. TCH automatically detects data meeting patterns, potentially classified as: <ul style="list-style-type: none"> TCH Restricted or TCH Confidential Data potentially containing PII, PCI, Source Code, or Intellectual Property Data potentially containing combinations of these – i.e. (PII plus PCI) or PII plus TCH Restricted. | Inspected the DLP program policies and procedures, Forcepoint and Arcsight configurations to determine that DLP procedures were established and tools configured so that DLP is identified to detect and prevent data exfiltration. For a selection of incidents, inspected tickets and supporting documentation to determine whether the incident was escalated and resolved. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| | TCH will also use pattern criteria designed to discover these data types potentially related to FFIEC, GLBA, PCI and other regulations, contractual agreements or pre-defined data patterns. | | |
| CC6.7.4 | <p>Encryption – MPLS and Connect:Direct with Secure Plus (EPN)</p> <p>EPN messages transmitted via Connect:Direct with Secure Plus are encrypted to protect the messages from alteration of data while in transit.</p> <p>In addition, transmissions over the MPLS network are encrypted using router configurations which use IP Security (IPSec) policy and an AES 256 encryption algorithm.</p> | <p>For a selection of customers using Connect:Direct with Secure Plus, inspected the node configurations to determine whether the data transmissions between customer and EPN were encrypted.</p> <p>For a selection of MPLS customers, inspected router configurations to determine whether the data transmissions used IPSec and were AES 256 encrypted.</p> | No exceptions noted. |
| CC6.7.5 | <p>Encryption – EPNAccess</p> <p>Customers use EPNAccess, a web based front-end system to transmit files to TCH. Access to EPNAccess requires a SecurID token, a valid ABA transit/routing number and associated password for file transmissions.</p> <p>EPNAccess utilizes a PSA VPN Appliance to provide security through the internet. The PSA integrates standards-based security and session encryption support is based on TLS. All files transmitted to and from EPN utilize encrypted links to ensure that the files are sent from an authorized source and are not altered or visible during transmission.</p> | <p>Inspected the EPNAccess logon screen to determine whether EPNAccess required a Secure ID token, a valid user ID or ABA transit/routing number and associated password.</p> <p>Inspected the EPNAccess logon screen and PSA VPN Appliance configuration to determine whether EPNAccess transmissions were encrypted using TLS protocol.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|----------------------|
| CC6.7.6 | <p>Encryption – FTP-S (EPN)</p> <p>FTP-S transmissions are routed through firewalls that allow only authorized customers to send and receive files based on IP address. Data transmissions via the internet are validated for authorized sending points by firewalls. All customer connectivity to the FTP-S system is controlled by allowing only customer host IP address and required port numbers. The EPN FTP-S transmissions are secured using TLS and PGP encryption. PGP encrypts and digitally signs files before sending them via the internet. EPN generates a pair of keys – a public key and a private key. TCH sends the public key to the EPN FTP-S customer. The customers are required to import the public key into its key files. The customer follows a required process to generate the public key and private key. New FTP-S customers are required to complete an FTP-S New Client Data Sheet with bank information and FTP-S transmission details.</p> | <p>For a selection of customer using FTP-S, inspected system generated connection log and configuration to determine whether the transmissions via FTP-S were encrypted using PGP and TLS encryption.</p> <p>Inspected firewall rules on a selection of firewalls to determine whether incoming traffic was restricted to specific number of logical communication and whether the rules were established to audit the incoming traffic and determine the source address.</p> <p>For a selection of new FTP-S customers, inspected the Client Data Sheet and connection log details to determine whether the Client Data Sheet was completed for new FTP connections and EPN/FTP-S transmissions were encrypted using PGP encryption.</p> <p>Refer to CC6.1.17 Firewall Rules for testing over Firewall Rules.</p> | No exceptions noted. |
| CC6.7.7 | <p>Data Encryption – Connect:Direct with Secure Plus and FTP-S (IXN)</p> <p>IXN messages transmitted via Connect:Direct with Secure Plus are encrypted to protect the messages from alteration of data while in transit.</p> <p>FTP-S transmissions are routed through firewalls that allow only authorized customers to send and receive files based on IP address. Data transmissions via the internet are validated for authorized sending points by firewalls. All customer connectivity to the FTP-S system is controlled by allowing only customer host IP address and required port numbers. The IXN FTP-S transmissions are secured using TLS and PGP encryption. PGP encrypts and digitally signs files before sending them via the internet using a pair of keys – a public key and a private key.</p> | <p>For a selection of customers using Connect:Direct with Secure Plus, inspected the node configuration to determine data transmissions between customer and IXN were encrypted.</p> <p>For a selection of customer using FTP-S, inspected system generated connection log and configuration to determine whether the transmissions via FTP-S were encrypted using PGP encryption and TLS.</p> <p>Inspected the system generated list of new IXN customers and noted there were no new FTP installs for new customers during the period; therefore, the operating effectiveness of this control for new client FTP installs could not be tested.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| | | Refer to CC6.1.17 Firewall Rules for testing over Firewall Rules. | |
| CC6.7.8 | <p>Encryption – MPLS and IBM MQ (CHIPS and RTP)</p> <p>CHIPS messages utilize IBM MQ and are encrypted using TLS protocol, and digital certificate for authentication. All RTP messages are encrypted twice during transmission – at the router level using AES 256 encryption and between the customers' MQ managers and the TCH MQ managers using IBM MQ. IBM MQ encrypts RTP messages using TLS 1.2 protocol. The sending customer's user ID is verified through standard MQ channel initiation procedures with x509 public certificates. MQCHLAUTH records validate at runtime for each MQ channel to ensure a match otherwise the connection is rejected. In addition, RTP messages are digitally signed to ensure they have not been altered during transmission.</p> <p>Transmissions over the MPLS network are encrypted using router configurations which use IP Security (IPSec) policy and an AES 256 encryption algorithm.</p> | <p>For a selection of CHIPS customers, inspected IBM MQ TLS configuration to determine whether CHIPS messages were encrypted using TLS, digital certificate and channel verifications was enabled.</p> <p>For a selection of RTP customers, inspected IBM MQ TLS configuration and selected channel log to determine whether RTP messages were encrypted using TLS, and channel verifications was enabled.</p> <p>For a selection of MPLS customers, inspected router configurations to determine whether the transmissions used IPSec and were AES 256 encrypted.</p> <p>For a selection of routers, inspected router configurations to determine whether the transmissions used IPSec and were AES 256 encrypted.</p> <p>Please refer to CC6.1.35 RTP Messages and Authentication for results of testing digitally signed messages.</p> | No exceptions noted. |
| CC6.7.9 | <p>Encryption – RTP Management Console</p> <p>The RTP Management Console is accessed through a third-party application security gateway, a PSA VPN Appliance, to enhance the security through the Internet. Access through the PSA is controlled through a series of authentications including RSA SecurID tokens, user groups and ACLs. The PSA provides extended secure access to corporate application resources to authorized users via standard web browsers. The PSA integrates standards-based security and session encryption is based on TLS.</p> | <p>Inspected the RTP Management Console logon screen to determine whether it was accessed via the PSA VPN appliance, and required a Secure ID token, a valid user ID and associated password.</p> <p>Inspected the PSA VPN Appliance configuration to determine whether RTP Management Console transmissions were encrypted using TLS protocol.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|----------------------|
| CC6.7.10 | <p>Encryption - Connect:Direct with Secure Plus (RTP)</p> <p>Clients may elect to receive standard reconciliation reports via Connect:Direct with Secure Plus which uses Transport Layer Security (TLS) providing a secure layer on top of TCP/IP over the MPLS network or secure VPN.</p> <p>In addition, transmissions over the MPLS network are encrypted via router configurations which use IP Security (IPsec) and an AES 256 encryption algorithm.</p> | <p>For a selection of nodes using Connect:Direct with Secure Plus, inspected the node configurations to determine whether the data transmissions between customer and RTP were encrypted.</p> <p>For a selection of MPLS routers, inspected router configurations to determine whether the data transmissions used IPsec and were AES 256 encrypted.</p> | No exceptions noted. |
| CC6.7.11 | <p>Output File Distribution (EPN)</p> <p>When output files are available, customers can login to EPNAccess or via Connect:Direct with Secure Plus, or FTP S to initiate a transmission job to receive their files from the EPN system.</p> <p>Customers use EPNAccess, a web based front-end system to transmit files to TCH. Access to EPNAccess requires a SecurID token, a valid ABA transit/routing number and associated password for file transmissions.</p> <p>EPNAccess utilizes a PSA VPN Appliance to provide security through the internet. The PSA integrates standards-based security and session encryption support is based on TLS. All files transmitted to and from EPN utilize encrypted links to ensure that the files are sent from an authorized source and are not altered or visible during transmission.</p> | <p>Inspected the EPNAccess logon screen to determine whether EPNAccess required a Secure ID token, a valid user ID or ABA transit/routing number and associated password.</p> <p>Inspected the EPNAccess logon screen and PSA VPN Appliance configuration to determine whether EPNAccess transmissions were encrypted using TLS protocol.</p> | No exceptions noted. |
| CC6.7.12 | <p>Report Distribution (CHIPS)</p> <p>Reports are electronically distributed to customers online. CHIPS provides a web-based management tool (CHIPSWeb) for customers to manage CHIPS activity through the internet using a secure connection. Customers can view CHIPS reports via this tool. Customer access to online reports is controlled through physical telecommunications connections</p> | <p>Inspected the CHIPSWeb logon screen and PSA VPN Appliance configuration to determine whether CHIPSWeb transmissions were encrypted using TLS protocol.</p> <p>For a selection of customers, inspected requests for secure token to determine whether issuances of the secure tokens were documented and approved.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| | <p>and authentication procedures to transmit data to a customer's system.</p> <p>Customers access CHIPSWeb through a secure VPN using TLS authentication. CHIPSWeb utilizes a PSA VPN Appliance to provide security through the internet. The PSA integrates standards-based security and session encryption support is based on TLS. A secure token is used for multi-factor authentication for accessing the VPN. A customer accessing VPN requires a secure token key, unique username and PIN which is issued by the Identity and Access Management department. Logical controls for the web servers are described in Control Objective 4. Data transmission controls are described in Control Objective 6.</p> <p>Customers must request, in writing, secure tokens from Client Service and the Identity and Access Management department. This department is responsible for distributing the secure key tokens and PINs to the customer.</p> | Observed TCH management access the CHIPSWeb and noted that a user ID, secure token key and PIN were required to gain access to the tool. | |
| CC6.7.13 | <p>Output Report Files Distribution (IXN)</p> <p>Upon completion of processing, IXN and TCH Mainframe Settlement system are updated real time. Output report files are made available online and retrieved by customers through SVPCOView. Access to SVPCOView requires user IDs and SecurID tokens assigned to each participant.</p> | Observed a Payments Specialist Representative logon to SVPCOView and noted that user ID, PIN and SecurID token key were required and that output report files were available online to be retrieved by customers through SVPCOView. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|--|---|---|----------------------|
| CC6.7.14 | <p>RTP Report Distribution</p> <p>Standard reports are electronically distributed to customers at their request. RTP provides an Internet/web-based management portal (RTP Management Console) for customers to view RTP activity, download reports, and make other configuration changes through the Internet using a secure connection. Customers can view RTP reports via this portal. Customers access the web-based application using a secure token, username and password.</p> <p>Additionally, participants may have reports securely transmitted to them using Connect:Direct with Secure Plus.</p> | <p>Observed the RTP Management Console and noted RTP reports were available for customers.</p> <p>For a selection of participants who opted for reports via Connect:Direct with Secure Plus, inspected configuration to determine whether reports were distributed via Connect:Direct with Secure Plus.</p> <p>Inspected the RTP Management Console logon screen to determine whether it was accessed via the PSA VPN appliance, and required a Secure ID token, a valid user ID and associated password.</p> | No exceptions noted. |
| Complementary User Entity Control(s) | | | |
| <p>Controls should be established at user entities so that:</p> <ul style="list-style-type: none"> • Users manage security for their Connect:Direct with Secure Plus software for encryption used for transmissions. • Users send acknowledgement of receipt of the Privacy-Enhanced Mail (PEM) to TCH. • Users store the Privacy-Enhanced Mail (PEM) containing public keys in a secure location and provide the public keys to TCH. • Only properly authorized users have access to terminals or other equipment used for transaction entry, and control procedures over the use of FTP-S user code and password and EPNAccess PIN are in place. | | | |

CC6.8 – The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity’s objectives.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| CC6.8.1 | <p>Systems Acquisition, Development and Maintenance Policy</p> <p>TCH has an Information Systems Acquisition, Development, and Maintenance policy that requires for detection of unauthorized hardware and software to be logged as an incident and subject to the incident response procedures. Such hardware and software will be promptly removed from the TCH environment. The policy is reviewed and updated annually by the Information Security leadership team in accordance with the Information Security policies.</p> <p>Controls related to problems reporting and tracking within ServiceNow are described in CC7.4.3.</p> | <p>Inspected the Information Systems Acquisition, Development, and Maintenance policy to determine whether it documented requirements for detection of unauthorized hardware and software to be logged as an incident and subject to the incident response procedures and was updated and reviewed annually by the Information Security leadership team.</p> <p>Refer to CC7.4.3 Problems Reporting and Tracking for test results of problems reporting and tracking within ServiceNow.</p> | No exceptions noted. |
| CC6.8.2 | <p>Security Administration and Security Violations</p> <p>ArcSight is used to support security administration including managing security violations for both mainframe and distributed environments. Security related activities such as user data change, file security attribute change and security violations including inappropriate user activity, unauthorized software, virus and firewall alerts are captured, logged and reported using ArcSight. ArcSight is configured to capture the defined security related activities and send an alert to the Information Security responsible personnel through the Information Security workstation and to their mobile phones when there is an event that meets the defined criteria such as possible security violation. Each alert is reviewed and triaged by the managed security service provider, Cipher, and followed up and cleared by Information Security, as necessary. On an ongoing basis, the Information Security responsible personnel reviews the alerts and other activities</p> | <p>Inspected the configuration for alert event setup in ArcSight to determine whether ArcSight was setup to capture and log the security related events such as user data change, file security attribute change and security violation including inappropriate user activity, unauthorized software, IDS, virus and firewall alerts and sends automatic alerts to Cipher, and the Information Security Analyst when an event that met the defined condition occurred.</p> <p>Observed online ArcSight alert messages on the ArcSight workstation located in a secure area of the Information Security group and noted Information Security responded to the alert in ArcSight and that alert remained pending until it was resolved.</p> <p>For a selection of months, inspected a selected ArcSight violation report to determine whether the</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| | to determine that alerts were responded to appropriately. Alerts remain pending in ArcSight until they are resolved. | security violations were captured and retained in ArcSight | |
| CC6.8.3 | <p>Virus and Unauthorized Software Monitoring</p> <p>TCH utilizes Symantec Endpoint Protection to protect against viruses, malware, malicious code and unauthorized software. Virus definitions are kept current and infected files are quarantined. Security alerts are logged, reported and analyzed via ArcSight.</p> <p>Controls related security alerts being logged, reported and analyzed are described in CC7.4.4 Security Administration and Security Violations.</p> | <p>Inspected the TCH Incident Response Plan to determine whether procedures regarding virus definitions being kept current and infected file quarantine were documented.</p> <p>Inspected the Symantec Endpoint Protection Manager configuration to determine whether TCH workstations were protected and virus definitions were updated on a recurring basis.</p> <p>For a selection of servers, inspected the Symantec Endpoint Protection Manager configuration to determine whether TCH servers were protected.</p> <p>Observed ArcSight and noted security alerts from Symantec Endpoint Protection were configured to be logged via ArcSight.</p> | No exceptions noted. |
| CC6.8.4 | <p>Software Control File/Checkfiles - Mainframe</p> <p>Program, system software names and parameters used in processing and their corresponding compilation/creation dates are maintained in a Software Control File (Control File). The Control Files are used to check the integrity of the programs used in the production processing.</p> <p>The Checkfiles program, an internally developed program, is automatically executed periodically throughout the day based on schedules to compare the names of production programs, system software and parameters and their compilation and creation dates of the program with the information maintained in the Control File. An alert message for a mismatch condition is sent to the Computer Operator console. The shift computer operator follows up and resolves the mismatched condition. The alert message for a mismatch condition is displayed on</p> | <p>For a selection of servers, inspected the Checkfiles schedule configuration of the workflow programs for Checkfiles processing, selected job log and selected Checkfiles report to determine whether the Checkfiles program was automatically processed based on schedules to check that approved versions of production programs and parameter files were used in production processing.</p> <p>Inspected the results of Checkfiles processing and noted that an alert message for a mismatch condition was displayed on the Computer Operator console until it was resolved.</p> <p>Please refer to CC6.3.1 Access Authorization – Logical Access for test results related to granting access to Checkfiles.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|-----------------------------|
| | <p>the Computer Operator console until the mismatch is resolved.</p> <p>After completion of Checkfiles processing, the Checkfiles program generates a report that is displayed on the console and is made available to the Network Operations Center Management. Controls related to granting access to Checkfiles are described in CC6.3.1.</p> | | |
| CC6.8.5 | <p>Access to Migrate to Production</p> <p>Authorized individuals migrate application changes to production upon receipt of a ServiceNow ticket approved by the Change Advisory Board. Access is restricted based on job responsibilities.</p> <p>Controls related to change management authorization are described in CC8.1.3 Application, Program and Configuration Change Request Initiation and Authorization.</p> | <p>Inspected the listing of users with access to implement changes to determine whether users were granted access based on their job responsibilities.</p> | <p>No exceptions noted.</p> |

CC 7.0 – Common criteria related to system operations

CC7.1 – To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC7.1.1 | <p>Server Hardening</p> <p>TCH provides hardening standards for system administrators in order to implement secure server configurations within the company's infrastructure. The guidelines are reviewed and updated when changes occur by the Information Security team.</p> <p>Monthly validation of compliance to hardening standards occurs through the use of BigFix. Weekly meetings are held to discuss compliance results, and if necessary, tickets are created for remediation or a policy exception is documented in Archer.</p> | <p>Inspected the hardening guidelines to determine whether they document approved hardening standards for server configurations.</p> <p>For a selection of months, inspected monthly compliance report to determine whether compliance checks were performed to ensure devices were hardened per defined standards.</p> <p>For a selection of weeks, inspected the compliance meeting invite and notes to determine whether compliance results were discussed, and if necessary, tickets were created for remediation of any noted issues or a policy exception was documented in Archer.</p> | No exceptions noted. |
| CC7.1.2 | <p>Vulnerability Third-party Notifications</p> <p>The TCH Vulnerability Management procedures include the following:</p> <p>Third-party software inspection and vulnerability management systems are used to notify TCH system administrators of the discovery of new vulnerabilities and availability of patches. Third-party and industry groups (e.g., FS-ISAC & US-CERT) broadcast notifications of new vulnerabilities on a periodic and ad-hoc basis. Notifications are actioned upon as needed by IS personnel for applicability to the current TCH environment.</p> | <p>Inspected the TCH Vulnerability Management procedures document to determine whether it included procedures to notify TCH system administrators of the discovery of new vulnerabilities and availability of patches.</p> <p>Inspected a selection of vendor notifications to determine whether TCH received third-party notifications of new vulnerabilities</p> <p>For a selection of vendor notifications, inspected documentation to determine whether corrective action was taken as needed by IS personnel.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC7.1.3 | <p>Security Administration and Security Violations</p> <p>ArcSight is used to support security administration including managing security violations for both mainframe and distributed environments. Security related activities such as user data change, file security attribute change and security violations including inappropriate user activity, unauthorized software, virus and firewall alerts are captured, logged and reported using ArcSight. ArcSight is configured to capture the defined security related activities and send an alert to the Information Security responsible personnel through the Information Security workstation and to their mobile phones when there is an event that meets the defined criteria such as possible security violation. Each alert is reviewed and triaged by the managed security service provider, Cipher, and followed up and cleared by Information Security, as necessary. On an ongoing basis, the Information Security responsible personnel reviews the alerts and other activities to determine that alerts were responded to appropriately. Alerts remain pending in ArcSight until they are resolved.</p> | <p>Inspected the configuration for alert event setup in ArcSight to determine whether ArcSight was setup to capture and log the security related events such as user data change, file security attribute change and security violation including inappropriate user activity, unauthorized software, IDS, virus and firewall alerts and sends automatic alerts to Cipher, and the Information Security Analyst when an event that met the defined condition occurred.</p> <p>Observed online ArcSight alert messages on the ArcSight workstation located in a secure area of the Information Security group and noted Information Security responded to the alert in ArcSight and that alert remained pending until it was resolved.</p> <p>For a selection of months, inspected a selected ArcSight violation report to determine whether the security violations were captured and retained in ArcSight.</p> | No exceptions noted. |
| CC7.1.4 | <p>Vulnerability Scans</p> <p>Weekly vulnerability scans over the network and servers are completed to identify any potential security threats that would impair system security and availability. Risks are then analyzed and appropriate corrective action is taken to address the security and availability risks identified through weekly vulnerability meetings. If necessary, the change management process is initiated as a result of any findings.</p> | <p>For a selection of weeks, inspected vulnerability scans and meeting invites and meeting minutes to determine whether the scans were completed, potential security and availability threats were identified, risks were analyzed and mitigation strategies were developed.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| CC7.1.5 | <p>External Network Risk Assessment</p> <p>On an annual basis, assessments of external network risks are performed to identify potential impairments that could impact system security and availability. Critical, High and Medium findings are entered into Archer for tracking where a criticality based on severity and likelihood as well as a remediation plan is documented. Findings are remediated based on assigned criticality and may be remediated via the change management process as applicable.</p> <p>Controls related to entering, tracking and remediating findings within Archer are documented in CC3.2.1 Assessing Risk.</p> | Inspected the third-party external risk assessment summaries and Archer findings to determine whether identified vulnerabilities were remediated based on criticality. | No exceptions noted. |
| CC7.1.6 | <p>Software Control File/Checkfiles - Mainframe</p> <p>Program, system software names and parameters used in processing and their corresponding compilation/creation dates are maintained in a Software Control File (Control File). The Control Files are used to check the integrity of the programs used in the production processing.</p> <p>The Checkfiles program, an internally developed program, is automatically executed periodically throughout the day based on schedules to compare the names of production programs, system software and parameters and their compilation and creation dates of the program with the information maintained in the Control File. An alert message for a mismatch condition is sent to the Computer Operator console. The shift computer operator follows up and resolves the mismatched condition. The alert message for a mismatch condition is displayed on the Computer Operator console until the mismatch is resolved.</p> <p>After completion of Checkfiles processing, the Checkfiles program generates a report that is displayed on the console and is made available to the Network Operations Center</p> | <p>For a selection of servers, inspected the Checkfiles schedule configuration of the workflow programs for Checkfiles processing, selected job log and selected Checkfiles report to determine whether the Checkfiles program was automatically processed based on schedules to check that approved versions of production programs and parameter files were used in production processing.</p> <p>Inspected the results of Checkfiles processing and noted that an alert message for a mismatch condition was displayed on the Computer Operator console until it was resolved.</p> <p>Please refer to CC6.3.1 Access Authorization – Logical Access for test results related to granting access to Checkfiles.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|----------------------|
| | Management. Controls related to granting access to Checkfiles are described in CC6.3.1. | | |
| CC7.1.7 | <p>System Components Inventory</p> <p>ServiceNow is used to provide a single system of record for system components and supports management of IT Asset and Configuration Items. The Asset Management module within ServiceNow is used to manage asset information for IT Assets throughout its lifecycle from request to disposal and aids in determining criticality of the asset. Service Catalog workflows in ServiceNow are used to support the procurement, receive and retirement of IT Assets. TCH also uses the Configuration Management Database (CMDB) in ServiceNow to manage configuration items throughout its lifecycle from operational to out of service. Maintaining the Asset Management module allows an inventory of assets which is used in threat management. To keep configuration items up to date in the CMDB, ServiceNow Discovery is used to automate CI population into the CMDB. ServiceNow Discovery uses conventional techniques and technology to extract information from computers and other devices.</p> | <p>Inspected the CMDB configuration to determine whether IT assets were managed throughout their lifecycle.</p> <p>Inspected the ServiceNow discovery IP range list and discovery schedule list to determine whether IT servers and IT assets were tracked.</p> <p>Refer to CC7.1.9 for testing over the new IT asset discovery.</p> | No exceptions noted. |
| CC7.1.8 | <p>Firewall and Network Standards</p> <p>The TCH network infrastructure is governed by hardening standards defined by Information Security. Network devices supporting the systems are deployed to those standards. Monthly compliance checks are performed to ensure the devices are functioning under the standards.</p> | <p>Inspected hardening standards to determine whether hardening standards for network infrastructure were defined and documented.</p> <p>For a selection of months, inspected monthly compliance report to determine whether compliance checks are performed to ensure devices are hardened per defined standards.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| CC7.1.9 | New System Discovery Management conducts a monthly review of devices newly detected by ServiceNow Discovery. A monthly export is generated for devices added in the last 30 days and management meets monthly to review the exported lists and takes action if necessary. | For a selection of months, inspected ServiceNow Discovery export listings and meeting invites to determine whether management reviewed newly detected devices | No exceptions noted. |

CC7.2 – The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| CC7.2.1 | <p>Vulnerability Scans</p> <p>Weekly vulnerability scans over the network and servers are completed to identify any potential security threats that would impair system security and availability. Risks are then analyzed and appropriate corrective action is taken to address the security and availability risks identified through weekly vulnerability meetings. If necessary, the change management process is initiated as a result of any findings.</p> | For a selection of weeks, inspected vulnerability scans and meeting invites and meeting minutes to determine whether the scans were completed, potential security and availability threats were identified, risks were analyzed and mitigation strategies were developed. | No exceptions noted. |
| CC7.2.2 | <p>External Network Risk Assessment</p> <p>On an annual basis, assessments of external network risks are performed to identify potential impairments that could impact system security and availability. Critical, High and Medium findings are entered into Archer for tracking where a criticality based on severity and likelihood as well as a remediation plan is documented. Findings are remediated based on assigned criticality and may be remediated via the change management process as applicable.</p> <p>Controls related to entering, tracking and remediating findings within Archer are documented in CC3.2.1 Assessing Risk.</p> | Inspected the third-party external risk assessment summaries and Archer findings to determine whether identified vulnerabilities were remediated based on criticality. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC7.2.3 | <p>Security Administration and Security Violations</p> <p>ArcSight is used to support security administration including managing security violations for both mainframe and distributed environments. Security related activities such as user data change, file security attribute change and security violations including inappropriate user activity, unauthorized software, virus and firewall alerts are captured, logged and reported using ArcSight. ArcSight is configured to capture the defined security related activities and send an alert to the Information Security responsible personnel through the Information Security workstation and to their mobile phones when there is an event that meets the defined criteria such as possible security violation. Each alert is reviewed and triaged by the managed security service provider, Cipher, and followed up and cleared by Information Security, as necessary. On an ongoing basis, the Information Security responsible personnel reviews the alerts and other activities to determine that alerts were responded to appropriately. Alerts remain pending in ArcSight until they are resolved.</p> | <p>Inspected the configuration for alert event setup in ArcSight to determine whether ArcSight was setup to capture and log the security related events such as user data change, file security attribute change and security violation including inappropriate user activity, unauthorized software, IDS, virus and firewall alerts and sends automatic alerts to Cipher, and the Information Security Analyst when an event that met the defined condition occurred.</p> <p>Observed online ArcSight alert messages on the ArcSight workstation located in a secure area of the Information Security group and noted Information Security responded to the alert in ArcSight and that alert remained pending until it was resolved.</p> <p>For a selection of months, inspected a selected ArcSight violation report to determine whether the security violations were captured and retained in ArcSight.</p> | No exceptions noted. |
| CC7.2.4 | <p>Intrusion Detection System</p> <p>The TCH networks include an Intrusion Detection System (IDS), CarbonBlack. This system detects and classifies suspicious events according to a library of signatures provide by the vendor. The IDS/IPS is programmed to send alerts when thresholds for particular attack signatures are exceeded. Information Security management are alerted of intrusion activities. Incidents noted are recorded in ArcSight and depending on the nature and type of problem, the incident is escalated to the designated group for follow-up and resolution. If necessary, corrective action is taken via updates to policies and/or the change management process due to the alerts.</p> | <p>For a selection of servers, inspected the CarbonBlack management console to determine whether CarbonBlack was configured to monitor traffic.</p> <p>For a selection of incidents, inspected tickets and supporting documentation to determine whether the incident was escalated and resolved.</p> <p>Inspected configured threat intelligence library in CarbonBlack to determine whether the system was configured to detect and classify events according to the signatures.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|----------------------|
| | <p>CarbonBlack is configured to generate alerts through ArcSight.</p> <p>Controls related incidents analysis and resolution are documented in CC7.4.4 Security Administration and Security Violations.</p> | <p>Inspected ArcSight management console to determine whether ArcSight was configured to alert Information Security in case of potential threats.</p> <p>Inspected the list of users with administrator access to CarbonBlack, job titles, and inquired of the management to determine whether administrative access to CarbonBlack was restricted to authorized personnel.</p> <p>Inquired of Information Security management regarding policy and process updates and were informed corrective action was taken via updates to policies and/or the change management process due to the alerts.</p> <p>Refer to CC7.4.4 Security Administration and Security Violations for test results of incident analysis and resolution for ArcSight.</p> | |
| CC7.2.5 | <p>Virus and Unauthorized Software Monitoring</p> <p>TCH utilizes Symantec Endpoint Protection to protect against viruses, malware, malicious code and unauthorized software. Virus definitions are kept current and infected files are quarantined. Security alerts are logged, reported and analyzed via ArcSight.</p> <p>Controls related security alerts being logged, reported and analyzed are described in CC7.4.4 Security Administration and Security Violations.</p> | <p>Inspected the TCH Incident Response Plan to determine whether procedures for virus definitions being kept current and infected files quarantine were documented.</p> <p>Inspected the Symantec Endpoint Protection Manager configuration to determine whether TCH workstations were protected and virus definitions were updated on a recurring basis.</p> <p>For a selection of servers, inspected the Symantec Endpoint Protection Manager configuration to determine whether TCH servers were protected.</p> <p>Observed ArcSight and noted security alerts from Symantec Endpoint Protection were configured to be logged via ArcSight.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|---|
| CC7.2.6 | <p>Employee Noncompliance</p> <p>TCH handles issues of noncompliance related to system availability and security policies as they arise. The employee is directly contacted by management and is required to take corrective action immediately. Employee noncompliance may impact performance evaluations and violations of the Code of Conduct may result in disciplinary action including termination.</p> <p>Reports of illegal, fraudulent, or unethical conduct can be made to management, or anonymously by mailing a written letter.</p> | For a selection of incidents including non-compliance issues, inspected tickets and supporting documentation to determine whether the incident was escalated and resolved. Inspected the Code of Conduct to determine whether methods of reporting illegal, fraudulent, or unethical conduct and impact of violations were documented. | No exceptions noted. |
| CC7.2.7 | <p>Problems Reporting and Tracking</p> <p>TCH has established incident response procedures which are documented in the TCH Incident Management Process Framework. TCH uses ServiceNow tickets to record incidents.</p> <p>Depending on the nature and type of incident, the ServiceNow ticket is escalated to the designated group for follow up and resolution. Once an incident is resolved, the ticket is closed.</p> | <p>Inspected the TCH Incident Management Process Framework document to determine whether procedures for incident responses, including roles and responsibilities, were documented.</p> <p>For a selection of incidents, inspected the ServiceNow tickets to determine whether the resolution of the incidents was recorded in the ServiceNow tickets.</p> | No exceptions noted. |
| CC7.2.8 | <p>Security Breaches and Response</p> <p>TCH employees are required to report breaches to management as dictated by the Information Security policies. Information Security staff will prepare a security incident report and ticket that includes the incident details and resolution. Each incident report is reviewed and resolved by the Incident Response Team in accordance with the response procedures documented in the Incident Response Plan.</p> <p>Contractors, and third-party users of information systems and services are required to note and report any observed or suspected IS incidents. These requirements are</p> | <p>Inspected the IS Incident Management and IS Communication and Operations Management policies and Incident Response Plan to determine whether they documented requirements for employees, contractors and third-party users to report security breaches to management and response procedures for the Incident Response Team.</p> <p>Inspected the security incident reports and tickets, and inquired of management, and noted that there were no security breach incidents during the period;</p> | Noted that there were no security breach incidents during the period; therefore, the operating effectiveness of this control could not be tested. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|----------------------|
| | <p>communicated during client onboarding or in third-party agreements.</p> <p>In the event that the incident involves the unauthorized access to, or use of sensitive information, the Incident Response Team is responsible for notifying the appropriate affected parties, regulatory agencies, and law enforcement a timely manner in accordance with applicable product rules and as required by applicable laws.</p> | therefore, the operating effectiveness of this part of the control could not be tested. | |
| CC7.2.9 | <p>Availability Monitoring</p> <p>TCH utilizes third-party tools to monitor performance, memory and disk space in the distributed systems environment to help ensure systems are fully functional. Automated email alerts are sent to operations management in the event of capacity and availability issues, risks are analyzed and appropriate corrective action is taken.</p> | <p>Inspected the monitoring tool configurations and an email notification and noted the tool was configured to distribute automated email alerts to Network Operations based on established performance rules and thresholds.</p> <p>Refer to CC7.4.3 Problems Reporting and Tracking for test results of incident reporting and tracking within ServiceNow.</p> | No exceptions noted. |
| CC7.2.10 | <p>System Security Monitoring</p> <p>TCH has an agreement with third-party provider to offer 24x7 security alert monitoring and adhere to TCH requirements.</p> | Inspected the agreement between Cipher and TCH to determine whether the responsibilities of the third-party provider were outlined and adhere to TCH requirements. | No exceptions noted. |
| CC7.2.11 | <p>Communication Line Monitoring</p> <p>Network Operations team monitor all communication lines on an ongoing basis. Incidents noted are recorded in ServiceNow tickets.</p> <p>Depending on the nature and type of problem, the incident is escalated to the designated group for follow up and resolution. Network Operations team notifies the customers or other parties if applicable. Once the incident is resolved, the ticket is closed.</p> | <p>Observed Network Operations monitor all in scope communication lines at the North Carolina Network Operations Center.</p> <p>For a selection of incidents, inspected the ServiceNow tickets to determine whether resolutions of the incidents were recorded in the ServiceNow tickets.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|------------------|
| CC7.2.12 | Database Monitoring (RTP) The DB2 database environment is monitored through multiple tools which includes system alerting through SCOM for critical performance alerts and performance and capacity management through IBM Data Server Monitoring. | Inspected SCOM alert configurations and IBM Data Server Manager dashboard to determine whether each tool was configured to monitor the performance and capacity management of the DB2 database environment. | |

CC7.3 – The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC7.3.1 | <p>Information Security Incident Management Policy</p> <p>The Information Security Incident Management Policy documents procedures to manage information security events, incidents, weaknesses and the gathering of forensic evidence. The policy covers identifying, reporting, investigating, and escalating incidents. The Incident Response Team (which includes members of Information Security, Technology and Operations, and Risk Management) evaluates, assesses and prioritizes incident impacts and isolates affected systems, takes corrective action and identifies lessons learned. The Incident Response Team identifies weaknesses in responses, if any, and implements changes to improve the incident response procedures.</p> | <p>Inspected the TCH Information Security Incident Management policy to determine whether policies and procedures for IS incident identification, reporting, investigating, escalating and corrective action were documented.</p> <p>Inspected updates made to the Incident Response Plan during the period to determine whether the Incident Response Team identified weaknesses in responses and implemented changes to improve procedures.</p> | No exceptions noted. |
| CC7.3.2 | <p>Employee Noncompliance</p> <p>TCH handles issues of noncompliance related to system availability and security policies as they arise. The employee is directly contacted by management and is required to take corrective action immediately. Employee noncompliance may impact performance evaluations and violations of the Code of Conduct may result in disciplinary action including termination. Reports of illegal, fraudulent, or unethical conduct can be made to management, or anonymously by mailing a written letter.</p> | <p>For a selection of incidents including non-compliance issues, inspected tickets and supporting documentation to determine whether the incident was escalated and resolved.</p> <p>Inspected the Code of Conduct to determine whether methods of reporting illegal, fraudulent, or unethical conduct and impact of violations were documented.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|--|
| CC7.3.3 | <p>Security Breaches and Response</p> <p>TCH employees are required to report breaches to management as dictated by the Information Security policies. Information Security staff will prepare a security incident report and ticket that includes the incident details and resolution. Each incident report is reviewed and resolved by the Incident Response Team in accordance with the response procedures documented in the Incident Response Plan.</p> <p>Contractors, and third party users of information systems and services are required to note and report any observed or suspected IS incidents. These requirements are communicated during client onboarding or in third-party agreements.</p> <p>In the event that the incident involves the unauthorized access to, or use of sensitive information, the Incident Response Team is responsible for notifying the appropriate affected parties, regulatory agencies, and law enforcement a timely manner in accordance with applicable product rules and as required by applicable laws.</p> | <p>Inspected the IS Incident Management and IS Communication and Operations Management policies and Incident Response Plan to determine whether they documented requirements for employees, contractors and third party users to report security breaches to management and response procedures for the Incident Response Team.</p> <p>Inspected the security incident reports and tickets, and inquired of management, and noted that there were no security breach incidents during the period; therefore, the operating effectiveness of this part of the control could not be tested.</p> | <p>Noted that there were no security breach incidents during the period; therefore, the operating effectiveness of this control could not be tested.</p> |
| CC7.3.4 | <p>Problems Reporting and Tracking</p> <p>TCH has established incident response procedures which are documented in the TCH Incident Management Process Framework. TCH uses ServiceNow tickets to record incidents.</p> <p>Depending on the nature and type of incident, the ServiceNow ticket is escalated to the designated group for follow up and resolution. Once an incident is resolved, the ticket is closed.</p> | <p>Inspected the TCH Incident Management Process Framework document to determine whether procedures for incident responses, including roles and responsibilities, were documented.</p> <p>For a selection of incidents, inspected the ServiceNow tickets to determine whether the resolution of the incidents was recorded in the ServiceNow tickets.</p> | <p>No exceptions noted.</p> |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| CC7.3.5 | <p>Security Administration and Security Violations</p> <p>ArcSight is used to support security administration including managing security violations for both mainframe and distributed environments. Security related activities such as user data change, file security attribute change and security violations including inappropriate user activity, unauthorized software, virus and firewall alerts are captured, logged and reported using ArcSight. ArcSight is configured to capture the defined security related activities and send an alert to the Information Security responsible personnel through the Information Security workstation and to their mobile phones when there is an event that meets the defined criteria such as possible security violation. Each alert is reviewed and triaged by the managed security service provider, Cipher, and followed up and cleared by Information Security, as necessary. On an ongoing basis, the Information Security responsible personnel reviews the alerts and other activities to determine that alerts were responded to appropriately. Alerts remain pending in ArcSight until they are resolved.</p> | <p>Inspected the configuration for alert event setup in ArcSight to determine whether ArcSight was setup to capture and log the security related events such as user data change, file security attribute change and security violation including inappropriate user activity, unauthorized software, IDS, virus and firewall alerts and sends automatic alerts to Cipher, and the Information Security Analyst when an event that met the defined condition occurred.</p> <p>Observed online ArcSight alert messages on the ArcSight workstation located in a secure area of the Information Security group and noted Information Security responded to the alert in ArcSight and that alert remained pending until it was resolved.</p> <p>For a selection of months, inspected a selected ArcSight violation report to determine whether the security violations were captured and retained in ArcSight</p> | No exceptions noted. |

CC7.4 – The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|--|
| CC7.4.1 | <p>Information Security Incident Management Policy</p> <p>The Information Security Incident Management Policy documents procedures to manage information security events, incidents, weaknesses and the gathering of forensic evidence. The policy covers identifying, reporting, investigating, and escalating incidents. The Incident Response Team (which includes members of Information Security, Technology and Operations, and Risk Management) evaluates, assesses and prioritizes incident impacts and isolates affected systems, takes corrective action and identifies lessons learned. The Incident Response Team identifies weaknesses in responses, if any, and implements changes to improve the incident response procedures.</p> | <p>Inspected the TCH Information Security Incident Management policy to determine whether policies and procedures for IS incident identification, reporting, investigating, escalating and corrective action were documented.</p> <p>Inquired of management regarding updates to the Incident Response Plan as a result of identified weaknesses and were informed there were none during the period.</p> | No exceptions noted. |
| CC7.4.2 | <p>Security Breaches and Response</p> <p>TCH employees are required to report breaches to management as dictated by the Information Security policies. Information Security staff will prepare a security incident report and ticket that includes the incident details and resolution. Each incident report is reviewed and resolved by the Incident Response Team in accordance with the response procedures documented in the Incident Response Plan.</p> <p>Contractors, and third party users of information systems and services are required to note and report any observed or suspected IS incidents. These requirements are communicated during client onboarding or in third-party agreements.</p> <p>In the event that the incident involves the unauthorized access to, or use of sensitive information, the Incident Response Team is responsible for notifying the appropriate affected parties, regulatory agencies, and law enforcement a</p> | <p>Inspected the IS Incident Management and IS Communication and Operations Management policies and Incident Response Plan to determine whether they documented requirements for employees, contractors and third party users to report security breaches to management and response procedures for the Incident Response Team.</p> <p>Inspected the security incident reports and tickets, and inquired of management, and noted that there were no security breach incidents during the period; therefore, the operating effectiveness of this part of the control could not be tested.</p> | <p>Noted that there were no security breach incidents during the period; therefore, the operating effectiveness of this control could not be tested.</p> |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| | timely manner in accordance with applicable product rules and as required by applicable laws. | | |
| CC7.4.3 | <p>Problems Reporting and Tracking</p> <p>TCH has established incident response procedures which are documented in the TCH Incident Management Process Framework. TCH uses ServiceNow tickets to record incidents.</p> <p>Depending on the nature and type of incident, the ServiceNow ticket is escalated to the designated group for follow up and resolution. Once an incident is resolved, the ticket is closed.</p> | <p>Inspected the TCH Incident Management Process Framework document to determine whether procedures for incident responses, including roles and responsibilities, were documented.</p> <p>For a selection of incidents, inspected the ServiceNow tickets to determine whether the resolution of the incidents was recorded in the ServiceNow tickets.</p> | No exceptions noted. |
| CC7.4.4 | <p>Security Administration and Security Violations</p> <p>ArcSight is used to support security administration including managing security violations for both mainframe and distributed environments. Security related activities such as user data change, file security attribute change and security violations including inappropriate user activity, unauthorized software, virus and firewall alerts are captured, logged and reported using ArcSight. ArcSight is configured to capture the defined security related activities and send an alert to the Information Security responsible personnel through the Information Security workstation and to their mobile phones when there is an event that meets the defined criteria such as possible security violation. Each alert is reviewed and triaged by the managed security service provider, Cipher, and followed up and cleared by Information Security, as necessary. On an ongoing basis, the Information Security responsible personnel reviews the alerts and other activities to determine that alerts were responded to appropriately. Alerts remain pending in ArcSight until they are resolved.</p> | <p>Inspected the configuration for alert event setup in ArcSight to determine whether ArcSight was setup to capture and log the security related events such as user data change, file security attribute change and security violation including inappropriate user activity, unauthorized software, IDS, virus and firewall alerts and sends automatic alerts to Cipher, and the Information Security Analyst when an event that met the defined condition occurred.</p> <p>Observed online ArcSight alert messages on the ArcSight workstation located in a secure area of the Information Security group and noted Information Security responded to the alert in ArcSight and that alert remained pending until it was resolved.</p> <p>For a selection of months, inspected a selected ArcSight violation report to determine whether the security violations were captured and retained in ArcSight</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| CC7.4.5 | <p>Disaster Recovery Plan</p> <p>Disaster Recovery plans are maintained and updated at least annually by all respective business unit managers/application owners, who are also responsible for providing the Disaster Recovery training to their team members, in order to address disaster risk. All Disaster Recovery plans must address strategies to achieve recovery time objective (RTO) and recovery point objective (RPO).</p> <p>IT Service Continuity Management performs Disaster Recovery testing at least once per year. Testing follows the Disaster Recovery plan and includes a failover to the alternate hosting sites. Results are documented and risks are assessed to improve/update the Disaster Recovery plan.</p> | <p>Inspected the plans to determine whether a review and approval process was established.</p> <p>Inspected the Business Continuity Management policy to determine whether it documented roles and requirements for maintenance and review of the Disaster Recovery plans, training, and addressing RTO and RPO strategies were established to address disaster risk.</p> <p>Inspected the annual Disaster Recovery testing results and Disaster Recovery Plan to determine whether the testing followed the Disaster Recovery Plan, results were officially documented and the Disaster Recovery Plan was updated to address identified risks.</p> | No exceptions noted. |
| CC7.4.6 | <p>Business Continuity Plan</p> <p>TCH has established a Business Continuity Program to provide capabilities, information, and training to ensure that employees are prepared for any interruption and know what to do in the event of an interruption incident at any of the TCH sites. The TCH Enterprise Risk Management Framework document and Business Continuity Management policy define roles and responsibilities for business continuity and disaster recovery plan development and maintenance, identify procedures to facilitate plan development, establish a review and approval process for business continuity plans, specify requirements for plan ownership, and provide requirements and frequency for plan test.</p> | <p>Inspected the TCH Enterprise Risk Management Framework and Business Continuity Management Policy documents, and recent business continuity plan tests to determine whether roles and responsibilities for business continuity and disaster recovery plan development and maintenance were defined, procedures to facilitate plan development were identified, a review and approval process for business continuity plans was established, requirements for plan ownership were specified, and requirements and frequency for plan test were provided.</p> <p>Inspected the business continuity plans to determine whether a review and approval process was established.</p> | No exceptions noted. |

CC7.5 – The entity identifies, develops, and implements activities to recover from identified security incidents.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC7.5.1 | <p>LiteSpeed Backup - IXN</p> <p>SQL database backups occur daily at 6 a.m. and are written locally by LiteSpeed. Two days' worth of backups are retained. Transaction log backups are also written to locally every hour. The results of the backups, including any issues, are communicated to the DBA group via email. ServiceNow tickets are opened to resolve any issues noted.</p> <p>Refer to CC7.4.3 Problems Reporting and Tracking for incident management testing.</p> | <p>Inspected the backup schedule to determine whether backups were configured to occur daily at 6 a.m.</p> <p>Inspected the SQL backup logs to determine whether the SQL backups were performed in accordance within the backup schedules.</p> <p>Please refer to CC6.1.8 Administrator Access - Distributed Environment for results of testing related to access to SQL database.</p> | No exceptions noted. |
| CC7.5.2 | <p>Avamar Backups - IXN</p> <p>Full Avamar backups occur daily and replicates the data to Pennsylvania and North Carolina data centers. Avamar backups are retained based upon a predefined schedule. The results of the backups, including any issues, are communicated to the Network Operations. ServiceNow tickets are opened to resolve any issues noted.</p> <p>Refer to CC7.4.3 Problems Reporting and Tracking for incident management testing.</p> | <p>For a selection of dates, inspected the Avamar backup tape logs to determine whether the Avamar backups were performed in accordance within the backup schedules.</p> <p>Inspected the replication schedule configuration and selected replication log to determine whether the Avamar backups replicate to the alternate data centers.</p> <p>Inspected the list of users with administrator access to Avamar job titles, and inquired of the management to determine whether administrative access to Avamar was restricted to authorized personnel.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC7.5.3 | <p>Virtual Tape Library</p> <p>Databases for EPN and CHIPS are backed up onto a virtual tape library (VTL) based on an automatic or manual schedule. BL Library (BL LIB), a tape management library system, is used to facilitate this process. Backup activities are monitored online by Network Operations as documented in the Operator Schedules. The tape management library system logs backup activities in the System Logged Tapes. Backup issues, if any, are followed up and resolved and recorded in a ServiceNow incident ticket.</p> <p>The PA data center is monitored and managed by North Carolina and the New York Operations Centers.</p> | <p>Observed Network Operations monitor the backup activities online through the computer operator console and the System Logged Tapes to determine whether the systems and databases were backed up onto virtual tape library.</p> <p>For a selection of dates, inspected the System Logged Tapes log to determine whether backups were completed.</p> <p>For a selection of dates, inspected the Operator Schedule for the North Carolina and New York Operations Centers to determine whether backup activities were monitored online by the Network Operations and noted no backup issues in the backup activities recorded on the Operator Schedule available for inspection.</p> <p>Please refer to CC7.4.3 Problems Reporting and Tracking for test results of problem reporting and tracking of backup failures.</p> | No exceptions noted. |
| CC7.5.4 | <p>Database Backups- RTP</p> <p>RTP database environments are backed up daily using native DB2 shells scripts with 3 days of backups maintained locally on the file system including transaction logs. Backup images are archived using the Avamar system. The results of the backups, including any issues, are communicated to the DBA group via email notifications. ServiceNow tickets are opened to follow up and resolve backup issues.</p> | <p>Inspected the database backup configuration to determine whether the RTP databases were configured to backup per schedule and retain 3 days of backups locally.</p> <p>For a selection of databases and dates, inspected the database backup logs to determine whether backups completed successfully per schedule, and noted no backup issues were recorded for the selected dates.</p> <p>Please refer to CC7.4.3 Problems Reporting and Tracking for test results of problem reporting and tracking of backup failures.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| CC7.5.5 | <p>Server Backups - RTP</p> <p>All servers are backed up by Avamar (for AIX servers) and Networker (for RHEL servers) at both North Carolina and Pennsylvania data centers. A backup storage system is used to facilitate this process. The backup management system logs backup activities and any backup issues are followed up and resolved within a ServiceNow Incident ticket. Transaction data/logs are backed up and retained for 90 days.</p> | <p>Inspected the server backup configuration to determine whether the RTP servers were configured to backup per schedule.</p> <p>For a selection of servers and dates, inspected the server backup logs to determine whether backups completed successfully per schedule, and noted no backup issues were recorded for the selected dates.</p> <p>Please refer to CC7.4.3 Problems Reporting and Tracking for test results of problem reporting and tracking of backup failures.</p> | No exceptions noted. |
| CC7.5.6 | <p>Online Backups</p> <p>For EPN, CHIPS and RTP, records are written from the active database system to the local standby database in North Carolina and routed to the remote database system in Pennsylvania through the use of leased lines that allow file operations to occur between local and remote hosts. All files associated with a given processing cycle are updated and mirrored real time at both data centers. RTP transactions are written on the database locally and replicated to the remote stand by systems as they are committed into active database. Database transactions associated with RTP are updated simultaneously at both data centers. Online replication activities are monitored by Network Operations as documented in the Operator Schedules. Any issues are followed up and resolved.</p> | <p>Inspected the network diagrams to determine whether the design included Optical Point-to-Point leased lines between the North Carolina and Pennsylvania data centers.</p> <p>Inspected the system disk pack configuration to determine whether EPN and CHIPS application files were written on internal mirror packs locally and on remote backup packs.</p> <p>Inspected the system replication configurations to determine whether RTP records were configured to write from active to local standby hosts.</p> <p>For a selection of dates, inspected the Operator Schedules to determine whether the online backup activities were monitored and noted no backup issues in the online backup activities recorded on the schedules for the selected dates.</p> <p>Please refer to CC7.4.3 Problems Reporting and Tracking for test results of problem reporting and tracking of backup failures.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|-----------------------------|
| CC7.5.7 | <p>Crisis Management Plan</p> <p>The TCH Crisis Management Plan has been developed to ensure TCH has a defined process for responding to and recovering from events likely to lead to negative consequences and/or unplanned business interruptions. The primary trigger for activation of the crisis management plan occurs via escalation from one of the internal incident response plans. The plan provides strategic response guidance for executives and senior managers to use when managing disruptive events. It also establishes a structure and process for integrating all levels of management including operational resources. The objective of the framework is to facilitate efficient and timely collaboration between all level of management to minimize the impact of unplanned interruptions and provide guidance for continuing operations during an unplanned event.</p> | <p>Inspected TCH's Crisis Management Plan to determine whether the plan established a process for responding and recovering from events causing negative consequences and unplanned business interruptions.</p> | <p>No exceptions noted.</p> |
| CC7.5.8 | <p>Redundancy Resiliency</p> <p>TCH uses redundant processing systems located at the two data centers in order to ensure system availability and maximum uptime. EPN, CHIPS and IXN customers are required to provide connectivity from their backup data center to TCH.</p> <p>RTP transaction processing runs "active-active" in the North Carolina and Pennsylvania data center (which is managed and controlled by Iron Mountain). RTP customers are required to maintain connectivity to both TCH data centers from their primary and backup sites.</p> | <p><i>EPN, CHIPS, and IXN</i></p> <p>Inspected system configurations and the annual failover tests, and inquired of management to determine whether EPN, CHIPS, and IXN employed intra and inter-site redundancy.</p> <p><i>RTP</i></p> <p>Inspected system and server processing configurations, and annual failover test, and inquired of management to determine whether RTP was configured to run active-active in the NC and PA data centers with intra and inter-site redundancy and in the event of a site outage, would continue processing on the alternate site.</p> | <p>No exceptions noted.</p> |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|---|---|-------------------------|------------------|
| Complementary User Entity Control(s) | | | |
| <p>Controls should be established at user entities so that:</p> <ul style="list-style-type: none"> • Users maintain active connections from their primary data center to both TCH data centers and to be able to send and receive payment messages to/from both data centers simultaneously. Customers maintain connectivity from their disaster recover/backup data centers to both TCH data centers. • Users notify TCH of outages. | | | |

CC 8.0 – Common criteria related to change management

CC8.1 – The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|-----------------------------|
| CC8.1.1 | <p>SDLC Policies and Methodologies</p> <p>Guidelines and methodology for application development for both the Unisys and distributed environments are documented in the Software Development Life Cycle (SDLC) and Project Management Handbook. The documents address requirements for application development and maintenance which include the following phases:</p> <p>Phase 1 – Project Initiation</p> <p>Phase 2 – Project Planning</p> <p>Phase 3 – Project Execution</p> <p>Phase 4 – Project Close Out</p> | <p>Inspected the SDLC and Project Management Handbook documents to determine whether the requirements for application development and major projects were documented and included requirements for project initiation, planning, execution, and close out.</p> | <p>No exceptions noted.</p> |
| CC8.1.2 | <p>Project Management</p> <p>Projects are initiated in response to the changing processing or regulatory environment or by Network Operations Center or System Development groups in response to ideas to improve operational, processing efficiencies or to resolve incidents. Major projects are those over a certain dollar value and require approval by the O&T Portfolio Steering Committee.</p> <p>Once a project is authorized by the O&T Portfolio Steering Committee, the project is created in CA Project & Portfolio Management software (CA PPM).</p> <p>Projects are recorded, tracked and monitored for timely completion and maintained in CA PPM. Major projects are required to follow the requirements in the SDLC and Project Management Handbook. The PM Sharepoint workflow</p> | <p>For a selection of major projects noted as completed from the Portfolio maintained in the CA PPM software, inspected the following documentation (based on the document checklist) to determine whether the project was recorded, tracked and approved in accordance with requirements in the SDLC and Project Management Handbook:</p> <ul style="list-style-type: none"> • Project Request Form/Project Business Case • Project Plan • Project Scope • Business and Functional Requirements • Document Checklist • Technical Design | <p>No exceptions noted.</p> |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|------------------|
| | <p>approval function is used to obtain electronic signatures of approval for all critical documents. Access to the PM Sharepoint site is controlled through the security features of Active Directory.</p> <p>Various documents when required, depending on the nature of project, are prepared to support the project development and implementation. Each document is approved by the related management. Key documents are guided by the PM checklist:</p> <ul style="list-style-type: none"> • Project Request Form/Project Business Case provides nature of project including other such as description, priority and timeline. • Project Plan provides each phase of the project and the related timeline from start to finish. • Business and Functional Requirements document provides objective of the project, requirements for system changes including system dependencies and constraints. • Technical Design document provides overview and details of changes, functional design and business continuing plan. • Implementation and Transition Plan document provides overall approach for the implementation including the roles and responsibilities of each group, timelines and backout procedures. <p>For major projects, ServiceNow tickets are created and the standard TCH change management process is performed including request, authorization, testing, approval and implementation.</p> | <ul style="list-style-type: none"> • Implementation and Transition Plan • Project Approvals <p>Observed the login process for the PM Sharepoint site and noted that user IDs and passwords were required to access the LAN and that access to PM Sharepoint was authenticated through Windows Active Directory.</p> | |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| CC8.1.3 | <p>Application, Program and Configuration Change Request Initiation and Authorization</p> <p>The Clearing House Change Control Policy document provides requirements for change initiation, approval, and the bi-weekly Change Advisory Board meeting and implementing a change.</p> <p>Requests for application development including report changes, changes to programs, and configuration changes to related utilities are documented in ServiceNow. A ServiceNow ticket is created for request for new programs and enhancements to existing programs including updates to specific tables. The ServiceNow ticket is reviewed by Technology and Product representatives to determine whether a program change should be developed. For in-house development, the program change is assigned to the appropriate development team and a ServiceNow Change ticket is created for the assignment. ServiceNow tickets are automatically routed to designated management for review and authorization prior to beginning development of the change.</p> <p>Timeline Not Met' emergency changes to resolve an issue that is negatively impacting TCH's systems are submitted for review and authorization outside of the change control process. A ServiceNow ticket indicating the nature of incidents and changes needed to address the incident is required. Authorization for these emergency changes can be obtained verbally and described in the related ServiceNow ticket. These emergency changes require an additional authorization from four ECAB members. The related ServiceNow ticket is reviewed and approved by Change Advisory Board prior to implementation in the production environment. Breakfix emergency changes are those requiring immediate action due to failure of service and can be verbally</p> | <p>Inspected The Clearing House Change Control Policy document to determine whether the document addressed the following: change initiation, authorization, approval, and the bi-weekly Change Advisory Board meeting, and implementing a change.</p> <p>For a selection of program changes (regular and emergency) and a selection of software releases for both the Unisys (Mainframe) and distributed (Windows) environments and configuration changes to related utilities, inspected the related ServiceNow tickets to determine whether the change requests were documented, included a description, and were authorized by required management.</p> <p>Inspected the configuration within ServiceNow of the routing functionality to determine whether ServiceNow was configured to automatically route change tickets to the approvers required by policy.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| | approved. Documentation for these types of emergency changes must be performed within 24 hours. | | |
| CC8.1.4 | <p>Application, Program and Configuration Program Development and Test Environment</p> <p>Based on the information in ServiceNow, the System Development Manager assigns or carries out the tasks in the design and development phases within the development system environment. Programmers develop programs on a stand-alone processor or servers dedicated for program development and testing.</p> <p>QC performs testing on the developed code to ensure requirements are met. When the test results are satisfactory, a ServiceNow change request is submitted by the development team to request the program to be promoted to the Quality Control (QC) test environment.</p> <p>Vendor software is installed and “smoke tested” in the development environment prior to being installed in the QC environment.</p> <p>RTP source code is developed by a third-party vendor. Requirements for RTP development work is provided to the third-party developer in business requirement documentation. Source code packages are provided and then deployed and tested within the development environment by TCH.</p> | <p>Inspected the system configuration for both the Unisys and distributed environments to determine whether test and development environments were separated from the production environments.</p> <p>For a selection of program changes, inspected the related ServiceNow tickets and supporting documentation to determine whether code development and testing were performed in environments separate from the production environment, and RTP business requirements given to the third-party were met.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|-----------------------------|
| CC8.1.5 | <p>Application, Program and Configuration Testing and Approval</p> <p>Upon receipt of required program documentation from the appropriate System Development Manager, QC performs the following:</p> <ul style="list-style-type: none"> • Reviews documentation of program specifications and customer and operating procedures, written authorizations, and code changes; and • Performs operational acceptance (integration) testing. <p>The nature of change dictates the requirement for Quality Control (QC) testing and environment where testing takes place. When the ServiceNow Change ticket requires quality assurance testing and is ready for testing, the ownership of the ticket is transferred to QC, who will oversee the change until it is implemented in the bank test environment, and as necessary, the business sponsor performs user acceptance testing. For projects that impact the application functionality, clients have the opportunity to further test the new application software in the bank test environment. Voluntary customer testing is performed for all major changes. Depending on the extent and nature of the change, customers may be required to perform certification testing in the bank test environment to prove their systems are ready for the change. Configuration changes to applications/utilities used in the controls do not require QC testing.</p> <p>For all releases, a backout plan is developed and documented in the project's PM Sharepoint folder. When the software is ready to move to the production environment, the development team submits a change request in ServiceNow to migrate into the production environment. Information Security approval is required for all code deployments prior to the program being deployed to production.</p> | <p>For a selection of program changes for both the Unisys (mainframe) and distributed (Windows) environments and configuration changes to related utilities, inspected ServiceNow tickets, testing documentation, and backout plans and IS approval to determine whether the changes passed the required testing, were reviewed (if applicable) by QC, and backout plans were documented, and IS approval was given for code deployments.</p> | <p>No exceptions noted.</p> |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|----------------------|
| CC8.1.6 | <p>Application, Program and Configuration Implementation</p> <p>A bi-weekly Change Advisory Board meeting, which is attended by designated members of Change Control, Application Development, Infrastructure, Quality Control, Information Security and other Technology and Network Operations Center representatives as needed, is conducted to review and approve each change that is scheduled for migration into the production environment. The meeting is monitored by Operation Services. The related ServiceNow ticket for a change is reviewed and approved by the Change Advisory Board prior to implementation in the production environment by the assigned implementers in the designated groups that are responsible for implementing the changes.</p> <p>The ServiceNow ticket is assigned to an implementer within the designated groups responsible for moving the executable programs into the production environment. For all program changes, individuals in the designated groups move the executable programs to production status upon receipt of a ServiceNow ticket approved by the Change Advisory Board. The ServiceNow ticket is closed after the completion of implementation. Each of the above steps is required to be documented in the related ServiceNow ticket.</p> | <p>For a selection of weeks, inspected the meeting evidence to determine whether program changes were reviewed for approval.</p> <p>For a selection of regular and emergency changes for both the Unisys and distributed environments, inspected the related ServiceNow tickets and supporting documentation to determine whether the tickets documented that:</p> <ul style="list-style-type: none"> • The programs were approved for implementation into the production environment; • The ServiceNow tickets were assigned to implementers within the designated groups for moving the programs into the production environment; and • The tickets were closed for completion following the changes being implemented in the production environment. <p>Inspected the listing of users with access to implement changes and job titles to determine whether users were granted access based on their job responsibilities.</p> | No exceptions noted. |
| CC8.1.7 | <p>Security and Availability-based Development and Testing</p> <p>The applicable development team codes solutions based on security and availability requirements per Information Security policies.</p> <p>Before turnover to Quality Control, the development teams perform unit testing to ensure that core components of the requirements are executable. For application changes, specific security-based testing is included in the unit testing (e.g. Fuzz, or dynamic scan).</p> | <p>Inspected the TCH Secure Software Development Policy and TCH Secure Software Best Practices document to determine whether developers are provided with secure coding guidelines and other best practices to apply during code development.</p> <p>For a selection of program changes, inspected the related ServiceNow tickets to determine whether security-based testing where applicable, was performed.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| CC8.1.8 | <p>Backout Plans</p> <p>Backout plans are documented to allow any changes to be reversed to the previous environment, as dictated by the change control policy.</p> | <p>Inspected the Change Control Policy document to determine whether policies were in place requiring changes to have documented backout plans.</p> <p>For a selection of changes, inspected the related ServiceNow tickets to determine whether backout plans were documented.</p> | No exceptions noted. |
| CC8.1.9 | <p>OS, Software and Infrastructure Change Management Policy and Procedures</p> <p>The process for upgrades and changes to operating system (OS), system software and infrastructure including network configuration files is controlled through a similar methodology used for application changes. The Clearing House Change Control Policy document provides requirements for change initiation, authorization, approval, bi-weekly Change Advisory Board meetings, and for implementing and closing a change request.</p> <p>New releases of system software from the software vendors and modifications to system software and infrastructure are implemented on the development system by the related Infrastructure team and reviewed by the Quality Control team in preparation for production release.</p> | <p>Inspected the Change Control Policy document to determine whether the document addressed procedures and requirements for change initiation, authorization, approval, bi-weekly Change Advisory Board meetings, and for implementing and closing a change request.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|-----------------------------|
| CC8.1.10 | <p>OS, Software and Infrastructure Change Upgrades/Change Initiation</p> <p>Upgrades/changes to the operating system, system software and infrastructure including network changes are authorized and prioritized based on the criticality of the system and follow the same processes and controls for application development and changes as described in CC8.1.3 Application, Program and Configuration Change Request Initiation and Authorization. Upgrades and changes are initiated, documented and authorized by management using ServiceNow.</p> | <p>For a selection of the operating system, system software and infrastructure changes/patches, inspected the related ServiceNow tickets to determine whether the change requests were documented and authorized as required.</p> | <p>No exceptions noted.</p> |
| CC8.1.11 | <p>OS, Software and Infrastructure Change Upgrade/Change Testing and Implementation</p> <p>Upgrades or changes to the operating system and system software are tested in the development environment or test servers by the support teams within the Infrastructure group. The nature of change dictates the requirement for QC testing and environment where testing takes place. Hardware changes do not require QC testing. The QC team reviews test results provided by the Support team and moves the software to the QC environment for independent testing.</p> <p>If the results of QC testing are satisfactory, the related ServiceNow ticket is routed to the Change Advisory Board for approval for installation in the production environment.</p> <p>The upgrades/changes are reviewed and approved in the bi-weekly Change Advisory Board meeting described in CC8.1.18.</p> <p>After the change is approved in the meeting, the Change Advisory Board updates the related ServiceNow ticket upon reviewing that the required approvals and implementation</p> | <p>Inquired of the Operation Services management regarding procedures and controls for the testing and implementation of OS and system software upgrades/changes.</p> <p>Inspected the system configuration to determine whether separate test and development environments existed.</p> <p>Please refer to CC8.1.18 Change Advisory Board Meetings for test of controls for the bi-weekly Change Advisory Board meeting.</p> <p>For a selection of operating system, system software and infrastructure changes/patches (regular and emergency), inspected the ServiceNow ticket and supporting documentation to determine whether:</p> <ul style="list-style-type: none"> The change was tested and the test results were approved by QC, if applicable, and Change Advisory Board prior to implementation in the production environment. | <p>No exceptions noted.</p> |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| | <p>information has been provided prior to installation in the production environment.</p> <p>Upgrades/changes are placed into the production environment by assigned implementers within the designated groups that are responsible for moving the implementing changes into the production environment.</p> | <ul style="list-style-type: none"> The ServiceNow ticket was assigned to implementers for moving the change into the production environment. | |
| CC8.1.12 | <p>Change Tracking</p> <p>ServiceNow is used to track the program development and changes throughout the cycle.</p> <p>Approval access in ServiceNow is granted to management members and designated authorized approvers who are responsible for approving the ServiceNow tickets.</p> <p>Controls related to access to ServiceNow are described in CC6.1.11 Access to ServiceNow and controls related to configuration changes to ServiceNow are described in CC8.1.3 Application, Program and Configuration Change Request Initiation and Authorization.</p> | <p>Inspected a selection of ServiceNow tickets to determine whether the tickets/reports provided status of each change and other elements related to the change such as description of the changes, assignment details and implementation date.</p> <p>Please refer to CC6.1.11 Access to ServiceNow for test results of access to ServiceNow and CC8.1.3 Application, Program and Configuration Change Request Initiation and Authorization for test results related to configuration changes to ServiceNow.</p> | No exceptions noted. |
| CC8.1.13 | <p>Access to the Production Environment</p> <p>Employees are granted access to the production environment and Control File based on their job responsibilities. Programmers do not have access to the production environment.</p> <p>Employees are granted access to the system files based on their job responsibilities. Logical access for the distributed environment is controlled by the security features of Active Directory. A valid user ID and password are required. Users are granted a level of access based on their job responsibilities. Administrative rights are restricted to authorized personnel based on their job responsibilities.</p> | <p>For a selection of mainframe servers and usercodes, inspected the Make User reports, a system generated security report for Unisys, and system-generated HR termination listings and inquired of management of the individuals' job responsibilities to determine whether programmers did not have access to the production environment and access to the Control File (Unisys) was limited to support teams and authorized management based on their job responsibilities.</p> <p>For a selection of servers, applications and databases in the distributed environment, inspected the users who were granted update access to the production environment (system administration</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| | TCH employs two levels of security over access to the RTP production environment. Server access is restricted by Windows Jump Server and for non-locally authenticated accounts, IBM Security Directory Server via LDAP. A valid user ID and password are required. Users are granted a level of access based on their job responsibilities. | capabilities), and system-generated HR termination listings and inquired of management of the individuals' job responsibilities to determine whether programmers did not have access to the production environment and access was limited to support teams and authorized management based on their job responsibilities. Observed personnel log into the RTP server environment and noted that access was restricted by Windows Jump Server and IBM LDAP, and for locally authenticated accounts that a valid user ID and password were required. | |
| CC8.1.14 | Network Database The Network group maintains a database of current network devices and configurations to facilitate network maintenance via SolarWinds. In addition, ServiceNow system scans all network subnets which also builds a device database. Network group management meets weekly to discuss needs for upgrades or changes in the network devices and configuration. | Inspected the network database, and ServiceNow system, to determine whether the inventory of network devices and related configuration was maintained to facilitate network maintenance. For a selection of weeks, inspected the network group management weekly calendar invite and meeting minutes to determine whether the group met to discuss needs for upgrades or changes in the network devices and configuration. | No exceptions noted. |
| CC8.1.15 | Network Management Procedures TCH has documented network management procedures which include network maintenance, managing the infrastructure and change management. Changes in the network components including hardware, software and configuration must follow TCH's change control procedures which include documentation, tests (where applicable depending on the nature of changes) and approval requirements using ServiceNow. Requests for network changes are documented in the related ServiceNow tickets. | Inspected the Network Architecture Technical Design document and Change Control Policy document to determine whether the documents addressed requirements for network maintenance and change management. For a selection of network changes, inspected the ServiceNow tickets to determine whether the tickets documented that changes in the network components were tested where required, approved and implemented. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| | <p>The network changes are reviewed and approved in the bi-weekly Change Advisory Board meeting described in CC8.1.18. After the change is approved in the meeting, Change Advisory Board updates the related ServiceNow ticket indicating approval for installation of changes the production environment. The changes are installed in the production environment by assigned individuals in the designated groups responsible for implement the change.</p> <p>Controls related to bi-weekly Change Advisory Board meeting are described in CC8.1.18 Change Advisory Board Meetings.</p> | Please refer to CC8.1.18 Change Advisory Board Meetings for test results of bi-weekly Change Advisory Board meeting. | |
| CC8.1.16 | <p>System Maintenance</p> <p>TCH management updates infrastructure, data, software, and policies and procedures as necessary. This includes patches, bug fixes, hardware upgrades, and software upgrades. Maintenance updates follow the change management controls as described in CC8.1.10 OS, Software and Infrastructure Change Upgrades/Change Initiation.</p> | <p>Inspected The Clearing House Change Control Policy document to determine whether it included patches, bug fixes, hardware upgrades, and software upgrades as maintenance updates.</p> <p>Refer to CC8.1.10 OS, Software and Infrastructure Change Upgrades/Change Initiation for test results of change management controls.</p> | No exceptions noted. |
| CC8.1.17 | <p>External Network Risk Assessment</p> <p>On an annual basis, assessments of external network risks are performed to identify potential impairments that could impact system security and availability. Critical, High and Medium findings are entered into Archer for tracking where a criticality based on severity and likelihood as well as a remediation plan is documented. Findings are remediated based on assigned criticality and may be remediated via the change management process as applicable.</p> <p>Controls related to entering, tracking and remediating findings within Archer are documented in CC3.2.1 Assessing Risk.</p> | Inspected the third-party external risk assessment summaries and Archer findings to determine whether identified vulnerabilities were remediated based on criticality. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC8.1.18 | <p>Change Advisory Board Meetings</p> <p>TCH holds a bi-weekly Change Advisory Board meeting to discuss changes, including environmental, regulatory and technological changes that affect system security and availability. Controls, policies and procedures are updated as needed based on the meeting discussions.</p> | <p>For a selection of weeks, inspected the change request report used in the bi-weekly Change Advisory Board meetings to determine whether changes, including environmental, regulatory and technological changes that affect system security and availability were discussed.</p> <p>Inquired of the VP of Information Security and VP of Operations Services and were informed that no updates were made to controls, policies, and procedures affecting security and availability during the period as a result of the Change Advisory Board meetings.</p> | No exceptions noted. |
| CC8.1.19 | <p>Enterprise Risk Management</p> <p>The Enterprise Risk Management department continually identifies, assesses, and monitors risks and reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities, risk assessments, Internal Audit findings, and Regulatory findings. These assessments include the identification and documentation of mitigating controls. If necessary, the change management process is initiated as a result of any findings.</p> | <p>Inspected the Enterprise Risk Management Framework document to determine whether procedures for risk identification, assessment, and monitoring, including roles and responsibilities, were documented.</p> <p>Inspected a selected RCSA assessment summary to determine whether the Enterprise Risk Management department identified, assessed, and monitored risks, reassessed the suitability of the design and implementation of control activities, and identified and documented mitigating controls as a result of any findings.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC8.1.20 | <p>Intrusion Detection System</p> <p>The TCH networks include an Intrusion Detection System (IDS), CarbonBlack. This system detects and classifies suspicious events according to a library of signatures provide by the vendor. The IDS/IPS is programmed to send alerts when thresholds for particular attack signatures are exceeded. Information Security management are alerted of intrusion activities. Incidents noted are recorded in ArcSight and depending on the nature and type of problem, the incident is escalated to the designated group for follow-up and resolution. If necessary, corrective action is taken via updates to policies and/or the change management process due to the alerts.</p> <p>CarbonBlack is configured to generate alerts through ArcSight.</p> <p>Controls related incidents analysis and resolution are documented in CC7.4.4 Security Administration and Security Violations.</p> | <p>For a selection of servers, inspected the CarbonBlack management console to determine whether CarbonBlack was configured to monitor traffic.</p> <p>For a selection of incidents, inspected tickets and supporting documentation to determine whether the incident was escalated and resolved.</p> <p>Inspected configured threat intelligence library in CarbonBlack to determine whether the system was configured to detect and classify events according to the signatures.</p> <p>Inspected ArcSight management console to determine whether ArcSight was configured to alert Information Security in case of potential threats.</p> <p>Inspected the list of users with administrator access to CarbonBlack, job titles, and inquired of the management to determine whether administrative access to CarbonBlack was restricted to authorized personnel.</p> <p>Inquired of Information Security management regarding policy and process updates and were informed corrective action was taken via updates to policies and/or the change management process due to the alerts.</p> <p>Refer to CC7.4.4 Security Administration and Security Violations for test results of incident analysis and resolution for ArcSight.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|----------------------|
| CC8.1.21 | <p>System Components Inventory</p> <p>ServiceNow is used to provide a single system of record for system components and supports management of IT Asset and Configuration Items. The Asset Management module within ServiceNow is used to manage asset information for IT Assets throughout its lifecycle from request to disposal and aids in determining criticality of the asset. Service Catalog workflows in ServiceNow are used to support the procurement, receive and retirement of IT Assets. TCH also uses the Configuration Management Database (CMDB) in ServiceNow to manage configuration items throughout its lifecycle from operational to out of service. Maintaining the Asset Management module allows an inventory of assets which is used in threat management. To keep configuration items up to date in the CMDB, ServiceNow Discovery is used to automate CI population into the CMDB. ServiceNow Discovery uses conventional techniques and technology to extract information from computers and other devices.</p> | <p>Inspected the CMDB configuration to determine whether IT assets were managed throughout their lifecycle.</p> <p>Inspected the ServiceNow discovery IP range list and discovery schedule list to determine whether IT servers and IT assets were tracked.</p> <p>Refer to CC7.1.9 for testing over the new IT asset discovery.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| CC8.1.22 | <p>Server Hardening</p> <p>TCH provides hardening standards for system administrators in order to implement secure server configurations within the company's infrastructure. The guidelines are reviewed and updated when changes occur by the Information Security team.</p> <p>Monthly validation of compliance to hardening standards occurs through the use of BigFix. Weekly meetings are held to discuss compliance results, and if necessary, tickets are created for remediation or a policy exception is documented in Archer.</p> | <p>Inspected the hardening guidelines to determine whether they document approved hardening standards for server configurations.</p> <p>For a selection of months, inspected monthly compliance report to determine whether compliance checks were performed to ensure devices were hardened per defined standards.</p> <p>For a selection of weeks, inspected the compliance meeting invite and notes to determine whether compliance results were discussed, and if necessary, tickets were created for remediation of any noted issues or a policy exception was documented in Archer.</p> | No exceptions noted. |
| CC8.1.23 | <p>Code Requirements - RTP</p> <p>Code requirements for RTP development work are provided to the third-party developer as part of the business requirement documentation. QC performs testing on the developed code to confirm requirements are met.</p> | <p>For a selection of RTP changes, inspected ServiceNow tickets, and testing documentation to determine whether code requirements were documented as part of business requirements and QC testing was performed to confirm requirements were met.</p> | No exceptions noted. |
| CC8.1.24 | <p>Patch Management</p> <p>TCH's Vulnerability Management procedural document includes patch management. As part of patch management, the Patch and Vulnerability Management Group (PVG) meets weekly to discuss patch availability, testing, implementation and planning, as well as emerging threats, critical vulnerabilities, patching and vulnerability management processes, current metrics, trending metrics, PCI requirements and other topics as appropriate.</p> | <p>Inspect Vulnerability Management procedural document to determine the patch management process was defined.</p> <p>For a selection of weeks, inspected the Patch and Vulnerability (PVG) weekly meeting invites and agendas to determine whether the patch management availability, testing, implementation and planning was discussed.</p> <p>Refer to CC8.1.11 OS, Software and Infrastructure Change Upgrade/Change Testing and Implementation for test over patching as part of the change management process.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|---|---|-------------------------|------------------|
| Complementary User Entity Control(s) | | | |
| <p>Controls should be established at user entities so that:</p> <ul style="list-style-type: none"> • Users perform testing for all network changes that require user testing and promptly notify TCH of the test results. • Optional customer testing is performed for each release depending on the extent and nature of the change. • Router changes that require user testing are tested and TCH is promptly notified of the test results. • Full certification testing is complete any time changes are made to the RTP interface or the message specifications, optional repeat of certification testing whenever customers make changes to their application. | | | |

CC 9.0 – Common criteria related to risk mitigation

CC9.1 – The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| CC9.1.1 | <p>Risk Meetings</p> <p>At a minimum, TCH holds quarterly risk meetings with the Enterprise Risk Management Committee (ERMC) and Enterprise Risk Committee (ERC) to discuss potential security and availability risks including evaluating security events, environmental threats, network usage and system capacity, and risks not properly mitigated from the prior quarter. ERM is responsible for reporting risks and issues to provide transparency and escalation. Objectives are captured during these meetings and incorporated into the ongoing risk assessment process. If necessary, the change management process is initiated due to the risks discussed.</p> | <p>For a selection of quarters, inspected risk meeting minutes to determine whether risk meetings were held with the Risk Management Committee (ERMC) and Enterprise Risk Committee (ERC), security and availability risks were discussed (including security events, environmental threats, network usage and system capacity, and risks not properly mitigated), objectives were captured, and if necessary, the change management process was initiated due to the risks.</p> <p>Inspected the ERM framework to determine whether ERM is responsible for reporting risks and issues.</p> | No exceptions noted. |
| CC9.1.2 | <p>Enterprise Risk Management</p> <p>The Enterprise Risk Management department continually identifies, assesses, and monitors risks and reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities, risk assessments, Internal Audit findings, and Regulatory findings. These assessments include the identification and documentation of mitigating controls. If necessary, the change management process is initiated as a result of any findings.</p> | <p>Inspected the Enterprise Risk Management Framework document to determine whether procedures for risk identification, assessment, and monitoring, including roles and responsibilities, were documented.</p> <p>Inspected a selected RCSA assessment summary to determine whether the Enterprise Risk Management department identified, assessed, and monitored risks, reassessed the suitability of the design and implementation of control activities, and identified and documented mitigating controls as a result of any findings.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC9.1.3 | Insurance Coverage Insurance for corporate level incidents includes coverage related to property, directors and officers, and computer crime. | Inspected the certificate of liability insurance to determine whether TCH had insurance coverage. | No exceptions noted. |
| CC9.1.4 | Business Continuity Plan TCH has established a Business Continuity Program to provide capabilities, information, and training to ensure that employees are prepared for any interruption and know what to do in the event of an interruption incident at any of the TCH sites. The TCH Enterprise Risk Management Framework document and Business Continuity Management policy define roles and responsibilities for business continuity and disaster recovery plan development and maintenance, identify procedures to facilitate plan development, establish a review and approval process for business continuity plans, specify requirements for plan ownership, and provide requirements and frequency for plan test. | Inspected the TCH Enterprise Risk Management Framework and Business Continuity Management Policy documents, and recent business continuity plan tests to determine whether roles and responsibilities for business continuity and disaster recovery plan development and maintenance were defined, procedures to facilitate plan development were identified, a review and approval process for business continuity plans was established, requirements for plan ownership were specified, and requirements and frequency for plan test were provided. Inspected the business continuity plans to determine whether a review and approval process was established. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC9.1.5 | <p>Disaster Recovery Plan</p> <p>Disaster Recovery plans are maintained and updated at least annually by all respective business unit managers/application owners, who are also responsible for providing the Disaster Recovery training to their team members, in order to address disaster risk. All Disaster Recovery plans must address strategies to achieve recovery time objective (RTO) and recovery point objective (RPO).</p> <p>IT Service Continuity Management performs Disaster Recovery testing at least once per year. Testing follows the Disaster Recovery plan and includes a failover to the alternate hosting sites. Results are documented and risks are assessed to improve/update the Disaster Recovery plan.</p> | <p>Inspected the plans to determine whether a review and approval process was established.</p> <p>Inspected the Business Continuity Management policy to determine whether it documented roles and requirements for maintenance and review of the Disaster Recovery plans, training, and addressing RTO and RPO strategies were established to address disaster risk.</p> <p>Inspected the annual Disaster Recovery testing results and Disaster Recovery Plan to determine whether the testing followed the Disaster Recovery Plan, results were officially documented and the Disaster Recovery Plan was updated to address identified risks.</p> | No exceptions noted. |

CC9.2 – The entity assesses and manages risks associated with vendors and business partners.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| CC9.2.1 | <p>Subservice Organization Agreements</p> <p>TCH maintains agreements established between TCH and subservice organizations that outline security and availability commitments, as well as the subservice organizations' responsibilities. These agreements are reviewed and approved by TCH and the organizations upon establishment. Updates and modifications to contracts and commitments are assessed as part of the contract management and vendor risk assessment process.</p> <p>Controls related to vendor risk assessment are described in CC9.2.3 Vendor Risk Management.</p> | <p>Inquired of Vendor Management and were informed that there were no new subservice organization agreements during the period; therefore, the operating effectiveness of this part of the control could not be tested.</p> <p>For a selection of existing subservice organizations, inspected the agreements to determine whether they were maintained by TCH.</p> | No exceptions noted. |
| CC9.2.2 | <p>Confidentiality Agreements and Information Handling Requirements</p> <p>TCH Legal review contracts with confidentiality obligations or information handling requirements to ensure the obligations imposed are consistent with existing practices and policies.</p> | <p>Inspected the Contract Authority Policy to determine whether legal review requirements were outlined.</p> | No exceptions noted. |
| CC9.2.3 | <p>Vendor Risk Management</p> <p>In accordance with ERM Framework, potential and existing vendor services must undergo the vendor management process which includes an onboarding risk assessment, evaluation of controls, and review over SOC reports, when available. Vendor Management performs risk assessments on specific tiered vendors on a recurring basis. Vendor Management is responsible for assigning a Vendor Impact Tier based on the vendor's commercial relevance and potential impact on core products and strategic initiatives. These tiers correlate to the vendor's inherent risk level, as defined by the Enterprise Risk Management Framework. Impact Tiers and risk assessment frequency include:</p> | <p>Inspected the ERM Framework to determine whether Vendor Risk Management procedures were established.</p> <p>For a selection of third-party vendors, inspected the Vendor Risk Assessments to determine whether risk assessments were completed on a recurring basis per specified tier and included evaluation of controls and review over SOC reports when available.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|----------------------|
| | 1. Critical – On-boarding and Annually 2. Very High – On-boarding and Annually 3. High – On-boarding and 18 months 4. Medium – On-boarding and Biennial 5. Low – On-boarding or Service Change and Biennial if categorized as SaaS | | |
| CC9.2.4 | Service Level Agreements and Monitoring Vendor Management and Information Security work with Vendor Relationship Owners (VROs) to monitor SLAs and performance standards via monthly performance scorecards and recurring risk assessments. | For a selection of vendors and a selection of months, inspected vendor risk assessments and performance scorecards to determine whether SLAs and performance standards were monitored for vendors. | No exceptions noted. |

Additional criteria for availability

A1.1 – The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|--|----------------------|
| A1.1.1 | <p>Capacity Management</p> <p>TCH's Communication and Operations Management policy documents established procedures for capacity management including TCH resources are to be monitored, tuned, and capacity projections made for future capacity requirements to ensure system performance.</p> <p>Controls related to the monitoring over capacity are described in A1.1.4 Utilization, Capacity Monitoring and Forecasting.</p> | Inspected the IS Communication and Operations Management policy to determine whether the document addressed procedures and requirements for capacity management. | No exceptions noted. |
| A1.1.2 | <p>Availability Monitoring</p> <p>TCH utilizes third-party tools to monitor performance, memory and disk space in the distributed systems environment to help ensure systems are fully functional. Automated email alerts are sent to operations management in the event of capacity and availability issues, risks are analyzed and appropriate corrective action is taken.</p> | <p>Inspected the monitoring tool configurations and an email notification and noted the tool was configured to distribute automated email alerts to Network Operations based on established performance rules and thresholds.</p> <p>Refer to CC7.4.3 Problems Reporting and Tracking for test results of incident reporting and tracking within ServiceNow.</p> | No exceptions noted. |
| A1.1.3 | <p>System Availability Metrics</p> <p>System availability and network usage by system are tracked, summarized and reported in the monthly management report. For any breached threshold over application uptime, a ServiceNow ticket is escalated to the designated group for follow-up and resolution. Once an incident is resolved, the ticket is closed.</p> | For a selection of months, inspected the monthly management reports to determine whether the systems and network statistics were tracked and summarized to management and for breached thresholds, if any, inspected the ServiceNow ticket to determine whether the issue was escalated to the designated group for follow-up and resolution, and ticket was closed. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| A1.1.4 | <p>Utilization, Capacity Monitoring and Forecasting</p> <p>TCH network team has tools which continuously monitor the network for utilization and capacity management. Monthly metrics are reviewed for capacity trends and utilized for capacity forecasting. If additional capacity needs result in a change to the system the standard change management process is followed.</p> | <p>Inspected the network monitoring tool dashboard to determine whether the network was continuously monitored for utilization, capacity and forecasting, as needed.</p> <p>For a selection of months, inspected the monthly management reports to determine whether the capacity trends were tracked and summarized to management.</p> <p>Inquired of management and were informed that the management reports are used for capacity forecasting.</p> <p>Please refer to CC8.1.10 OS, Software and Infrastructure Change Upgrades/Change Initiation for results of testing related changes resulting from additional capacity needs.</p> | No exceptions noted. |
| A1.1.5 | <p>Risk Meetings</p> <p>At a minimum, TCH holds quarterly risk meetings with the Enterprise Risk Management Committee (ERMC) and Enterprise Risk Committee (ERC) to discuss potential security and availability risks including evaluating security events, environmental threats, network usage and system capacity, and risks not properly mitigated from the prior quarter. ERM is responsible for reporting risks and issues to provide transparency and escalation. Objectives are captured during these meetings and incorporated into the ongoing risk assessment process. If necessary, the change management process is initiated due to the risks discussed.</p> | <p>For a selection of quarters, inspected risk meeting minutes to determine whether risk meetings were held with the Risk Management Committee (ERMC) and Enterprise Risk Committee (ERC), security and availability risks were discussed (including security events, environmental threats, network usage and system capacity, and risks not properly mitigated), objectives were captured, and if necessary, the change management process was initiated due to the risks.</p> <p>Inspected the ERM framework to determine whether ERM is responsible for reporting risks and issues.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| A1.1.6 | <p>Checkactive Disk Monitoring (CHIPS and EPN)</p> <p>The Checkactive program, an internally-developed program, is automatically executed periodically in the mainframe environment throughout the day based on schedules to monitor disk usage. An alert message for a mismatch condition is sent to the Network Operations console. Network Operations follows up and resolves the mismatched condition. The alert message for a mismatch condition is displayed on the Network Operations console until the mismatch is resolved. A ServiceNow ticket is escalated to the designated group for follow-up and resolution. Once the mismatch is resolved, the ticket is closed.</p> | <p>Inspected the configuration of the Checkactive program to determine whether the program was automatically processed based on schedules to monitor disk usage.</p> <p>Inspected an alert message for a Checkactive mismatch condition to determine whether the alert was generated automatically.</p> | No exceptions noted. |
| A1.1.7 | <p>Uptime Commitments</p> <p>The Network Operations Center (NOC) performs system availability monitoring using automated tools including SCOM and SolarWinds. These tools detect anomalies affecting system uptime and performance and alert operators to such conditions. Network Operations receive the alerts and open incidents in SNAP to triage, and may notify additional support teams to address the issue if necessary. Any incident causing actual downtime is rated a Severity 1 or 2 incident, and the duration is managed and reported. On a monthly basis, Network Operations calculates overall system uptime based on Severity 1 and 2 tickets impacting production, and reports as a key metrics to TCH management.</p> <p>Controls related to the monthly reporting of uptime and availability are documented in A1.1.3 System Availability Metrics.</p> | <p>Inspected SCOM configurations and associated alerts to determine whether Network Operations were notified of uptime and performance issues requiring investigation.</p> <p>Inspected the network monitoring tool dashboard to determine whether the network was continuously monitored for utilization, capacity and forecasting, as needed.</p> <p>For a selection of months, inspected the monthly management reports to determine whether system uptime was tracked and summarized to management.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| A1.1.8 | <p>Load Balancing</p> <p>The application and network infrastructure employs load balancing and redundancy to eliminate "single points of failure". The network infrastructure has been built with full redundancy at both data centers including the communications at all customer locations. This also includes all firewalls deployed within the infrastructure, which are built as an active/standby cluster. For RTP, the application runs "active-active" in the PA and NC data centers. In addition, within each data center, all components are clustered and redundant, providing both intra-site and inter-site redundancy. In the event of a server or site outage, RTP will continue processing payments on the remaining servers or site.</p> <p>Furthermore, all network devices are monitored via SolarWinds, this includes devices, interfaces, health conditions and capacity. SolarWinds also provides a weekly capacity report which provides future capacity forecasting on memory, CPU, interface utilization and disk usage.</p> | <p>Inspected the network database in SolarWinds, report schedule configuration and a selected capacity report to determine whether devices, interfaces, health conditions and capacity was monitored.</p> <p><i>EPN, CHIPS, and IXN</i></p> <p>Inspected system configurations and the annual failover tests, and inquired of management to determine whether EPN, CHIPS, and IXN employed load balancing and redundancy with intra and inter-site redundancy.</p> <p><i>RTP</i></p> <p>Inspected system and server processing configurations, and annual failover test, and inquired of management to determine whether RTP was configured to run active-active in the NC and PA data centers with intra and inter-site redundancy and in the event of a site outage, would continue processing on the alternate site.</p> | No exceptions noted. |

A1.2 – The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| A1.2.1 | <p>Environmental Control Systems Maintenance</p> <p>Environmental control systems are maintained based on schedules to help determine that they are functioning as intended.</p> <p>Environmental system maintenance controls for the Pennsylvania data center are managed and performed by Iron Mountain and are not in scope of this report.</p> | Inspected the facilities maintenance and service reports for fire protection, UPS, generator, and CRAC/HVAC systems to determine whether environmental control systems devices were maintained based on schedules. | No exceptions noted. |
| A1.2.2 | <p>Environmental Control System Monitoring</p> <p>Environmental control systems for the data center are monitored by the Network Operations Centers.</p> <p>The Operator Schedules for the North Carolina Operations Center is completed to document the completion of the environment control system monitoring tasks.</p> <p>For the Pennsylvania data center managed by Iron Mountain, Corporate Real Estate and Corporate Security review environmental SLA requirements for a facility as a whole on a monthly basis.</p> | <p>For a selection of dates, inspected the Operator Schedules for the North Carolina Operations Centers to determine whether the operations staff signed off their results of monitoring the environmental control systems.</p> <p>For a selection of months, inspected the environmental SLA requirements reviewed performed by the Corporate Real Estate and Corporate Security group to determine whether Pennsylvania environmental were monitored.</p> | No exceptions noted. |
| A1.2.3 | <p>Network Redundancy</p> <p>Telecommunications services are provided by two network hubs, AT&T and CenturyLink, in order to provide network redundancy.</p> | Inspected network diagrams to determine whether the network design included network redundancy provided by AT&T and CenturyLink. | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|-----------------------------|
| A1.2.4 | <p>Data Center and Computer Room Architecture</p> <p>The North Carolina computer facility (data center) is the primary processing site for EPN, CHIPS and IXN and the Pennsylvania data center serves as a backup processing site. The North Carolina facilities are equipped with uninterruptible power supply (UPS) systems, dual diesel generators, fire protection systems, and hardware and software sufficient to operate all the production systems concurrently.</p> <p>Environmental controls for the Pennsylvania data center as a facility are managed and performed by Iron Mountain and are not in scope of this report.</p> <p>RTP runs “active-active” in the North Carolina and Pennsylvania data center (which is managed and controlled by Iron Mountain).</p> | <p>Toured the North Carolina data center and observed that UPS devices, diesel generators, and heat and smoke detecting devices were installed at the data centers.</p> | <p>No exceptions noted.</p> |
| A1.2.5 | <p>Online Backups</p> <p>For EPN, CHIPS and RTP, records are written from the active database system to the local standby database in North Carolina and routed to the remote database system in Pennsylvania through the use of leased lines that allow file operations to occur between local and remote hosts. All files associated with a given processing cycle are updated and mirrored real time at both data centers. RTP transactions are written on the database locally and replicated to the remote stand by systems as they are committed into active database. Database transactions associated with RTP are updated simultaneously at both data centers. Online replication activities are monitored by Network Operations as documented in the Operator Schedules. Any issues are followed up and resolved.</p> | <p>Inspected the network diagrams to determine whether the design included Optical Point-to-Point leased lines between the North Carolina and Pennsylvania data centers.</p> <p>Inspected the system disk pack configuration to determine whether EPN and CHIPS application files were written on internal mirror packs locally and on remote backup packs.</p> <p>Inspected the system replication configurations to determine whether RTP records were configured to write from active to local standby hosts.</p> <p>For a selection of dates, inspected the Operator Schedules to determine whether the online backup activities were monitored and noted no backup issues in the online backup activities recorded on the schedules for the selected dates.</p> | <p>No exceptions noted.</p> |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| | | Please refer to CC7.4.3 Problems Reporting and Tracking for test results of problem reporting and tracking of backup failures. | |
| A1.2.6 | <p>LiteSpeed Backup - IXN</p> <p>SQL database backups occur daily at 6 a.m. and are written locally by LiteSpeed. Two days' worth of backups are retained. Transaction log backups are also written to locally every hour. The results of the backups, including any issues, are communicated to the DBA group via email. ServiceNow tickets are opened to resolve any issues noted.</p> <p>Refer to CC7.4.3 Problems Reporting and Tracking for incident management testing.</p> | <p>Inspected the backup schedule to determine whether backups were configured to occur daily at 6 a.m.</p> <p>Inspected the SQL backup logs to determine whether the SQL backups were performed in accordance within the backup schedules.</p> <p>Please refer to CC6.1.8 Administrator Access - Distributed Environment for results of testing related to access to SQL database.</p> | No exceptions noted. |
| A1.2.7 | <p>Avamar Backups - IXN</p> <p>Full Avamar backups occur daily and replicates the data to Pennsylvania and North Carolina data centers. Avamar backups are retained based upon a predefined schedule. The results of the backups, including any issues, are communicated to the Network Operations. ServiceNow tickets are opened to resolve any issues noted.</p> <p>Refer to CC7.4.3 Problems Reporting and Tracking for incident management testing.</p> | <p>For a selection of dates, inspected the Avamar backup tape logs to determine whether the Avamar backups were performed in accordance within the backup schedules.</p> <p>Inspected the replication schedule configuration and selected replication log to determine whether the Avamar backups replicate to the alternate data centers.</p> <p>Inspected the list of users with administrator access to Avamar job titles, and inquired of the management to determine whether administrative access to Avamar was restricted to authorized personnel.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|---|----------------------|
| A1.2.8 | <p>Virtual Tape Library</p> <p>Databases for EPN and CHIPS are backed up onto a virtual tape library (VTL) based on an automatic or manual schedule. BL Library (BL LIB), a tape management library system, is used to facilitate this process. Backup activities are monitored online by Network Operations as documented in the Operator Schedules. The tape management library system logs backup activities in the System Logged Tapes. Backup issues, if any, are followed up and resolved and recorded in a ServiceNow incident ticket.</p> <p>The PA data center is monitored and managed by North Carolina and the New York Operations Centers.</p> | <p>Observed Network Operations monitor the backup activities online through the computer operator console and the System Logged Tapes to determine whether the systems and databases were backed up onto virtual tape library.</p> <p>For a selection of dates, inspected the System Logged Tapes log to determine whether backups were completed.</p> <p>For a selection of dates, inspected the Operator Schedule for the North Carolina and New York Operations Centers to determine whether backup activities were monitored online by the Network Operations and noted no backup issues in the backup activities recorded on the Operator Schedule available for inspection.</p> <p>Please refer to CC7.4.3 Problems Reporting and Tracking for test results of problem reporting and tracking of backup failures.</p> | No exceptions noted. |
| A1.2.9 | <p>Database Backups - RTP</p> <p>RTP database environments are backed up daily using native DB2 shells scripts with 3 days of backups maintained locally on the file system including transaction logs. Backup images are archived using the Avamar system. The results of the backups, including any issues, are communicated to the DBA group via email notifications. ServiceNow tickets are opened to follow up and resolve backup issues.</p> | <p>Inspected the database backup configuration to determine whether the RTP databases were configured to backup per schedule and retain 3 days of backups locally.</p> <p>For a selection of databases and dates, inspected the database backup logs to determine whether backups completed successfully per schedule, and noted no backup issues were recorded for the selected dates.</p> <p>Please refer to CC7.4.3 Problems Reporting and Tracking for test results of problem reporting and tracking of backup failures.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|---|---|----------------------|
| A1.2.10 | Server Backups - RTP All servers are backed up by Avamar (for AIX servers) and Networker (for RHEL servers) at both North Carolina and Pennsylvania data centers. A backup storage system is used to facilitate this process. The backup management system logs backup activities and any backup issues are followed up and resolved within a ServiceNow Incident ticket. Transaction data/logs are backed-up and retained for 90 days. | <p>Inspected the server backup configuration to determine whether the RTP servers were configured to backup per schedule.</p> <p>For a selection of servers and dates, inspected the server backup logs to determine whether backups completed successfully per schedule, and noted no backup issues were recorded for the selected dates.</p> <p>Please refer to CC7.4.3 Problems Reporting and Tracking for test results of problem reporting and tracking of backup failures.</p> | No exceptions noted. |
| A1.2.11 | Network Connectivity to Recovery Site The network infrastructure is built to mirror each other at both data centers. The network infrastructure is built to allow the application to run as active/active. It also allows for site isolation if needed. | <p>Inspected the network diagrams to determine whether the design of the network at both data centers was mirrored and built to run active/active and included redundancy, routers and firewalls.</p> | No exceptions noted. |
| A1.2.12 | Uptime Commitments The Network Operations Center (NOC) performs system availability monitoring using automated tools including SCOM and SolarWinds. These tools detect anomalies affecting system uptime and performance and alert operators to such conditions. Network Operations receive the alerts and open incidents in SNAP to triage, and may notify additional support teams to address the issue if necessary. Any incident causing actual downtime is rated a Severity 1 or 2 incident, and the duration is managed and reported. On a monthly basis, Network Operations calculates overall system uptime based on Severity 1 and 2 tickets impacting production, and reports as a key metrics to TCH management. | <p>Inspected SCOM configurations and associated alerts to determine whether Network Operations were notified of uptime and performance issues requiring investigation.</p> <p>Inspected the network monitoring tool dashboard to determine whether the network was continuously monitored for utilization, capacity and forecasting, as needed.</p> <p>For a selection of months, inspected the monthly management reports to determine whether system uptime was tracked and summarized to management.</p> | No exceptions noted. |

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|---|--|-------------------------|------------------|
| | Controls related to the monthly reporting of uptime and availability are documented in A1.1.3 System Availability Metrics. | | |
| Complementary User Entity Control(s) | | | |
| <p>Controls should be established at user entities so that:</p> <ul style="list-style-type: none"> • Users maintain active connections from their primary data center to both TCH data centers and to be able to send and receive payment messages to/from both data centers simultaneously. Customers maintain connectivity from their disaster recover/backup data centers to both TCH data centers. • Users notify TCH of outages. | | | |

A1.3 – The entity tests recovery plan procedures supporting system recovery to meet its objectives.

| Control # | Controls Specified by The Clearing House Payments Company, L.L.C. | Tests performed by KPMG | Results of tests |
|-----------|--|--|----------------------|
| A1.3.1 | <p>Business Continuity Plan</p> <p>TCH has established a Business Continuity Program to provide capabilities, information, and training to ensure that employees are prepared for any interruption and know what to do in the event of an interruption incident at any of the TCH sites. The TCH Enterprise Risk Management Framework document and Business Continuity Management policy define roles and responsibilities for business continuity and disaster recovery plan development and maintenance, identify procedures to facilitate plan development, establish a review and approval process for business continuity plans, specify requirements for plan ownership, and provide requirements and frequency for plan test.</p> | <p>Inspected the TCH Enterprise Risk Management Framework and Business Continuity Management Policy documents, and recent business continuity plan tests to determine whether roles and responsibilities for business continuity and disaster recovery plan development and maintenance were defined, procedures to facilitate plan development were identified, a review and approval process for business continuity plans was established, requirements for plan ownership were specified, and requirements and frequency for plan test were provided.</p> <p>Inspected the business continuity plans to determine whether a review and approval process was established.</p> | No exceptions noted. |
| A1.3.2 | <p>Disaster Recovery Plan</p> <p>Disaster Recovery plans are maintained and updated at least annually by all respective business unit managers/application owners, who are also responsible for providing the Disaster Recovery training to their team members, in order to address disaster risk. All Disaster Recovery plans must address strategies to achieve recovery time objective (RTO) and recovery point objective (RPO).</p> <p>IT Service Continuity Management performs Disaster Recovery testing at least once per year. Testing follows the Disaster Recovery plan and includes a failover to the alternate hosting sites. Results are documented and risks are assessed to improve/update the Disaster Recovery plan.</p> | <p>Inspected the plans to determine whether a review and approval process was established.</p> <p>Inspected the Business Continuity Management policy to determine whether it documented roles and requirements for maintenance and review of the Disaster Recovery plans, training, and addressing RTO and RPO strategies were established to address disaster risk.</p> <p>Inspected the annual Disaster Recovery testing results and Disaster Recovery Plan to determine whether the testing followed the Disaster Recovery Plan, results were officially documented and the Disaster Recovery Plan was updated to address identified risks.</p> | No exceptions noted. |

Section V Other
information provided by
The Clearing House
Payments Company L.L.C.

Management responses to exceptions

| Control # | Controls specified by The Clearing House Payments Company, L.L.C. | Exceptions noted | Management responses |
|---------------------|---|---|---|
| CC6.1.3, CC6.6.1 | <p>Security Configuration - Mainframe</p> <p>Access to the Unisys production environment and development environment is controlled by the Unisys MCP operating system and the Unisys InfoGuard access control package. MCP allows programs and users access only to defined computer resources. InfoGuard is a software package which provides logical security options beyond that provided by the MCP operating system. Hardening guidelines for the security configuration of the Unisys MCP operating systems are documented and implemented within the system.</p> <p>TCH has implemented the following security rules in the production environments per the Unisys MCP hardening standard:</p> <ul style="list-style-type: none"> Employee individual accesscode and group usercode passwords must meet a minimum length requirement. Employee individual accesscode and group usercode passwords must be changed at specified intervals. | <p>Exceptions Noted:</p> <p>Individual accesscodes</p> <ul style="list-style-type: none"> For 2 out of 120 individual accesscodes selected, the minimum password length was not set. For 25 of 120 individual accesscodes selected, the password was not set to expire. For 25 of 120 individual accesscodes selected, the password history was not set. For 116 of 120 individual accesscodes selected, the password lockout setting was set; however, it was not in accordance with TCH policy requirements. For 4 of 120 individual accesscodes selected, the password lockout setting was not set. <p>Group usercodes</p> <ul style="list-style-type: none"> For 1 of 40 group usercodes selected, the minimum password length was set; however, it was not in accordance with TCH policy requirements. | <p>Preceding compensating controls exists within the environment that require users to authenticate to Active Directory prior to gaining access to Mainframe systems. Active Directory passwords do expire and meet all policy-based password security requirements. No access to the Mainframe is possible without first passing those preceding controls. Mainframe authentication requires the use of dual controls, one of which is known to a group of users (usercode) and one known only to the individual (accesscode).</p> |

| Control # | Controls specified by The Clearing House Payments Company, L.L.C. | Exceptions noted | Management responses |
|-----------|---|---|----------------------|
| | <ul style="list-style-type: none"> Employee individual accesscode and group usercode passwords must be different from a certain number of passwords previously used (password history). Employee individual usercodes (with and without accesscodes) are suspended after a specified number of violations per day. Terminals are disabled after a number of invalid access attempts within certain duration of time. | <ul style="list-style-type: none"> For 13 of 40 group usercodes selected, the password was not set to expire. For 19 of 40 group usercodes selected, the password history was not set. For 39 of 40 group usercodes selected, the password lockout setting was set; however, it was not in accordance with TCH policy requirements. For 1 of 40 group usercodes selected, the password lockout setting was not set. | |

| Control # | Controls specified by The Clearing House Payments Company, L.L.C. | Exceptions noted | Management responses |
|---------------------|--|---|---|
| CC6.1.4, CC6.6.2 | <p>Security Rules - Distributed</p> <p>TCH has implemented the following security rules for the servers, applications and databases in the distributed environment:</p> <ul style="list-style-type: none"> • A user ID and password are required. Passwords must be changed at specified interval. • Passwords must meet a minimum length requirement. • New passwords must be different from a certain number of passwords previously used. • User IDs are disabled after a number of invalid access attempts within certain duration of time. | <p>Exceptions Noted:</p> <p>Windows Databases:</p> <p>Noted that management had identified local database accounts where password rules were not enforced per TCH policy.</p> <p>Linux Servers:</p> <p>Password parameter settings for local server accounts were configured, however, not established in accordance with TCH policy; per TCH policy minimum password length required is 15 characters, however, configuration was set to 8 characters.</p> | <p>Windows Databases</p> <p>Preceding compensating controls exists within the environment that require users to authenticate to Active Directory prior to gaining access to the noted local database accounts. Remote access requires users go through multi-factor authentication to connect to the network requiring valid TCH domain credentials and authentication via a RSA remote access token and a user PIN. Management and Information Security have documented policy exceptions.</p> <p>Linux Servers</p> <p>Preceding compensating controls exist within the environment that require users to authenticate using multi-factor authentication (pin and token) to gain access to a jump server, allowing access to the environment. TCH will review configuration settings for in-scope servers and assess opportunities to improve adherence to policy.</p> |