# Q2 Software, Inc.

# Platform (Online Banking)

System and Organization Controls Report

Report on Controls Placed in Operation and Tests of Operating Effectiveness

For the Period

October 1, 2019, to September 30, 2020

**Q2.com**

Q2

# Contents


I. Independent Service Auditor's Report ..... 1

II. Q2 Software, Inc.'s Assertion ..... 4

III. Description of Q2 Software, Inc.'s Online Banking System ..... 6

Overview of Operations and Processing Environment ..... 6

Scope of Report ..... 6

Relevant Aspects of the Control Environment, Risk Assessment and Monitoring Activities ..... 9

Control Environment ..... 9

*Personnel Practices and Policies* ..... 10

Risk Assessment ..... 10

Monitoring Activities ..... 11

General Computer Controls ..... 11

Computer Operations ..... 11

Access Controls ..... 12

Q2Online Authentication Controls ..... 13

Q2Central Authentication Controls ..... 13

PIQs Security ..... 14

ETMS Security ..... 14

DTS Security ..... 14

Application System Development and Maintenance ..... 15

Application and Control Processes ..... 19

Customer Implementation and Account Maintenance ..... 19

Customer Service ..... 20

Reporting ..... 21

Information Produced by Q2 Software ..... 21

Complementary User Entity Control Considerations ..... 23

IV. Q2 Software, Inc.'s Control Objectives and Related Controls and RSM US LLP's Tests of Controls and Results of Tests ..... 24

Computer Operations ..... 24

Logical Access ..... 28

Physical Access ..... 30

Change Management ..... 31

V. Other Information Provided by Q2 Software, Inc. ..... 35
Business Continuity Planning ..... 35
Q2 consoles ..... 36
Q2 Software, Inc. Informational Documents ..... 36
Management Responses to Testing Exceptions ..... 37

# I. Independent Service Auditor's Report

RSM US LLP

To Management of Q2 Software, Inc.:

*Scope*

We have examined Q2 Software, Inc.'s description of its information technology controls for the Online Banking system, titled "Description of Q2 Software, Inc.'s Online Banking System," (the description) for processing user entities' transactions throughout the period October 1, 2019, to September 30, 2020, and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "Q2 Software, Inc.'s Assertion" (the "assertion"). The controls and control objectives included in the description are those that management of Q2 Software, Inc. believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the information technology controls for the online banking system that are not likely to be relevant to user entities' internal control over financial reporting.

The information included in Section V, titled "Other Information Provided by Q2 Software, Inc.," is presented by management of Q2 Software, Inc. to provide additional information and is not a part of Q2 Software, Inc.'s description of its information technology controls for the online banking system made available to user entities during the period October 1, 2019, to September 30, 2020. Information about Q2 Software, Inc.'s Q2 consoles, information documents and management responses to testing exceptions has not been subjected to the procedures applied in the examination of the description of the information technology controls for the online banking system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the information technology controls for the online banking system, and accordingly we express no opinion on it.

Q2 Software, Inc. uses CyrusOne, Inc. (subservice organization) for co-location data center services. The description includes only the control objectives and related controls of Q2 Software, Inc. and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified by Q2 Software, Inc. can be achieved only if complementary subservice organization controls assumed in the design of Q2 Software, Inc.'s controls are suitably designed and operating effectively, along with the related controls at Q2 Software, Inc. Our examination did not extend to controls of the subservice organization, and we have not evaluated the suitably of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Q2 Software, Inc.'s controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

*Service Organization's Responsibilities*

In Section II of this report, Q2 Software, Inc. has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. Q2 Software, Inc. is responsible for preparing the description and assertion, including the completeness, accuracy and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

*Service Auditor's Responsibilities*

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period October 1, 2019, to September 30, 2020. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- Performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion
- Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved
- Evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion

*Inherent Limitations*

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not; therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

*Description of Tests of Controls*

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

*Opinion*

In our opinion, in all material respects, based on the criteria described in Q2 Software, Inc.'s assertion:

- The description fairly presents the information technology controls for the online banking system that was designed and implemented throughout the period October 1, 2019, to September 30, 2020.
- The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1, 2019, to September 30, 2020, and subservice organizations and user entities applied the complementary controls assumed in the design of Q2 Software, Inc.'s controls throughout the period October 1, 2019, to September 30, 2020.
- The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period October 1, 2019, to September 30, 2020, if complementary subservice organization and user-entity controls assumed in the design of Q2 Software, Inc.'s controls operated effectively throughout the period October 1, 2019, to September 30, 2020.

*Restricted Use*

This report, including the description of tests of controls and results thereof in Section IV of this report, is intended solely for the information and use of management of Q2 Software, Inc., user entities of Q2 Software, Inc.'s information technology controls for the online banking system during some or all of the period October 1, 2019, to September 30, 2020, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.

RSM US LLP

Dallas, Texas
January 26, 2021

# II. Q2 Software, Inc.'s Assertion

We have prepared the description of Q2 Software, Inc.'s information technology controls for the online banking system titled "Description of Q2 Software, Inc.'s Online Banking System" for processing user entities' transactions throughout the period October 1, 2019, to September 30, 2020 (the description), for user entities of the system during some or all of the period October 1, 2019, to September 30, 2020, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by subservice organizations and user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

Q2 Software, Inc. uses CyrusOne, Inc. (subservice organization) for co-location data center services. The description includes only the control objectives and related controls of Q2 Software, Inc. and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified by Q2 Software, Inc. can be achieved only if complementary subservice organization controls assumed in the design of Q2 Software, Inc.'s controls are suitably designed and operating effectively, along with the related controls at Q2 Software, Inc. The description does not extend to controls of the subservice organization. The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of the information technology controls for the online banking system's controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

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

- The description fairly presents the information technology controls for the online banking system made available to user entities of the system during some or all of the period October 1, 2019, to September 30, 2020, for processing their transactions. The criteria we used in making this assertion were that the description:
    - Presents how the system made available to user entities of the system was designed and implemented to process relevant transactions, including, if applicable:
        - The types of services provided, including, as appropriate, the classes of transactions processed
        - The procedures, within both automated and manual systems, by which services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary and transferred to the reports presented to user entities of the system

  - The information used in the performance of procedures including, if applicable, related accounting records, whether electronic or manual, and, supporting information involved in initiating, authorizing, recording, processing and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information presented for user entities

  - How the system captures and addresses significant events and conditions, other than transactions

  - The process used to prepare reports and other information for user entities

  - Services performed by a subservice organization, if any, including whether the carve-out method or inclusive method has been used in relation to them

  - The specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the service organization's controls

  - Other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities and monitoring activities that are relevant to the services provided

- Includes relevant details of changes to the service organization's system during the period covered by the description

- Does not omit or distort information relevant to the scope of the service organization's system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the information technology controls for the online banking system that each individual user entity of the system and its auditor may consider important in its own particular environment

- The controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period October 1, 2019, to September 30, 2020, to achieve those control objectives if subservice organizations and user entities applied the complementary controls assumed in the design of Q2 Software, Inc.'s controls throughout the period October 1, 2019, to September 30, 2020. The criteria we used in making this assertion were that:

  - The risks that threaten the achievement of the control objectives stated in the description have been identified by management of the service organization.

  - The controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.

  - The controls were consistently applied as designed; including whether manual controls were applied by individuals who have the appropriate competence and authority.

# III. Description of Q2 Software, Inc.'s Online Banking System

## *Overview of Operations and Processing Environment*

Q2 Software, Inc. (or Q2) was founded to provide applications and technology to community financial institutions in the United States. Q2 Software, Inc. markets and develops software solutions under the Q2 brand. Q2 trades on the New York Stock Exchange (NYSE), under the ticker symbol "QTWO."

Q2 develops, provides and hosts online banking solutions for financial institutions. The financial institutions may elect to implement these services directly on their servers or interface with a version of the products residing on a company-owned and operated server.

Q2Online banking provides customers of the financial institution with the ability to view account information and perform certain transactions (e.g., payments and fund transfers) over the internet. Q2Online also allows customers to utilize commercial payment utilities such as ACH payments, wire transfers, tax payments and online authorization rights for drafting and authorizing payments.

Q2Mobile services enable financial institutions to provide their customers with the mobile products and services transactions anytime, anywhere and from any supported device.

Q2Voice banking service is built with technology that provides a complete audit trail and reporting engine, while providing consumer and business customers with access to their account information anytime, anywhere over the phone utilizing the same e-banking platform.

The Q2Central administration and operations console provides the financial institution with single-point administration for Q2Online, Q2Mobile and Q2Voice via a Windows-based client/server application. This administration includes customer management, transaction processing, system configuration and general administration. Q2Central is packaged with Q2Online, Q2Mobile or Q2Voice licenses.

Payments I.Q. System (PIQs) provides ACH general reporting and validation services for both originated and incoming ACH transactions.

Exact/TMS (ETMS) provides positive pay and reconciliation services.

Dispute Tracking System (DTS) provides customer dispute tracking services.

### Scope of Report

This report has been prepared to provide information to user entities on IT general controls applicable to Q2 Software's online banking system provided to user entities and relevant applications hosted at the CyrusOne data center facilities in Austin, Texas, and Carrolton, Texas, and covers the functionality related to the Q2Online application Version 4.4.0 (internet banking), Q2Central Version 4.4.0 (administrative portal), Q2Mobile Version 4.4.0, Q2Voice Version 4.4.0, ETMS Version 8.3.5, PIQs Version 6.3.7 and DTS Version 6.9.0. Q2 Software products

and solutions that are hosted by third parties or hosted on-premises by clients are not included in the scope of this report. Unique contractual arrangements or customized solutions developed for user entities are also not included in the scope of this report.

Q2 Software uses CyrusOne, Inc. (subservice organization) for co-location data center services. The scope of this report does not include services provided or controls performed by the identified subservice organization.

*Infrastructure and Software*

Q2 Software's products are developed, operated and maintained by Q2 Software staff. Modifications and enhancements to these products are developed on versions of the products contained on servers at Q2Software's data centers. Git and BitBucket are utilized as source code repositories for Q2 Software's products.

The Online Banking system is hosted on a Windows Active Directory network. Application servers and databases at the co-location facilities are running Windows and Linux operating systems. Access to applications, back-end servers, databases, VPN, endpoint security and firewalls are controlled via Active Directory.

In order to obtain customer financial information, as well as perform the necessary transactions, Q2 Software's products interface with the host systems at the financial institutions through secure point-to-point VPNs, which allows the financial institution customer to perform transactions and see account activity.

*Online Banking*

Data can be input or received via one of the following:

- A banking customer/end user can input data directly via Q2Online, Q2Voice or Q2Mobile.
- Voice has its own dedicated service integrated through the Q2Online application interface (API).
- Q2Online and Q2Mobile data is received via .NET services via HTTPS utilizing Transport Layer Security (TLS) encryption protocol.
- A banking employee end user can input data directly via Q2Central or generate reports and transactions from Q2 Central to update core banking systems or process transactions via a core banking system or third party.
- Q2Central is accessed via desktop application and data is received via .NET services via HTTPS utilizing TLS encryption protocol.
- Core banking data can be received and/or sent real time via a wedge API adapter for financial institutions or third parties, and is connected through web services or Transmission Control Protocol (TCP) socket requests.

- Batch file data can be received from and/or sent to core banking applications or third parties via a secure File Transfer Protocol (SFTP) server running job schedules over a VPN connection provided and managed by TrustGrid.

For Q2Online and its API, all data is input via .NET web service via TLS protocol. Data is encrypted over web service transmissions and is unencrypted in the Q2Online environment using a private key infrastructure. The application and database environments are segregated via virtual local area networks (VLANs), and host data input or pulled from the back-end is via web service over Port 80. Data is archived from databases on a nightly basis, unless a data retention policy is defined by the customer. Critical vendors that may have access, or receive data or proprietary information, utilize encrypted connections. Transmissions between data centers are secured via private link VPN tunnels.

*PIQs*

PIQs provides ACH general reporting and validation services for both originated and incoming ACH transactions. ACH originated transactional data is received via an API call to the online banking application and extracts ACH transactions that occurred that day. The API is an internally developed web service that calls and pulls from specific database paths. The API calls and pulls operate on a job schedule. A windows service pulls the ACH originated transactional data into the PIQs production database. Incoming ACH transactional data must be uploaded by the client's financial institution to the data center for PIQs to build into the PIQs production database.

*ETMS*

ETMS provides positive pay and reconciliation services to financial institutions. Transactional data can be input or received via one of the following:

- Transactional data is received from the financial institution's banking core application via a secure FTP server.
- Financial institutions will add a trigger file to the secure FTP server, and ETMS web services monitor for the trigger file and pull data files upon receipt over encrypted VPN or encrypted internet connections.
- Financial institutions will securely transmit transactional data to Q2 Software's secure FTP server.
- Financial institutions and their customers/end users can upload transactional data files directly into the ETMS application via single sign-on through the online banking application, which uses .NET services via HTTPS utilizing TLS encryption protocol.
- Transactional data is received via the online banking wedge API adapter using real-time requests through a defined address, and the wedge will push the data into ETMS internally via batch files.
- A windows service pulls the transactional data into the ETMS production database.

*DTS*

DTS provides customer dispute tracking services. The API is an internally developed web service that allows clients to document, track investigation and documentation requirements, and process adjustments for disputes received from banking customers. Dispute data is entered directly into the user interface by financial institution users. A windows service pulls financial institution account and transaction data into the DTS production database from financial institutions. Incoming ACH transactional data must be uploaded by the client's financial institution to the data center for DTS to build into the DTS production database. ACH files can be generated from DTS to process adjustments to accounts for disputed transactions.

## *Relevant Aspects of the Control Environment, Risk Assessment and Monitoring Activities*

Control Environment

The company's control environment reflects the overall attitude, awareness and actions of management, employees and others concerning the importance of controls and the emphasis given to controls in its policies, procedures, methods and organizational structure. Q2's control environment originates with and is the responsibility of the Senior Management Team, which considers the following components:

Integrity and ethical values: Organizational values and behavioral standards have been established and communicated to personnel through the policies, work rules and code of ethics reflected in the Q2 Employee Handbook.

Authority and responsibility: Lines of authority and responsibility are established throughout the organization and are communicated through Q2's, (1) management philosophy and operating style, (2) organizational structure, (3) policies and procedures, and (4) delineation in the Employee Handbook.

Human resources (HR): Q2's HR department is responsible for, (1) assisting senior management in establishing HR policies, (2) assisting employees with employment and benefit issues, (3) supporting the managers and directors of operating departments in their roles overseeing employees, and (4) supporting organization compliance with employment laws and regulations.

Q2 maintains an organizational structure, which provides for segregation of duties between organizational elements. Q2 maintains an organizational chart that delineates the roles of executive personnel within the organization. The organizational chart delineates operational departments for product development, product adoption, customer installation, customer support and network support. Separate departments are also maintained for accounting and sales.

*Personnel Practices and Policies*

New and existing employees are onboarded, managed and monitored in various ways in order to maintain expectations and qualifications of the organization. Job candidates' qualifications and prior experience are assessed during the application process, and background checks are completed as part of the onboarding process. Q2's Employee Handbook includes employment standards, administrative standards, pay practices, employee benefits and services, and business conduct. This handbook is provided to new employees who sign an agreement stating that they have read and understand its terms. A new hire checklist identifies items issued to the employee, payroll information and other items (which include background checks, issuance of the Employee Handbook, collecting acknowledgement forms, dissemination of policies and GLBA training). As part of the hiring requirements, Q2 performs background checks on employee candidates prior to employment. The security department provides training in the form of presentations to new employees that addresses GLBA compliance and internal security guidelines.

Written system and physical security policies, which outline commitments and responsibilities of internal users, are reviewed and approved by corporate management on an annual basis. Policies are available to internal users on an internal portal. Q2 Software has documented career ladders for employees within the consulting, IT, marketing, customer support, project manager, sales and accounting departments. Written career ladders are in place for the personnel responsible for the implementation of security, availability and confidentiality roles and responsibilities. A performance review is completed for employees on an annual basis. Employees are required to complete security awareness training, and training specific to their job function on an annual basis.

## Risk Assessment

Q2 Software has documented risk assessment requirements and procedures that define the risk assessment process, and has been incorporated as a component of departmental policies and procedures, and policies and procedures related to security, availability and confidentiality. A risk assessment is performed by management, and the assessment includes identification and ranking of risks relating to business objectives, commitments and requirements, privacy considerations, internal operations and external factors (e.g., business environment, regulatory environment, technological environment). Risks identified are addressed and mitigation strategies are documented and tracked using a risk matrix. The risk assessment is communicated to the risk and compliance committee and board of directors on an annual basis. The formal risk assessment process is performed throughout the year in order to provide full enterprise-wide coverage, and updates are provided to senior management and the risk and compliance committee throughout the year. The risk and compliance committee meets quarterly to discuss regulatory, information security, including cybersecurity and compliance risks and issues.

Q2 Software has developed a risk assessment level and audit frequency guidelines document that describes the timelines and frequencies for planned audits. This document is used as a reference by management, the risk and compliance committee and the board of directors when preparing and planning for upcoming audits.

### Monitoring Activities

Q2's board of directors meets on a quarterly basis with the risk and compliance committee to approve policies and procedures, approve minutes, and discuss business, financial, operational, regulatory and compliance updates. The board receives a report from the risk and compliance committee during each meeting to review. Board of directors and senior management meet quarterly to review and provide oversight of financial performance, operations and strategic planning.

Q2's executive leadership team directs and controls operations, and establishes, communicates and monitors control policies and procedures. The executive leadership team comprises the compliance, IT accounting, security, HR, development, product management, support and sales departments, and meets periodically to discuss overall business objectives and topics related to the departments.

The risk and compliance committee maintains an internal tracking mechanism to verify that Q2 Software performs audits and updates policies and procedures. Corporate management meetings are held on an annual basis to assess new and existing mitigation strategies documented in the risk matrix to determine that mitigation strategies are designed and operating effectively.

## *General Computer Controls*

General computer controls include controls over computer operations, access, and systems development and maintenance. General computer controls, if suitably designed and operating effectively, provide an environment for the development and processing of applications to achieve specific application control objectives.

### Computer Operations

*Overview*

Q2's headquarters is located in a commercial building in Austin, Texas. The corporate computing infrastructure is distributed across both the headquarters and the data center, with mission-critical corporate services being hosted in the data center. This includes various technical infrastructure components that support the campus directly. The primary data center operations, which include customer databases and the production instance of Q2 products, reside at the co-location facilities located between Austin, Texas, and Carrolton, Texas.

*Database Backup and Recovery*

Full backups for client databases hosted in Q2 Software's data centers are scheduled weekly and, once completed, the data is stored on a dedicated backup appliance that encrypts the data and replicates it to a backup application in an authorized off-site location. The system is configured to run full server backups on a weekly basis. The system is configured to run differential database backups daily and incremental transaction log backups every 15 minutes. The incremental backups are replicated between data centers via transaction logs. The transaction logs are transmitted via a secure VPN tunnel. Backup and replication status is reviewed and documented on a daily operations checklist. Cases are created and assigned to the backup administrator to identify the cause and resolve errors in the process, if necessary. Resolution is noted on the daily operations checklist.

Restoration of backups is tested during the business continuity and disaster recovery plan testing that is performed on an annual basis. Results are communicated to corporate management.

## Access Controls

*Overview*

Q2 Software utilizes Microsoft Windows Active Directory group policies and access controls to enforce security requirements for users who log on to internal network systems. Role-based security is utilized and is configured to restrict the unauthorized access to the network, applications, servers, databases and network infrastructure. Routers and firewalls that separate the private network from the public internet protect Q2 Software's internal systems.
Q2 Software maintains security policies that define the oversight and administration of procedures related to security and logical IT internal controls. The policy is approved by the board on an annual basis.

*Physical Access*

Q2 Software does not host client environments at their corporate office. The online banking environments reside in CyrusOne data centers located in Carrollton, Texas, and Austin, Texas. CyrusOne is responsible for providing physical access and environmental controls for the data centers.

CyrusOne provides physical access administration based on Q2 Software requests. Access to the CyrusOne data center is approved by IT management and the request is sent to CyrusOne. CyrusOne is responsible for granting access to the data center only after receiving approval from Q2 Software IT management. Data center access is requested to be removed upon notification of employee or contractor termination by the HR manager. CyrusOne is responsible for removing physical access to the data center facilities upon notification from Q2 Software. Access to the data center is reviewed and approved by Q2 IT management on a quarterly basis to determine that access is restricted and appropriate.

*Logical Access and Security Controls*

New employee onboarding procedures include the completion of a new hire checklist by HR and the approval of an access request form by management. New user access and elevated access requests are submitted through the ticketing system. Access is assigned based on an access matrix outlining access needs by position. The access matrix is reviewed and approved by management on a quarterly basis. User access change requests follow the same processes for new user access and the removal of user access (after notification by the HR manager). Upon termination of an employee, HR submits a request in the ticketing system. The system administrator removes or disables user accounts upon notification of an employee's termination by the HR manager.

The company has user authentication requirements over its network and servers. Logical access is limited to personnel requiring access to complete their job functions. Users authenticate through Windows Active Directory. Group policies require passwords to be at least fourteen characters long and meet complexity requirements. Active Directory also remembers a history of 24 passwords and will lockout an account after five failed login attempts. Access to production environment systems, applications, servers, databases and networking equipment is controlled via group memberships and related permissions configured within Active Directory. Server and database password authentication configurations are set up to enforce a password policy.

Administrator and local user access rights to Q2 Software's network, servers and databases are limited to authorized personnel. User account access to the network and related permissions, including administrator access, direct access to data and access to job scheduling tools, are reviewed for appropriateness and authorized by management on a quarterly basis. Service and application accounts are reviewed by management quarterly to validate the accounts are authorized and current. Issues noted during the review are documented and resolved via the ticketing system.

## Q2Online Authentication Controls

Q2Online banking uses multifactor authentication. Based on information the user provides during the user profile account setup, the system uses this information during the authentication process. Password requirements and complexity are configurable by the financial institution. Q2Online requires one-time password verification and multifactor authentication. Q2Online requires the user to change the password after the initial login. Session time-out settings, configurable by the financial institution, deactivates the session after a predefined period of user inactivity.

## Q2Central Authentication Controls

Access to Q2Central requires the user to change the password after the initial login. Q2Central user passwords are masked when entered. Before an authorized user is able to access Q2Central, a user account must be created for the user, which requires a valid user ID and user password. Q2Central administrator access is restricted and does not include the ability to view accountholder passwords. Q2Central has session time-out settings to deactivate the session after a period of inactivity.

Q2Central logs user activity and transactions. User activity and transactional data can be generated and viewed from Q2Central by administrators. User accounts and permissions created in Q2Central are completely and accurately reflected in Q2Central user access listings.

## PIQs Security

Access to the PIQs system requires the user to change the password after the initial login. PIQs user passwords are masked when entered. Before an authorized user is able to access PIQs, a user account is created, which requires a valid user ID and user password. PIQs has session time-out settings to deactivate the session after a period of inactivity.

PIQs logs user activity and transactions. User activity and transactional data can be generated and viewed from PIQs by administrators. User accounts and permissions created in PIQs are completely and accurately reflected in PIQs user access listings.

## ETMS Security

Access to ETMS requires the user to change the password after the initial login. No password change is required if the user is authenticated through single sign-on. ETMS user passwords are masked when entered. Before an authorized user is able to access ETMS, a user account is created, which requires a valid user ID and user password. ETMS has session time-out settings to deactivate the session after a period of inactivity.

ETMS logs user activity and transactions. User activity and transactional data can be generated and viewed from ETMS by administrators. User accounts and permissions created in ETMS are completely and accurately reflected in ETMS user access listings.

## DTS Security

Access to DTS requires the user to change the password after the initial login. DTS user passwords are masked when entered. Before an authorized user is able to access DTS, a user account is created, which requires a valid user DTS and user password. DTS has session time-out settings to deactivate the session after a period of inactivity.

DTS logs user activity and transactions. User activity and transactional data can be generated and viewed from DTS by administrators. User accounts and permissions created in DTS are completely and accurately reflected in DTS user access listings.

### *Encryption*

Data transmitted within the application is encrypted by utilizing HTTPS for Q2Online, Q2Mobile, Q2Voice, PIQs, ETMS and DTS, which enforces the usage of strong cipher suites. To segment the instances of the user's data, a distinct and separate database has been set up for each client. This layer of client data resides in a segregated private network. Data is encrypted at rest within production databases.

*Remote Access*

As defined as an employee accessing our network externally from any of the company's offices, data centers or corporate LAN directly, Q2 Software maintains a Remote Access Policy that discusses the purpose and requirements for remote access. Remote access is provided to the network via VPN or dedicated circuit. VPN traffic is encrypted during the remote session. Domain credentials and permissions, and associated token (two factor), are required to access the Q2 Software online banking environment via a jump box. Access is allowed through VMWare virtual desktop infrastructure (VDI) using Remote Desktop Protocol (RDP) technology.

End users authenticate to online banking environments via web browsers. Authorized users enter a user ID and password to obtain account access to Q2Online, Q2Mobile, Q2Voice, PIQs, ETMS and DTS. User-authenticated web sessions are encrypted utilizing HTTPS. Web servers are encrypted utilizing TLS certification. User entities that elect to host the Q2 Software platform on their servers are responsible for providing logical security for their server, operating system and database environment where the Q2 Software product resides. This security is to include the use and configuration of firewalls and strong user authentication procedures (e.g., password complexity).

*Firewall Management*

For products that reside on Q2 servers, a customized routing device is used to route data traffic between Q2 products and the host systems of the financial institutions. Q2 also maintains and manages the use of redundant firewalls in a demilitarized zone (DMZ) configuration. Q2's web servers are located behind the perimeter firewalls and application load balancers (protected from direct access via the internet). Q2 database servers are located behind a second pair of firewalls. The connection to the financial institution's network is through a VPN tunnel and is terminated on a firewall in Q2 network.

A firewall is in place between the network and the internet to restrict access. Q2 has implemented restrictions on firewall configuration settings to allow authorized traffic and deny unauthorized traffic.

## Application System Development and Maintenance

*Overview*

Changes to products follow a structured software development process that results in new releases and patches available to financial institutions. Q2 Software has documented policies and procedures. Included in the policies are requirements for development, testing, approvals, documentation and customer notification. Q2 Software has established a tracking process to address application defects and core system enhancements. The change advisory board meets on a biweekly basis to schedule resources, review future IT infrastructure changes, and evaluate risks and timelines associated with future changes. A monthly meeting is held to review available system software patches and updates. Patches and updates are approved via the change management process, and then promoted to production after testing is completed in the quality assurance (QA) environment when applicable.

*Initiation, Authorization and Prioritization*

Application change control is managed through an internally supported and hosted version of the JIRA application, and via change control cases in the Salesforce application. The steps in the program change process are documented in these applications and, therefore, represent the primary repositories for evaluating the status and issues with changes. Customer support or the project manager creates a change control case in the Salesforce application for product defects. The case is reviewed by Level 3 support personnel and, if needed, a JIRA ticket is created and linked to the change control case. Product management determines which products/features will be included in each release and creates JIRA tickets for product enhancements.

The development department, which is managed by the senior vice president of engineering, is responsible for addressing and prioritizing issues. Priority levels help define the business impact that a problem has on the customer's operation, establish expectations with the financial institution and maintain contact with them until the issue is resolved. High-priority issues are defined as issues relating to the production system being down, the Q2 Software product being unavailable to the end user or an event that affects security. Medium-priority issues are defined as issues relating to the failure of a major feature or function causing customer operations to be restricted. Low-priority issues include other fixes regarding the functionality of the product, including ease of use and cosmetic issues. The Customer Service Guide and Software Development Life Cycle Policy defines these priority levels, as well as the resolution procedures for priorities. Either the director of release management or director of test engineering (or their designated proxy with a director or above approval) approves releases prior to promotion to production.

*Version Control*

Q2 Software maintains a dedicated development environment and build server to create and test changes to its product applications. Version control of changes is tracked using a source control system. When code is placed into the source control repository after development, it is packaged and a unique version number is created for that packaged code. The unique version number of the packaged code will carry over to implementation to production. If there is a change made to the packaged code, the version number will change. This application allows developers to monitor the development of changes and roll back to previous versions when necessary.

Access to promote changes to the core production application platform and related databases is reviewed and approved by IT management on a quarterly basis to determine that access is appropriate and authorized, and that developers do not have access to core production applications. Issues noted during the review are documented and resolved via the ticketing system.

*Database Monitoring*

Q2 Software relies on detective controls to monitor for changes to high-risk database changes and data fields to validate that changes made to online banking databases are authorized. IT management retroactively reviews elevated access instances to production databases on a monthly basis to validate that each instance of user access to production databases via the DBTracks tool was appropriate based on a business need and authorized. As part of the review, IT management validates that each access instance had an associated change ticket or work order to justify the access, and the ticket or work order was authorized. IT management documents their review via the ticketing system, and includes investigation and resolution of identified changes without associated and/or authorized tickets or work orders.

Native SQL functions are used to monitor changes to certain high-risk database tables and/or fields contained in the online banking databases. The SQL functions issues automated alerts via email to the Data Servicing Team when changes to defined database tables and fields are identified. The data servicing team reviews the alerts and validates that database table and/or field changes had an associated change ticket or work order to justify the change, and the ticket or work order was authorized. The review is documented via the ticketing system, and includes investigation and resolution of identified changes without associated and/or authorized tickets or work orders. Alerts are investigated to determine whether the change was authorized. The following databases changes are monitored:

- User logon table additions reach maximum user threshold
- New privileged database user accounts are added
- Changes to the following database tables:

An internally developed tool is used to monitor changes to certain high-risk data fields contained in the online banking production databases. The tool automatically tracks and logs changes to certain high-risk data fields. The compliance team reviews data field changes logged by the monitoring tool on a monthly basis. As part of the review, the compliance team validates that data field changes had an associated change ticket or work order to justify the change, and the ticket or work order was authorized. The compliance team documents their review via the ticketing system, and includes investigation and resolution of identified changes without associated and/or authorized tickets or work orders. The following data field changes are logged by the monitoring tool:

- Q2_RecipientAccount (AccountNumber, ABA)
- Q2_FundsTransfer (ToAccount)
- Q2_GeneratedTransactions (TransactionAmount)
- Q2_WireTransfer (ToAccount)
- Q2_AchPpdCcdDetail (ABA, AccountNumber, Amount)
- Q2_ThirdPartyData (DataValue)

*Testing*

Core application and related database releases are tested in a release package by QA before promotion to production. Verification of issue resolution with associated product release regression testing is performed, at a minimum. Hotfixes are minimally tested using current customer versions of product components with the expectation that additional testing will occur in the customer environment. For new features, applicable inspection points (user interface, database logs, output, etc.) are evaluated. Documented feature requirements, exception handling and usability are verified during the testing process. Defects and enhancement suggestions are submitted into JIRA. Issues are communicated with development and project management. Testing steps and results are documented by QA before promotion to production. The unique product component version combinations tested are recorded.

*Promotion to Production*

After approvals are obtained, QA or a development operations manager moves the updated code from the QA environment to the applicable software release folders within a source control repository. The ability to move changes into customer production environments is limited to authorized individuals. The repository requires a username and password for access, and read-only or read-write access is granted based on user roles and is enforced by the repository when end users connect. Write access to the repository is restricted based on job role. The repository records the identity of the publisher. The code repository is located on a secure server. Application code release and related database change migration to production is performed by operations. QA publishes packages to the repository for operations for product upgrades and controls the implementation process for instances of products.

Core production application and related database releases and changes are performed during stated maintenance windows or other times prearranged with the financial institution. These windows are during off-peak periods and are communicated to financial institution customers in advance. The Release Management Team publishes release notes for feature releases and patches. Release management publishes a release notification upon promotion of releases to general or limited availability.

Promotion of hotfixes is communicated by release management to affected project teams at a minimum. User entities are responsible for electing to accept or deny a new release.

Emergency changes require the performance and retention of testing, management approval and customer notifications before promotion to production; however, the documentation can occur retroactively.

Q2 Software maintains several types of documentation about its products that are available to its customers, such as internal product documentation (used to educate Q2 Software employees), and customer or end-user documentation (intended to assist customers on using Q2 Software applications). Depending on the nature of changes to its products, modifications to the documentation is required. Changes to the documentation are performed in conjunction with the release being promoted to production. A scheduled maintenance

calendar is available on the customer portal to notify customers of potential system downtime. Q2 Software is required to amend their service agreements with external users if system changes occur that affect system security, availability or confidentiality.

## *Application and Control Processes*

### Customer Implementation and Account Maintenance

Financial institution customers may elect to implement Q2 products directly on their servers or interface with a version of the products residing on a Q2-owned and operated server. If the customer elects to implement the products on their own servers, Q2's involvement in the implementation is limited to certain specified procedures as determined by the institution. The following procedures are described for financial institution customers that elect to maintain Q2 products on Q2's servers at the co-location facilities.

Q2 utilizes a structured process for the implementation and configuration of its products for a new financial institution customer. A Master License Service Agreement (MLSA) or Master Data Processing Service Agreement (MDPSA) is established prior to the project's go-live date, and the agreement is signed by the financial institution and Q2. Once the contract is signed, a new customer account is established in Q2's Customer Relationship Management (CRM) system according to the terms of the contract. A project manager is then assigned to the institution as the primary contact during the implementation process. This project manager works with an Implementation Team and the financial institution to facilitate the implementation process.

Sales orders are signed by the financial institution and an officer of Q2 as an exhibit to the MLSA or MDPSA prior to the project's go-live date. A Work Order Form is completed for new clients to document requested initial online banking configuration settings, including data file format requirements and job schedules. Implementation testing is completed as necessary and a peer review of the implementation project and implementation testing is completed to validate that the Online Banking system setup is in accordance with processing commitments and responsibilities. The project manager completes a setup checklist that details the specific steps required in the implementation process, as well as the specific hardware, software, security and application configuration requirements necessary for the institution. The Implementation Team schedules periodic meetings for team introductions, Q2 and financial institution demonstrations to finalize configuration settings and to verify that issues are resolved prior to completion of the installation. Within the first three months of the implementation process, Q2 performs an internal QA process and limited production testing after five months. Adjustments to the configuration may be required during this testing process and Q2's Implementation Team will work with the customer to resolve issues.

*Job Processing*

Q2 transmits and/or receives data and transaction files from customers on a daily basis that details transactional data and account details for online banking users. A procedural document is in place that identifies the steps taken to process the transactional files, and what actions to take if there is a processing error. Q2 maintains either a dedicated VPN connection

to customers to retrieve and transmit data files or sends and receives requests via real time via a wedge API adapter connected through web services. These transactional, balance and data files are captured by Q2 by running automated scripts that communicate with the customer's network via a dedicated VPN connection or a wedge API adapter, and picks up a batch file at a designated location. Automated scripts are configured to securely log into customers' environments and retrieve transactional and balance files. In the event of an error in the retrieval process, the operations group is notified via the alert monitoring framework that feeds into an internal webpage. A case is manually created and assigned to customer support for resolution.

Once the files are retrieved and received by Q2, the files are then processed into the internal Q2 databases. The Data Services Team in support runs automated scripts in the morning to verify that the database load has occurred successfully. The results of these scripts are fed into an internal reporting page used by the Data Services Team as their primary dashboard in their daily morning validation. The Dashboard will show a history of the previous three days that allows personnel to view trending information for the record counts of transactions processed. If there are large discrepancies in the amount of file transactions processed for the day as compared to previous days, the support personnel are able to identify and troubleshoot the issue.

Job scheduling tools are used for automatic job processing based on job schedules and monitoring for extended job run times or job errors (such as file integrity or data validation errors that prevent completion of data processing). The job scheduling tools are configured to log or issue automated alerts to the Data Services Team via email when jobs are running longer than expected thresholds or job errors occur. The Data Services Team documents issued alerts, investigation of the alert and resolution via the ticketing system. Financial institutions are contacted, if necessary, to resolve the issues. User account access to the job scheduling tools is reviewed for appropriateness and approved by management on a quarterly basis. Issues noted during the review are documented and resolved via the ticketing system.

## Customer Service

Q2 has established policies and procedures to communicate customer support expectations. These include required timelines to handle service issues, establishing priority levels (high, medium and low), and target resolution time frames. Separate processes have been established depending on the nature of the customer issue. Q2 Software has established an incident reporting hotline and portal for external users to report issues regarding security, availability, customer support and other issues or concerns. Customer service representatives are assigned to issues and are responsible to document issue resolution with the financial institution in the ticketing system within 30 days. Change requests are opened if necessary to resolve customer issues. Minor system performance issues are documented within the CRM system to provide historical/background information on the issue, as well as status information on the closure of the issue. More complex customer issues are processed through a change management process.

Q2's customer service representatives administer customer service issues. Customer service representatives are assigned to issues and are responsible to document issue resolution with the financial institution in the ticketing system. In some cases, a case may travel from the initial, level-one representative to a representative in level two or level three support depending on the nature of the issue. In certain circumstances, the information documented for an issue may be utilized to develop a patch to a Q2 product.

Reporting

The Q2 administration console has three standard reports, operations, audit and compliance, and usage and activity. The Q2 database servers are also configured to log customer transactions and activities. Q2Central can be used by the data center administrators to view the audit log detail. End users do not have the ability to access application databases to perform ad hoc reports. Standard settings are available within the application to configure report content and format. Financial institutions can contact customer support to inquire if a customized report can be developed.

### *Information Produced by Q2 Software*

The following are standard key reports Q2 Software produces:

| Report Name | Control Number | Description | Source System | Report Use |
|---|---|---|---|---|
| Active Directory User Listings | 2.3<br>3.5<br>5.5 | Vendor tool used to aggregate the Active Directory user access listing and related permissions/group memberships for management to review network access, group memberships, administrative or elevated access, server/database access, networking equipment access and remote access. | Microsoft Active Directory—Q2 Software is unable to modify the report code, as it is purchased from the vendor. | Execution of a control by the service organization |

| Report Name | Control Number | Description | Source System | Report Use |
|---|---|---|---|---|
| Data Center Authorized User Portal | 4.3 | Vendor tool used to aggregate personnel authorized to have access to the data centers and/or perform administrative functions for management to review authorized Q2 Software personnel. | CyrusOne Authorized User Portal—Q2 Software is unable to modify the report code, as it is purchased from the vendor. | Execution of a control by the service organization |
| DBTracks Elevated Access Log | 5.7 | Proprietary tool used to aggregate elevated access instances to production databases | DBTracks—Q2 Software is able to modify the report code, as the tool and log configurations are managed by Q2 Software. | Execution of a control by the service organization |
| Data Field Change Log | 5.8 | Proprietary tool used to aggregate changes made to production data fields | MS SQL—Q2 Software is able to modify the report code, as the tool and log configurations are managed by Q2 Software. | Execution of a control by the service organization |

*Third-Party Risk Management*

Q2 Software maintains relationships with several third-party vendors and subservice providers (collectively "third parties"). The third parties defined as critical may have access to or receive/transmit confidential data. Service agreements for critical third parties (as defined by Q2 Software's internal standards) have been established and signed by both parties that define the terms of the relationship. The agreements define the confidential nature and nondisclosure requirements of the relationship, and include timely notification of a known or suspected breach of data, a nondisclosure clause and limitations for use of third parties prior to execution of a contract or integration.

Third-party risk management performs an assessment of critical third parties which is outlined in the third-party risk management program. Identification of risks, assessment of performance, completion of the privacy questionnaire and review of third-party assurance reports, if applicable, are part of the assessment. The third-party assessment results are communicated to the risk and compliance committee on an annual basis. Q2 Software obtains and reviews SOC reports annually from their subservice providers identified in this report.

*Subservice Organization*
Q2 Software uses a subservice organization to perform various functions to support the delivery of services. The scope of this report does not include the controls and related control objectives at the subservice organization. The following is a description of services the subservice organization provides and the complementary subservice organization controls expected to implemented at the subservice organization.

| Subservice Organization | Service Provided |
|---|---|
| CyrusOne | CyrusOne is a data center co-location provider that hosts Q2's production servers in Austin, Texas, and Carrolton, Texas, facilities. |

| Applicable Criteria | Controls Expected to Be Implemented at the Subservice Organization |
|---|---|
| Control Objective 4<br>Controls provide reasonable assurance that physical access to computer and other resources relevant to user entities' internal control over financial reporting is restricted to authorized and appropriate personnel. | • Access to the facility is restricted to personnel or visitors authorized by the tenant.<br>• Access to the facility is removed/disabled upon tenant notification, and access to the facility and sensitive areas is reviewed and approved to validate that access is authorized and appropriate.<br>• Administrative access to the physical security system is restricted to authorized and appropriate personnel.<br>• Reports are generated completely and accurately from the physical security system used by customers to conduct access reviews. |

## *Complementary User Entity Control Considerations*

Q2 Software's Online Banking system was designed with the assumption that certain complementary controls would be placed in operation by user entities in order to achieve the stated control objectives. Accordingly, Q2 Software's user entities and their auditors should consider whether the following complementary controls have been designed correctly and operating effectively at user entities:

- Notifying Q2 Software when a customer service issue has been successfully or unsuccessfully resolved. (Control Objective 2)
- Notifying Q2 Software of bugs or issues encountered by the customer during the operation of a Q2 Software product. (Control Objective 2)
- Electing whether to accept or deny a new release. (Control Objective 5)

# IV. Q2 Software, Inc.'s Control Objectives and Related Controls and RSM US LLP's Tests of Controls and Results of Tests

Q2 Software, Inc.'s control objectives and related controls are an integral part of management's description of the system and are included in this section for presentation purposes. RSM US LLP included the description of the tests performed to determine whether the controls were operating with sufficient effectiveness to achieve the specified control objectives and the results of tests of controls, as specified below.

Tests of the control environment, risk assessment, information and communication, and monitoring activities included inquiries of appropriate management, supervisory and staff personnel, observation of Q2 Software, Inc.'s activities and operations, and inspection of Q2 Software, Inc. documents and records. The results of those tests were considered in planning the nature, timing and extent of RSM US LLP's testing of the controls designed to achieve the related control objectives. As inquiries were performed for substantially all of Q2 Software, Inc.'s controls, the inquiry procedures are not listed individually for every control in the tables below.

## *Computer Operations*

**Control Objective 1:** Controls provide reasonable assurance that data relevant to user entities' internal control over financial reporting is backed up regularly, and is available for restoration in the event of processing errors and/or unexpected processing interruptions.

| | ***Provided by Q2 Software, Inc.*** | ***Procedures Performed by RSM US LLP*** | |
|---|---|---|---|
| | **Control** | **Test Performed** | **Test Results** |
| 1.1 | The system is configured to run full server backups on a weekly basis. | Inspected the server backup configurations to determine whether full backups were configured to run on a weekly basis. | No exceptions noted. |
| 1.2 | The system is configured to run full database backups weekly, differential backups daily and incremental transaction log backups shipped between data centers every 15 minutes. | Inspected the database backup configurations to determine whether the system was configured to run full database backups weekly, differential backups daily, and incremental log shipping backups between data centers every 15 minutes. | No exceptions noted. |
| 1.3 | Backup and replication status is reviewed and documented on a daily operations checklist. Backup and replication errors that are identified and resolved are documented on the daily operations checklist. | Inspected daily operations checklists for a sample of days to determine whether backup and replication status was reviewed and errors were documented and resolved. | No exceptions noted. |

| **Control Objective 1:** Controls provide reasonable assurance that data relevant to user entities' internal control over financial reporting is backed up regularly, and is available for restoration in the event of processing errors and/or unexpected processing interruptions. | | | |
|---|---|---|---|
| ***Provided by Q2 Software, Inc.*** | | ***Procedures Performed by RSM US LLP*** | |
| | **Control** | **Test Performed** | **Test Results** |
| 1.4 | Restoration of backups is tested during the business continuity and disaster recovery plan testing that is performed on an annual basis. Results are communicated to corporate management. | Inspected the backup restoration testing results from the business continuity and disaster recovery testing to determine whether the results were communicated to corporate management. | No exceptions noted. |

| **Control Objective 2:** Controls provide reasonable assurance that application and system processing relevant to user entities' internal control over financial reporting are executed in a complete and timely manner, and deviations, problems and errors that may affect user entities' internal control over financial reporting are identified, tracked, recorded and resolved in a complete, accurate and timely manner. | | | |
|---|---|---|---|
| ***Provided by Q2 Software, Inc.*** | | ***Procedures Performed by RSM US LLP*** | |
| | **Control** | **Test Performed** | **Test Results** |
| 2.1 | A Work Order Form is completed for new clients to document requested initial online banking configuration settings, including data file format requirements and job schedules. Implementation testing is completed as necessary and a peer review of the implementation project, and implementation testing is completed to validate that the Online Banking system setup is in accordance with processing commitments and responsibilities. | Inspected work orders for a sample of new clients to determine whether work orders were completed and documented requested initial online banking configuration settings, including data file format requirements and job schedules, where applicable, and the implementation was tested and peer reviewed. | No exceptions noted. |
| 2.2 | Q2 Software has established an incident reporting hotline and portal for external users to report issues regarding security, availability, customer support and other issues or concerns. Customer service representatives are assigned to issues and are responsible to document issue resolution with the financial institution in the ticketing system within 30 days. Change requests are opened if necessary to resolve customer issues. | Observed the existence of a reporting hotline number and portal to determine whether external users had the tools to report issues regarding security, availability, customer support, and other issues or concerns. | No exceptions noted. |
| | | Inspected tickets for a sample of reported incidents to determine whether incidents were tracked for investigation and resolution within 30 days, and change requests were opened if necessary. | No exceptions noted. |

| **Control Objective 2:** Controls provide reasonable assurance that application and system processing relevant to user entities' internal control over financial reporting are executed in a complete and timely manner, and deviations, problems and errors that may affect user entities' internal control over financial reporting are identified, tracked, recorded and resolved in a complete, accurate and timely manner. | | | |
|---|---|---|---|
| ***Provided by Q2 Software, Inc.*** | | ***Procedures Performed by RSM US LLP*** | |
| | **Control** | **Test Performed** | **Test Results** |
| 2.3 | Job scheduling tools are used for automatic job processing based on job schedules and monitoring for extended job run times or job errors (such as file integrity or data validation errors that prevent completion of data processing). The job scheduling tools are configured to log or issue automated alerts to the Data Services Team via email when jobs are running longer than expected thresholds or job errors occur. The Data Services Team documents issued alerts, investigation of the alert and resolution via the ticketing system. Financial institutions are contacted, if necessary, to resolve the issues. | Inspected the job scheduling tools configurations for a sample of processing jobs to determine whether job processing was scheduled to run automatically and alerts were issued when errors occurred. | No exceptions noted. |
| | | Inspected tickets for a sample of job errors to determine whether issued alerts were documented, investigated and resolved, and financial institutions were contacted, if necessary, to resolve the issue. | No exceptions noted. |

## *Logical Access*

**Control Objective 3:** Controls provide reasonable assurance that logical access to programs, data and computer resources relevant to user entities' internal control over financial reporting is restricted to authorized and appropriate users, and such users are restricted to performing authorized and appropriate actions.

| *Provided by Q2 Software, Inc.* | | *Procedures Performed by RSM US LLP* | |
|---|---|---|---|
| **Control** | | **Test Performed** | **Test Results** |
| 3.1 | Role-based security is utilized and is configured to restrict the unauthorized access to the network, applications, servers, databases and network infrastructure. | Inspected the network user groups and permissions to determine whether role-based security was utilized and configured to restrict the unauthorized access to the network, applications, servers and network infrastructure. | No exceptions noted. |
| 3.2 | New user access and elevated access requests are submitted through the ticketing system. Access is assigned based on an access matrix outlining access needs by position. The access matrix is reviewed and approved by management on a quarterly basis. | Inspected access requests for a sample of new accounts and elevated access to existing accounts to determine whether an access request was authorized through the ticketing system and access was granted based on the approval. | Exceptions noted.<br>For six of 25 new accounts sampled, documentation of the access request approval was not documented and retained. |
| | | Inspected access matrix review results for a sample of quarters to determine whether management reviewed and approved the matrix. | No exceptions noted. |
| 3.3 | User accounts are removed or disabled upon notification of employee or contractor termination by the HR manager. | Inspected notifications and user listings for a sample of terminated employees and contractors to determine whether HR notified IT and access was removed or disabled. | No exceptions noted. |
| 3.4 | Authentication requirements have been established for the network and servers with following parameters enforced:<br>• Password history of 15<br>• Minimum length of 14 characters<br>• Account lockout after five attempts<br>• Complexity enabled | Inspected the network and server authentication requirements to determine whether the following password parameters were enforced:<br>• Password history of 15<br>• Minimum length of 14 characters<br>• Account lockout after five attempts<br>• Complexity enabled | No exceptions noted. |

| **Control Objective 3:** Controls provide reasonable assurance that logical access to programs, data and computer resources relevant to user entities' internal control over financial reporting is restricted to authorized and appropriate users, and such users are restricted to performing authorized and appropriate actions. | | | |
|---|---|---|---|
| ***Provided by Q2 Software, Inc.*** | | ***Procedures Performed by RSM US LLP*** | |
| **Control** | | **Test Performed** | **Test Results** |
| 3.5 | User account access to the network and related permissions, including administrator access, direct access to data and access to job scheduling tools, are reviewed for appropriateness and authorized by management on a quarterly basis. Service and application accounts are reviewed by management quarterly to validate that the accounts are authorized and current. Issues noted during the review are documented and resolved via the ticketing system. | Inspected network user account, service account and application account access review results for a sample of quarters to determine whether user account access to the network and related permissions, including administrator access, direct access to data, and access to job scheduling tools was reviewed and validated by management, and issues noted during the review were documented in the ticketing system and tracked to resolution. | No exceptions noted. |
| | | Observed the generation of the network users listing to determine whether the correct source was queried, correct parameters were utilized and no inappropriate exclusions were applied. | No exceptions noted. |
| 3.6 | External system access is permitted only through a two-factor encrypted VPN connection. | Inspected the VPN configurations to determine whether external access was restricted to a two-factor-encrypted VPN connection. | No exceptions noted. |
| 3.7 | Server and database password authentication configurations are setup to enforce a password policy. | Inspected password configurations for a sample of servers to determine whether servers were set up to enforce a password policy. | No exceptions noted. |
| | | Inspected password configurations for a sample of databases to determine whether databases were set up to enforce a password policy. | Exceptions noted.<br>For seven out of seven databases sampled, a password policy was not configured to be enforced for service accounts with write-access. |

## *Physical Access*

**Control Objective 4:** Controls provide reasonable assurance that physical access to computer and other resources relevant to user entities' internal control over financial reporting is restricted to authorized and appropriate personnel.

| *Provided by Q2 Software, Inc.* | | *Procedures Performed by RSM US LLP* | |
|---|---|---|---|
| **Control** | | **Test Performed** | **Test Results** |
| 4.1 | Access to the CyrusOne data center is approved by IT management and the request is sent to CyrusOne. | Inspected physical access requests for a sample of new individuals added to the data center access rights listing to determine whether IT management approved the access request prior to access being granted. | No exceptions noted. |
| 4.2 | Data center access is requested to be removed upon notification of employee or contractor termination by the HR manager. | Inspected notifications for a sample of terminated employees to determine whether HR notified IT and access was removed. | No exceptions noted. |
| 4.3 | Access to the data center is reviewed and approved by IT management on a quarterly basis to determine that access is restricted and appropriate. | Inspected data center access review results for a sample of quarters to determine whether IT management reviewed and approved access to validate that access was restricted and appropriate. | No exceptions noted. |
| | | Observed the generation of the CyrusOne user listing from the CyrusOne portal to determine whether the correct source was queried, correct parameters were utilized and no inappropriate exclusions were applied. | No exceptions noted. |

## *Change Management*

| **Control Objective 5:** Control Objective 5: Controls provide reasonable assurance that changes to application programs and related data management systems are tested, documented, approved and implemented. | | | |
|---|---|---|---|
| | ***Provided by Q2 Software, Inc.*** | ***Procedures Performed by RSM US LLP*** | |
| | **Control** | **Test Performed** | **Test Results** |
| 5.1 | Q2 Software has documented change management policies and procedures available on an internal portal. Included in the policies are product change and system software patch requirements for testing, approvals and documentation. Change management policies are reviewed and approved by corporate management on an annual basis. | Inspected the internal portal to determine whether change management policies and procedures were available, and outlined product change and system software patch requirements for testing, approvals and documentation. | No exceptions noted. |
| | | Inspected change management policies to determine whether corporate management reviewed and approved the policies annually. | No exceptions noted. |
| 5.2 | Changes to the core production applications and related databases are tested and approved before the change is approved for general release to production by the Release Management Team. | Inspected tickets for a sample of changes to core production applications and related databases to determine whether the change was tested and approved prior to the change being approved for general release by the Release Management Team. | No exceptions noted. |
| 5.3 | Emergency changes require the performance and retention of testing, management approval and customer notifications; however, the documentation can occur retroactively after promotion to production. | Inspected tickets for a sample of emergency changes to core production applications and related databases to determine whether the emergency change required the performance and retention of testing, management approval and customer notifications. | No exceptions noted. |
| 5.4 | Access to promote changes to the core production applications and related databases is reviewed and approved by IT management on a quarterly basis to determine that access is appropriate and authorized, and that developers do not have access to core production applications. Issues noted during the review are documented and resolved via the ticketing system. | Inspected access review results for a sample of quarters to determine whether IT management reviewed and approved access to the core production applications and related databases, and issues noted during the review were documented in the ticketing system and tracked to resolution. | No exceptions noted. |
| | | Observed the generation of the network users listing to determine whether the correct source was queried, correct parameters were utilized and no inappropriate exclusions were applied. | No exceptions noted. |

| **Control Objective 5:** Control Objective 5: Controls provide reasonable assurance that changes to application programs and related data management systems are tested, documented, approved and implemented. | | | |
|---|---|---|---|
| ***Provided by Q2 Software, Inc.*** | | ***Procedures Performed by RSM US LLP*** | |
| **Control** | | **Test Performed** | **Test Results** |
| 5.5 | Native SQL functions are used to monitor changes to certain high-risk database tables and/or fields contained in the online banking databases. The SQL functions issues automated alerts via email to the data servicing team when changes to defined database tables and fields are identified. The Data Servicing Team reviews the alerts and validates that database table and/or field changes had an associated change ticket or work order to justify the change, and the ticket or work order was authorized. The review is documented via the ticketing system, and includes investigation and resolution of identified changes without associated and/or authorized tickets or work orders. Alerts are investigated to determine whether the change was authorized. The following database changes are monitored:<br>• User logon table additions reach maximum user threshold<br>• New privileged database user accounts are added | Inspected the system configurations to determine whether the SQL functions were configured to issue automated alerts to the Data Services Team when following database changes occurred:<br>• User logon table additions reached maximum user threshold<br>• New privileged database user accounts were added | No exceptions noted. |
| | | Inspected tickets for a sample of automated alerts issued by the SQL monitoring functions to determine whether the alerts were reviewed and validated that database table and/or field changes had an associated change ticket or work order to justify the change, and the ticket or work order was authorized. | No exceptions noted. |
| 5.6 | IT management retroactively reviews elevated access instances to production databases on a monthly basis to validate that each instance of user access elevation to production databases via the DBTracks tool was appropriate based on a business need and | Inspected review results for a sample of months to determine whether IT management performed the review of the DBTracks elevated access log on a monthly basis to validate that each access instance had an associated change ticket or work order to justify the access, and the ticket or work order was authorized and identified issues were documented, investigated and resolved. | No exceptions noted. |

| **Control Objective 5:** Control Objective 5: Controls provide reasonable assurance that changes to application programs and related data management systems are tested, documented, approved and implemented. | | | |
|---|---|---|---|
| | ***Provided by Q2 Software, Inc.*** | ***Procedures Performed by RSM US LLP*** | |
| | **Control** | **Test Performed** | **Test Results** |
| | authorized. As part of the review, IT management validates that each access elevation instance had an associated change ticket or work order to justify the access, and the ticket or work order was authorized. IT management documents their review via the ticketing system, and includes investigation and resolution of identified changes without associated and/or authorized tickets or work orders. | Inspected a test DBTracks access request to determine whether the request was completely and accurately reflected in the elevated access log. | No exceptions noted. |
| 5.7 | An internally developed tool is used to monitor changes to certain high-risk data fields contained in the online banking production databases. The tool automatically tracks and logs changes to certain high-risk data fields. The compliance team reviews data field changes logged by the monitoring tool on a monthly basis. As part of the review, the compliance team validates that data field changes had an associated change ticket or work order to justify the change, and the ticket or work order was authorized. The compliance team documents their review via the ticketing system, and includes investigation and resolution of identified changes without associated and/or authorized tickets or work orders. The following data field changes are logged by the monitoring tool: | Inspected the configuration of the internally developed tool to determine whether it was configured to monitor changes to the following high-risk data fields contained in the online banking production databases:<br>• Q2_RecipientAccount (AccountNumber, ABA)<br>• Q2_FundsTransfer (ToAccount)<br>• Q2_GeneratedTransactions (TransactionAmount)<br>• Q2_WireTransfer (ToAccount)<br>• Q2_AchPpdCcdDetail (ABA, AccountNumber, Amount)<br>• Q2_ThirdPartyData (DataValue) | No exceptions noted. |
| | | Inspected the compliance team review of logged data field changes for a sample of months to determine whether the compliance team validated that data field changes had an associated change ticket or work order to justify the change, and the ticket or work order was authorized and the review was documented via the ticketing system, and included investigation and resolution of identified changes without associated and/or authorized tickets or work order. | No exceptions noted. |

| **Control Objective 5:** Control Objective 5: Controls provide reasonable assurance that changes to application programs and related data management systems are tested, documented, approved and implemented. | | |
|---|---|---|
| ***Provided by Q2 Software, Inc.*** | ***Procedures Performed by RSM US LLP*** | |
| **Control** | **Test Performed** | **Test Results** |
| • Q2_RecipientAccount (AccountNumber, ABA)<br>• Q2_FundsTransfer (ToAccount)<br>• Q2_GeneratedTransactions (TransactionAmount)<br>• Q2_WireTransfer (ToAccount)<br>• Q2_AchPpdCcdDetail (ABA, AccountNumber, Amount)<br>• Q2_ThirdPartyData (DataValue) | Inspected a test data change to determine whether the data field change was completely and accurately logged. | No exceptions noted. |

# V. Other Information Provided by Q2 Software, Inc.

The information included in this section of the report is presented by Q2 to provide additional information to user organizations and is not a part of Q2's description of controls placed in operation. The information in this section has not been subjected to the procedures applied in the examination of the description of Online Banking system controls related to the processing of transactions for user organizations and, accordingly, RSM US LLP expresses no opinion on it.

The company provides the following products and services that are in addition to those described in Section III of this report:

## *Business Continuity Planning*

In the event of loss of service availability due to disaster events, Q2 Software has developed a Business Continuity Plan for its hosted customers that consist of several key areas:

- Customer communication—to communicate the outage to affected customers and establish expectations related to the resumption of services based upon known information
- Execution of plan—to include any recovery of backup data, network availability or application services depending on the customer base affected and recovery checkpoint objectives
- Customer communication of resolution—to communicate the root cause of the outage and the mitigation plan to address similar events in the future

Q2 Software offers Business Continuity Plans to customers who are hosted at the Q2 Software data centers. Customers that host Q2 Software applications at their own data center are responsible for the development and execution of their own Business Continuity Plan. However, Q2 Software can assist these customers (as a normal customer service event) in the development and execution of their own Business Continuity Plan.

Business continuity and disaster recovery plans are reviewed and approved by corporate management on an annual basis. The company's disaster recovery strategies include replication and backup/restore procedures, among other considerations. Business continuity and disaster recovery plans, including restoration of backups, are tested on an annual basis. Results are communicated to corporate management.

## *Q2 consoles*

Many operational controls are available directly to financial institution customers via the Q2Central operations and administration console, whereby financial institutions have the ability to:

- Monitor system alerts
- Manage groups, customers, users and user rights
- Manage electronic banking transactions
- Process electronic banking transactions
- Communicate directly with their electronic banking customers
- Manage system configurations
- Administer system changes
- Review audit log information

The Q2Central application places responsibility on the customer for the administration of electronic banking services and, therefore, limits the involvement of Q2 personnel in daily electronic banking operations.

## *Q2 Software, Inc. Informational Documents*

The company maintains other information that may be helpful to its financial institution customers and interested parties, including the following:

- Q2 website address: www.q2.com
- Q2 management biographies: http://q2.com/our-story
- Q2 product sheets for:
    - Q2Mobile
    - Q2Online
    - Q2Voice
- Q2 policies, including the following:
    - Q2Policy—Mobile Device Policy
    - Q2Policy—Data Retention and Disposal Policy
    - Q2Policy—Technology Availability Plan

These documents are available as requested or needed by the company's customers.

## *Management Responses to Testing Exceptions*

Q2 Software has taken measures to address the exceptions to the control objective identified in this report as summarized below.

| Control | Test Results | Management Response: |
|---|---|---|
| Control 3.2<br>New user access and elevated access requests are submitted through the ticketing system. Access is assigned based on an access matrix outlining access needs by position. The access matrix is reviewed and approved by management on a quarterly basis. | Exceptions noted.<br>For six of 25 new accounts sampled, documentation of the access request approval was not documented and retained. | As part of our continued process improvement, Q2 implemented controls and processes during the report period; however, all controls were not fully implemented or operating as expected during the control period. Q2 management expects that these controls will be fully implemented and operating effectively during Q1 2021 |
| Control 3.7<br>Server and database password authentication configurations are setup to enforce a password policy. | Exceptions noted.<br>For seven out of seven databases sampled, a password policy was not configured to be enforced for service accounts with write-access. | The local SQL database service accounts are created with a password minimum length of 11 characters including password complexity requirements. When using the "enforce password policy enabled" feature in the database, the database enforces Q2's group policy that is configured to require a 14 character password. Therefore, when "Enforce Password Policy" is enabled for the local SQL database accounts, an error occurs and the application will not respond. Q2 will place the SQL database accounts in a different Group Policy that has a minimum password requirement of 11 characters. |