Confirmation.com

CAPITAL CONFIRMATION, INC.

INDEPENDENT PRACTITIONER'S TRUST SERVICES REPORT FOR THE CONFIRMATION.COM™ SYSTEM

FOR THE PERIOD OF DECEMBER 1, 2017, TO MAY 31, 2018

Attestation and Compliance Services

schellman
Quality, above all.

INDEPENDENT PRACTITIONER'S TRUST SERVICES REPORT

To the Management of Capital Confirmation, Inc.:

We have examined management's assertion that during the period December 1, 2017, to May 31, 2018, Capital Confirmation, Inc. ("CCI") maintained effective controls over the Confirmation.com™ system (the "system") , including controls over the privacy of personal information collected by the system, for the security, availability, processing integrity, confidentiality and privacy principles set forth in the 2016 TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Principles and Criteria)* (applicable trust services criteria), to provide reasonable assurance that

- the system was protected against unauthorized access, use, or modification to meet the entity's commitments and system requirements;
- the system was available for operation and use to meet the entity's commitments and system requirements;
- system processing was complete, valid, accurate, timely, and authorized to meet the entity's commitments and system requirements;
- information designated as confidential is protected to meet the entity's commitments and system requirements;
- personal information is collected, used, retained, disclosed, and disposed to meet the entity's commitments and system requirements; and
- CCI complied with its commitments in its privacy notice.

As indicated in the description, CCI uses Equinix, Inc. ("Equinix") for data center hosting and infrastructure monitoring. The description indicates that certain applicable trust services criteria can be met only if certain types of controls that management expects to be implemented at Equinix are suitably designed and operating effectively. The description presents CCI's system; its controls relevant to the applicable trust services criteria; and the types of controls that CCI expects to be implemented, suitably designed, and operating effectively at the Equinix to meet certain applicable trust services criteria, and compliance with the commitments in CCI's privacy notice. The description does not include any of the controls expected to be implemented at Equinix. Our examination did not extend to the services provided by Equinix, or their compliance with the commitments in their privacy notice, and we have not evaluated whether the controls management expects to be implemented at Equinix have been implemented or whether such controls were suitably designed and operating effectively throughout the period December 1, 2017, to May 31, 2018.

CCI's management is responsible for this assertion. Our responsibility is to express an opinion based on our examination. Management's description of the aspects of the Confirmation.com™ system covered by its assertion is attached. We did not examine this description, and accordingly, we do not express an opinion on it.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of CCI's relevant controls over the security, availability, processing integrity, confidentiality and privacy of personal information of the Confirmation.com™ system; (2) testing and evaluating the operating effectiveness of the controls; (3) testing compliance with CCI's commitments in its privacy notice; and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of the nature and inherent limitations of controls, CCI's ability to meet the aforementioned criteria and the commitments in its privacy notice may be affected. For example, controls may not prevent or detect and correct error or fraud, unauthorized access to systems and information, or failure to comply with internal and external

policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

In our opinion, management's assertion referred to above is fairly stated, in all material respects, in conformity with CCI's privacy notice, based on the AICPA and CPA Canada applicable trust services criteria.

Schellman & Company, LLC

Tampa, Florida
July 9, 2018

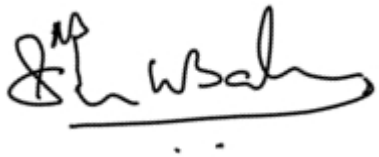
MANAGEMENT'S ASSERTION

July 9, 2018

During the period December 1, 2017, to May 31, 2018, Capital Confirmation, Inc. ("CCI") maintained effective controls over the Confirmation.com™ system (the "system"), including controls over the privacy of personal information collected by the system, for the security, availability, processing integrity, confidentiality and privacy principles set forth in the 2016 TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Principles and Criteria)* (applicable trust services criteria), to provide reasonable assurance that:

- the system was protected against unauthorized access, use, or modification to meet the entity's commitments and system requirements;
- the system was available for operation and use to meet the entity's commitments and system requirements;
- system processing was complete, valid, accurate, timely, and authorized to meet the entity's commitments and system requirements;
- information designated as confidential is protected to meet the entity's commitments and system requirements;
- personal information is collected, used, retained, disclosed, and disposed to meet the entity's commitments and system requirements; and
- CCI complied with its commitments in its privacy notice.

The attached system description identifies the aspects of the Confirmation.com™ system covered by the assertion.



Mr. Chris Schellhorn
Chief Executive Officer
Capital Confirmation, Inc.

Mr. Suresh Babu
Chief Information Officer
Capital Confirmation, Inc.

Mr. Brian Fox
President & Founder
Capital Confirmation, Inc.

SYSTEM DESCRIPTION OF THE CONFIRMATION.COM™ SYSTEM

Company Background

Capital Confirmation, Inc. (CCI) is a provider of computerized audit confirmation services. CCI provides patented Software as a Service (SaaS) solution to over 250,000 clients for audit confirmations. CCI's clients include major financial institutions, investment and brokerage firms, law firms, and large accounting firms, as well as public, private, not-for-profit and government entities. Through a secure centralized clearinghouse, this service allows for the automation of millions of audit confirmations for the purpose of improving turnaround time and providing authentication for both requestors and responders. CCI is a privately held company, headquartered in Brentwood, Tennessee.

In 2013, CCI's information technology (IT) division formed a wholly owned subsidiary named Confirmation Technology Services, LLC (CTS), headquartered in Delray Beach, Florida. CTS retained its responsibilities for supporting the IT systems that are utilized by the CCI computerized audit confirmation services. The executive management of CCI retained shared leadership over the existing CCI parent company and the new CTS subsidiary. Any references to CCI within this report are inclusive of its wholly owned subsidiary, CTS.

Description of Services Provided

Confirmation.com™ is an online confirmation process designed to increase efficiency while providing patented fraud detection/prevention capabilities to the requestors and responders of audit confirmation requests. Where case studies show that the paper confirmation process is circumvented by fraudsters, CCI provides independent, third party validated confirmation requests and responses.

Features include automatic document management, a secured network and the ability to download confirmations and confirmation reports directly into electronic work files eliminating manual steps that are often required with traditional manual paper-based confirmations. Confirmation.com™ is designed to ensure that both requestors and responders of confirmations are authorized and authenticated, and to provide complete control to both parties while improving and streamlining the confirmation process.

Due to the inherent inefficiency and the ease of circumventing the paper confirmation process for fraudulent purposes, confirmation requestors and responders may not be identifying confirmation fraud and may be deficient in the resources necessary to ensure the validity of the requestor and responder and may therefore be exposed to risk. This creates the need for a secure clearinghouse for audit confirmations where the parties in the confirmation process are independently authorized and authenticated. Confirmation.com™ streamlines the confirmation process by replacing the paper-based confirmation process with secure electronic confirmation processes where responses move toward real-time. The authorization and authentication procedures not only help requestors and responders detect fraud but also are designed to serve as a deterrent or preventative measure against those hoping to circumvent the audit confirmation process.

The Confirmation.com™ online confirmation solution provides legal confirmations, accounts payable (AP) and accounts receivable (AR) confirmations along with more than 50 types of bank confirmations, such as the following:

- Cash
- Debt
- Alternative investment
- Bond issue
- Commercial real estate
- Derivatives
- Escrow account
- Letter of credit
- Line of credit
- Money market fund
- Mortgage debt
- Pension plan assets
- Safe deposit
- Securities

Confirmation.com™ provides the following core capabilities:

- Multiple layers of authentication and security controls to validate the authenticity of responders
- Web-based interface for performing audit confirmations
- A record of activity on every confirmation that provides a traceable path of accountability to each individual involved in the confirmation process

Infrastructure and Software

The Confirmation.com™ system consists of a three-tier architecture running Windows Server 2008 platforms for web server applications, structured query language (SQL) server database services and other related transaction processing functions.

CCI personnel manage the architecture of the system including the production and high availability servers maintained within physically secured facilities and the encryption of application data within the database. CCI is also responsible for the secure handling, storage, backup up, transmission, and destruction of application data and related media.

The in-scope infrastructure utilized by CCI to support the Confirmation.com™ system consists of multiple applications, operating system (OS) platforms and databases, as summarized in the table below:

Primary Infrastructure		
Production Application	**Business Function Description**	**Physical Location**
Windows Active Directory (AD) / Network Domain Controllers	A Windows AD domain controller is utilized to enforce global policy configurations and perform logical access and authentication administration for the network.	Equinix (Miami, FL / Culpeper, VA)
Confirmation.com™ Web Application	Publicly facing web application used to facilitate Confirmation.com™ services including fraud detection / prevention capabilities to the requestors and responders of the audit confirmation requests.	Equinix (Miami, FL)
Confirmation.com™ Databases	SQL Server databases containing information about Confirmation.com™ application users, transactional data, and logging activity, as well as project related sourcing and distribution documents.	Equinix (Miami, FL / Culpeper, VA)
Iron Mountain Live Vault / SQL Management Studio	Automated backup system software and network of servers that provide backup and recovery for subscribing customers.	Equinix (Miami, FL / Culpeper, VA)
SiteScope	Enterprise monitoring applications that provide real time monitoring and alerts related to availability, capacity, performance of infrastructure hardware and intrusion prevention system (IPS) services.	Equinix (Miami, FL / Culpeper, VA)
ChangeNet	Automated ticketing software that provides centralized storage.	Equinix (Miami, FL)
Team Foundation Server	Workflow for management of infrastructure issues and resolution.	CCI (Delray Beach, FL)

Primary Infrastructure		
Production Application	**Business Function Description**	**Physical Location**
Symantec	Automated antivirus protection software that provides updates of virus definitions and scanning for known viruses or infections on protected devices.	Equinix (Miami, FL) CCI (Delray Beach, FL)
Malwarebytes	Automated malware detection and removal of viruses, worms, trojans, rootkits, dialers and spyware software that provides access to rapid response malware database and heuristics updates and real-time active malware prevention; blocks known threats; and prevents new Zero Day malware infections.	Equinix (Miami, FL) CCI (Delray Beach, FL)
KillDisk	Information disposal software that destroys all data on hard disks, USB drives and floppy disks completely, excluding any possibility of future recovery of deleted files and folders.	Equinix (Miami, FL) CCI (Delray Beach, FL)

People

CCI serves customers around the world with its U.S.-based employees supporting the business overall. The CCI teams of IT personnel, who adhere to quality assurance (QA) testing and data security standards, and management personnel collaborate to support the Confirmation.com™ services system architecture and business processes. A subset of these teams executes in the following functional areas:

- Executive management – responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives.
- Business operations, customer support, and enrollment – responsible for providing support and services to user entities of the system; validates confirmation requestor identities and complete verification checklists.
- IT operations - manages, monitors, and supports user entities' information and systems from unauthorized access and use while maintaining integrity and availability; responsible for monitoring and tracking system performance metrics.
- Systems administrators (approved by executive committee) – activates customer accounts in the Confirmation.com™ system.
- Development - responsible for developing code to support and enhance Confirmation.com™.

Procedures

CCI's procedures related to the Confirmation.com™ system and the supporting services, respectively, are included below.

Physical and Environmental Security

Physical access to IT computing resources is restricted by office suite doors secured by dead bolt locks 24 hours per day at the Delray Beach, Florida, office facility and by cipher locks at the Brentwood, Tennessee, corporate office facility. Processes and procedures are in place for the control of visitor and temporary access to the facility. Visitors are required to present government-issued identification and sign a visitor log maintained by CCI personnel. Upon termination of an employee, physical access keys for the Delray Beach, Florida, office facility

are collected by the employee's manager, and human resources at the Brentwood, Tennessee, corporate office facility will request combination lock change in locations where the terminated employee had access.

Production and high availability servers are maintained within physically secured facilities and application data is encrypted within the database. Application data and related media are also secured as handled, stored, backed up, transmitted and/or destroyed. CCI has contracted with Equinix to provide data center hosting and infrastructure monitoring services. CCI utilizes Equinix's Miami, Florida, location as their primary data center facility with a secondary production site located in Culpeper, Virginia. The Equinix data centers were not included in the scope of this examination.

The CCI corporate office facilities are equipped with fire detection and suppression devices, heating, ventilating and air conditioning (HVAC) units and uninterruptible power supply (UPS) units for the safeguard of IT computing resources and employee workstations. Fire suppression equipment third party inspections occur on an annual basis and are employed by the multi-tenant office building facility's operations team.

Logical Access, Authentication and Authorization

CCI employs an information security program consisting of a set of regularly reviewed policies, standards, and procedures that define how resources are provisioned and access controls are managed. Access control standards define the requirements for user account password policies and network access. Changes in the environment are reflected in security systems in a timely manner through both automated and manual processes. CCI has documented and published Standards, Guidelines, and Standard Operating Procedures. The policies are approved by the executive committee, distributed to employees, and formally acknowledged by each employee.

Access to IT computing resources including desktops and servers is restricted by the implementation of identification, authentication, and authorization mechanisms. Internal users are required to authenticate through the network layer prior to being able to access applications, member load and premium reconciliation processing data, and key financial reports. Network user accounts and authentication is governed by group policies in Microsoft AD on the domain controller. Group policies are configured to enforce use of a valid user id (UID) and minimum password requirements including length, expiration, complexity, history, and account lockout. The ability to administer the network domain is restricted to user accounts accessible by persons authorized IT personnel.

Network audit logs are monitored by an automated monitoring application. Network and database audit logs are reviewed on a daily basis as a component of the daily operations checklist performed by IT operations personnel. IT operations personnel review the audit logs for account logins, account management, directory services, and policy changes.

The CCI Operations and Security Policies and Procedures document the formalized process for requesting, establishing, suspending, and closing a user account. Upon hire or termination of an employee, the respective manager submits a request ticket to CCI's IT operations personnel. IT operations personnel complete the ticket request by granting access to the CCI network and application systems for new hires and disabling user access to the network and application systems for terminated employees.

A client user must provide proper authorization for the use of Confirmation.com™ for electronic audit confirmations by both the requestor and responder. To ensure proper authorization to request confirmations, the application restricts client setup to authenticated requestor accounts and requires an electronic authorization from the client. The client is required to provide the authorization via electronic signature to grant the authority to request confirmations. This authorization expires after 365 days. Confirmation requests are limited to the requestor who received the authorization from the client. The application restricts incomplete confirmation requests and requires a bank/financial institution/law firm, an account number, an account type, an authorized signer, and balance request date.

Customer support agents complete a checklist to document re-inspections for a random sample of 10% of requestor and responder entities and associated users on a semi-annual basis. Re-inspections are performed for each requestor and responder entity and its associated users at least once every five years. These re-inspections are reviewed by a CCI director, Confirmation.com™ systems administrator, or officer.

Logical Access Requests and Access Revocation

Upon hire or termination of an employee, the respective manager submits a request ticket to IT operations personnel. IT operations personnel complete the ticket request by granting access to the CCI network and application systems for new hires and disabling user access to the network and application systems for terminated employees. New hire and termination access follow the change management process documented in the CCI Operations and Security Policies and Procedures document.

Authenticating proper source establishes the fundamental guidelines and practices for properly authenticating and authorizing users of CCI's service. A user is defined as a requestor of or a responder to a confirmation request and includes the client for whom the confirmation request is made. A requestor can be, but is not limited to, individual employees of an accounting firm. A responder can be, but is not limited to, individual employees of a financial institution, investment and brokerage firms, law firms, and companies. A client can be, but is not limited to, a public, private, governmental, or not-for-profit entity.

To be granted access to the application, a user must first enroll and be validated. Enrollment personnel utilize authentication methods for validations including, but not limited to public web sites, third party authentication services, state licensing boards, governmental agencies, and industry associations. To ensure validation occurs, CCI utilizes validation checklists, which are reviewed by a CCI director, Confirmation.com™ systems administrator, or officer, to help ensure the required activities for requestor and user validation such as physical address and contact information are completed.

To enroll in Capital Confirmation's service the user is required to register on Confirmation.com™. Upon enrolling, the enrollee is prompted to enter their personal and firm information including e-mail address and agrees to applicable service and user agreements. The application is configured to automatically validate the e-mail domain of all enrollees against authenticated requestor entities. After the user has entered their enrollment account information validated e-mail domains are required to verify their e-mail address prior to account activation. The ability to enroll and grant user account permissions to respond to audit confirmations is restricted to authenticated responder supervisors, lawyers, and legal professionals.

Change Management

Documented policies and procedures are maintained to help guide personnel in the change management process. Additionally, documented coding standards policies and procedures are maintained to help guide personnel in the application code development process.

CCI has established corporate procedures that outline the requirements of the change management process. Every change to a CCI resource such as operating systems, computing hardware, networks, and application maintenance is subject to the Change Management Policy, documented in the CCI Operations and Security Policies and Procedures document, and must follow the Change Management Procedures.

For example, application changes are documented and tracked within a ticketing system; once a change is requested, it is assigned a unique change number in the ticketing system. Once the code has been developed, QA testing is completed in a test environment that is logically separated from the production environment. Once QA testing has completed successfully, the change manager approves the change for implementation. Evidence of successful QA testing is evidenced by an e-mail to the change manager, and the change manager approves the change via e-mail to operations personnel. The build manager then compiles the changes into a release package that is implemented by authorized operations personnel. Operations personnel send an e-mail notification to evidence successful implementation.

CCI safeguards source code within a version control application that restricts write access to authorized personnel. Additionally, the ability to implement changes is restricted to authorized personnel and no users with source code write access have the ability to implement changes. For added assurance, an automated file monitoring tool is utilized to calculate a checksum of the production files and identify changes to the contents of the files. Reports from the file monitoring tool are reviewed by operations personnel on a daily basis.
Systems Monitoring

The IT infrastructure is configured for redundancy and certain network devices as well as the Confirmation.com™ websites are monitored for uptime and other operational statistics. The enterprise monitoring application is configured to notify IT operations personnel via e-mail if certain thresholds such as connectivity or availability are met or exceeded. Operations personnel generate system performance reports and complete daily checklists to help ensure that agreed service levels are maintained. Problem management systems are utilized to log and track operational and application issues through resolution.

An automated patch management system is utilized to help ensure software/hardware products and operating systems patches are up to date and installed according to predetermined timeframes. Antivirus and antimalware software is maintained on centralized servers to detect and prevent the transmission of virus signatures, malware, and ransomware within the production network. The central antivirus and antimalware servers are configured to enforce scheduled scans on registered client servers and workstations, as well as monitor, deploy, and install definition updates on the devices.

Data Backup and Disaster Recovery

CCI maintains formalized policies and procedures around the data backup, data recovery, service level performance, incident procedures, and systems monitoring and maintenance processes. Automated backup systems are utilized in conjunction with a replication tool to perform daily backups of the application system and database, and automatically replicate the daily backup data to a third-party storage provider's secure off-site location. Backup processing is monitored for accuracy and completeness and logs are reviewed on a daily basis. Potential issues are identified and logged for management review, follow-up, and resolution. The automated backup system are also configured to notify operations personnel via e-mail regarding the success or failure of the backup performed.

Data restoration activities are performed by IT operations personnel as a component of normal business operations, and the status of restorations is stored within the automated backup system log history. The ability to retrieve backup data is restricted to user accounts accessible by authorized operations personnel. In addition, backup recovery is tested quarterly to help ensure completeness and accuracy of data backups as well as to familiarize IT operations personnel with recovery procedures.

Data classification is governed by the Information Sensitivity Policy. Data classified as confidential is encrypted and secured as it is handled, stored, transmitted, and/or destroyed. Transactions and customer data are retained for a minimum of ten years in accordance with the retention policy and records retention schedule. The automated backup system and replication tool are configured to encrypt database and network backups at rest and in transit via 256-bit Advanced Encryption Standard (AES-256) encryption.

CCI has developed a business resumption plan (BRP) to assist with the management and handling of operations in the event of a serious disruptive crisis. The BRP identifies key business processes comprising those functions whose loss could cause a major impact to CCI within a few hours. It contains information on emergency contact details, strategies to mitigate impact, procedures to be implemented and communications to be followed in response to a serious disruptive event. A risk assessment process will be repeated on a periodic basis to help ensure that changes to the processing and physical environments are reflected in recovery planning. CCI administration recognizes the low probability of severe damage to data processing, telecommunications or support services capabilities that support the company. Nevertheless, because of the potential impact to CCI, a plan for reducing the risk of damage from a disaster is considered vital. The BRP is designed to reduce the risk to an acceptable level by ensuring the restoration of critical processing as quickly as possible and essential production operations within a timely manner. The BRP identifies the critical functions for business resumption and provides guidelines for ensuring that personnel and resources are available for disaster preparation and response.

Network Security

CCI maintains a formally documented network diagram outlining the CCI production network. A demilitarized zone (DMZ) subnetwork separates the internal network from external Internet traffic; untrusted inbound Internet traffic terminates in the DMZ. A firewall system is in place to provide perimeter security for the internal network and is configured to deny any type of network connection not explicitly authorized by a firewall rule. The firewall system is also configured with parameters to mask internal IP addresses via network address translation (NAT). The firewall system is setup in a clustered pair for high availability failover; a primary firewall operates in an active

mode and a secondary firewall in standby mode. Failover is automated in the event that the primary firewall fails or is compromised. Firewall logs are reviewed by operations personnel on a daily basis and evidenced on the daily operations checklists.

Formally documented policies and procedures are in place to help guide personnel in the firewall system change process. Changes are documented and tracked in an automated ticketing system; once requested, a unique change number is created within the ticketing system. Changes are approved prior to implementation and evidence of approval is documented via e-mail. The ability to administer the firewall system is restricted to authorized IT personnel.

Encrypted virtual private network (VPN) connections are utilized to help ensure the privacy and integrity of the data passing over the public network. VPN sessions are encrypted using the AES-256 algorithm. VPN access is revoked as a component of the employee termination process and the ability to administer the VPN system is restricted to authorized IT personnel.

The Confirmation.com™ website utilizes transport layer security (TLS) 1.2 encryption to secure Internet browser sessions. Additionally, an intrusion prevention system (IPS) is utilized to monitor network segments with Internet connectivity. IT operations personnel perform internal vulnerability assessment of the production network on a quarterly basis and obtain assessment reports as evidence that an external vulnerability testing is performed on a monthly basis. On a daily basis, IT operations personnel obtain assessment reports as evidence that a network vulnerability scan is performed. A web application firewall is in place to monitor encrypted traffic and identify vulnerabilities to the Confirmation.com™ application and is configured to generate on-screen alerts when predefined security events are detected.

Incident Response

CCI has implemented formal incident response and escalation procedures for reporting security, availability, processing integrity, confidentiality and privacy incidents. These procedures are provided to both internal and external users to guide them in identifying and reporting failures, incidents, concerns, and other complaints. Incidents are tracked in the ticketing system. Management meets weekly to discuss incidents and provide resolutions.

Electronic Signatures

The Confirmation.com™ application utilizes legally valid electronic signatures which are restricted to a single unique user account. Each user account is restricted to one role of requestor, client, or responder and the ability to request or respond to confirmations is restricted to the assigned user accounts. In addition, users who obtain user accounts are bound to the terms of the online user agreement and services agreement.

Privacy

CCI's roles and responsibilities for information privacy policy designates customer information that is considered private (e.g., credit card numbers, account numbers, user's personal information) as "most sensitive" and treats such information accordingly.

CCI has implemented an information privacy committee (IPC), comprised of both CCI executive management, responsible for governance and oversight of the enterprise information privacy program.

The IPC performs the following:

- Analyzes and manages institutional risks
- Reviews and recommends policies, procedures, and standards
- Ensures consistency in disciplinary processes for violation

CCI has identified an information privacy officer responsible for directing, defining, and implementing the company information privacy program. The information privacy officer performs the following:

- Establishes standards for business use of information

- Assigns administrative responsibility to business owners
- Considers developments in technology and the impact of applicable laws or regulations on the entity's confidentiality and privacy policies, seeking legal counsel review as necessary
- Monitors compliance and review violations
- Coordinates the development and maintenance of information privacy policies and standards
- Ensures implementation of policies, and, documentation of process and procedures for guaranteeing the privacy of information

Data

Data provided by CCI to user entities includes confirmation reports for AR and AP transactions uploaded by the user entity. Confirmation.com™ application data includes transactional and customer data and application activity logs. Application data is subject to the corporate Data Retention and Information Sensitivity Policies, which are intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed without proper authorization. Customer data could include personally identifiable information, or PII. Legal confirmation requests could contain protected health information, or PHI, and may be stored on CCI's systems as a document attachment. CCI classifies customer data as confidential.

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
AR and AP transactions	CCI	Confidential
Transactional and customer data and application activity logs	CCI	Confidential
Customer data that could include PII	CCI	Confidential
Legal confirmation requests that could contain PHI and may be stored on CCI's systems as document attachments	CCI	Confidential

Data utilized by CCI also includes information received from monitoring applications to address security and infrastructure events, in addition to human resource records that are utilized to perform user access provisioning and revocation procedures.

Significant Changes During the Review Period

No relevant changes to the Confirmation.com™ system occurred during the review period.

System Boundaries

As outlined in the 2016 TSP section 100A, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* a system is designed, implemented, and operated to achieve specific business objectives (for example, delivery of services, production of goods) in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures and data.

Subservice Organizations

The data center hosting and infrastructure monitoring services provided by Equinix, Inc. (Equinix) were not included within the scope of this examination. Therefore, the description does not address the (a)(i)(4) and (a)(i)(5)(b) criteria in Section 2.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at Equinix, alone or in combination with controls at CCI, and the types of controls expected to be implemented at Equinix to meet those criteria.

Control Activity Expected to be Implemented by Equinix	Applicable Trust Services Criteria
Equinix is responsible for ensuring physical access control systems are in place to restrict access to and within the data centers housing the offline storage, backup data, production systems, and media (including portable media), to properly authorized individuals.	CC5.5, CC5.7
Equinix is responsible for the design, development, implementation, operations, maintenance and monitoring of environmental security safeguards to meet availability commitments and requirements. Additionally, Equinix is responsible for ensuring that a recovery facility is in place to permit the resumption of IT operations in the event of a disaster at its data center.	A1.2, PI1.1

CCI has not delegated any responsibility of the personal information life cycle to Equinix.

PRIVACY NOTICE

CCI provides the privacy notice to individuals about whom personal information is collected, used, retained, disclosed, and disposed of or anonymized. Therefore, the description does not address the (a)(i)(12) criteria in Section 2. The below Privacy Notice has been prepared in conformity with the relevant criteria set forth in TSP section 100.

CCI posts a link to its privacy notice within the footer of its website. The following privacy notice utilized for the purpose of this examination was obtained from https://www.confirmation.com/Modals/PrivacyPolicy.aspx.

Capital Confirmation, Inc. PRIVACY STATEMENT

Effective on: April 16, 2018

This privacy policy applies to www.confirmation.com, bba.confirmation.com, edu.confirmation.com, and www.creditconfirm.com ("Confirmation Website(s)") owned and operated by Capital Confirmation, Inc. (“Capital Confirmation”). This privacy policy describes how Capital Confirmation collects and uses the personal information you provide on the Confirmation Website(s). It also describes the choices available to you regarding our use of your personal information and how you can access and update this information.

1. What personal data and protected health information (PHI) Capital Confirmation collects.
2. What personal data third parties collect through the Website(s).
3. What organization collects the information.
4. How Capital Confirmation uses the information.
5. With whom Capital Confirmation may share user information.
6. What choices are available to users regarding collection, use and distribution of the information.

7. What types of security procedures are in place to protect the loss, misuse or alteration of information under capital Confirmation's control.
8. How users can correct any inaccuracies in the information.

Information Collection and Use

Registration

In order to use the Confirmation website(s), a user must first complete the registration form. During registration a user is required to give professional and personal contact information (such as name and email address). We use this information to validate our users, and to therefore grant access to our service. We also ask our accounting customers to provide their CPA registration/credentialing information in order to validate his/her status to include employment verification.

Order

We request information from the user on our order form. A user must provide contact information (such as name, email, and shipping address) and financial information (such as credit card number, expiration date). This information is used for billing purposes and to fill customer's orders. If we have trouble processing an order, the information is used to contact the user.

Third party information is collected on the site (such as client information entered for the purpose of conducting confirmations of accounts) The following are the types of information that are requested for a client: contact information, client's name, client contact name, client address, client contact's email address. This information is used to validate the client users of the service. A welcome email is generated to the clients to notify them that they have been set up on the service by their accountant and to provide them notification of their initial security codes. These emails are only used for
the primary purpose of providing the service of the site and are not used for any secondary purposes.

Information Use

Capital Confirmation, through its online service production Confirmation website(s), collects three types of information:

1. General Personal Data
2. Customer Financial Information
3. Protected Health Information (PHI)

General Personal Data is used to validate the user, associate transactional confirmation activities including authorization, determine access permissions, and to facilitate communications from the site. The customer is free to modify this information at any time.

Customer Financial Information includes certain bank/company balance information that is stored in our database on a temporary basis, and credit card payment information provided by the customer at the time of the payment for the provision of services.

PHI may be stored on Capital Confirmation’s HIPAA compliant system as a document attachment to a legal confirmation request when/if this information is deemed pertinent to the legal confirmation audit.

All Customer Financial information or legal confirmation attachments containing PHI residing within Capital Confirmation's secure processing controls will be maintained and stored according to our stated security and privacy policies. Capital Confirmation takes no responsibility for Customer Financial Information once this data is no longer within Capital Confirmation’s control (e.g., data downloaded by user, or mailed confirmations). The Confirmation website(s) serve the function of an on-line provider of balance assurance services for its customers.

This service is designed for use by accountants in their conducting of audit procedures as described by Generally Accepted Accounting Standards (GAAS).

We process General Personal Data only for so long as is necessary for the purpose(s) for which it was originally collected, after which it will be deleted or archived except to the extent that it is necessary for us to continue to comply with our legal obligations, resolve disputes, and enforce our agreements.

Profile

We store information specifically given to us by our users through the account set up process, and/or the account edit process. In addition, we store IP address, browser type, Internet Service Provider (ISP) and access times. We do not store information provided through the use of cookies. A profile has stored information that provides the company with information describing the end user of our service. All such collected information is used only for the conducting of the provision of our service.

Cookies and Other Tracking Technologies

We Capital Confirmation and our analytics or service providers use cookies or similar technologies in analyzing trends, administering the site, tracking users' movements around the site and to gather demographic information about our user base as a whole. We may receive reports based on the use of these technologies by these companies on an individual as well as aggregated basis.

We use cookies for to remember users' settings (e.g. language preference), for authentication. Users can control the use of cookies at the individual browser level. If you reject cookies, you may still use our site, but your ability to use some features or areas of our site may be limited.

Online Advertising

We use Google AdWords, Google Analytics, Google Display Network, Adobe Analytics, and HubSpot to track user behavior and manage our advertising on other sites. Our third party partners may use technologies such as cookies to gather information about your activities on this site and other sites in order to provide you advertising based upon your browsing activities and interests. If you wish to not have this information used for the purpose of serving you interest based ads, you may opt-out by clicking here. Please note this does not opt you out of being served ads. You will continue to receive generic ads.

Log Files

Like most standard website(s) servers we use log files. This includes Internet Protocol (IP) addresses, browser type and Internet Service Provider (ISP), referring/exit pages, operating system and access time. Capital Confirmation and its production Confirmation Website(s), use log files only to track errors in the system. Log file information is not tied to a user's personal data.

Information Collected for Our Clients

Capital Confirmation collects information under the direction of its clients and has no direct relationship with the individuals whose personal data it processes. If you are a customer of one of our Clients and would no longer like to be contacted by one of our Clients that use our service, please contact the Client that you interact with directly. We may transfer personal information to companies that help us provide our service. Transfers to subsequent third parties are covered by the service agreements with our Clients.

An individual who seeks access, or who seeks to correct, amend, or delete inaccurate data should direct his query to the Capital Confirmation's Client (the data controller). If requested to remove data we will respond within 30 days.
We will retain personal data we process on behalf of our Clients for as long as needed to provide services to our Client. Capital Confirmation will retain this personal information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements.

Communications from the Site

Core Communications

These include email, mail, and call communications to facilitate the processing of audit confirmations, announce new enhancements to the service, aid in common user account administration functions, distribute information on upcoming site maintenance, and to provide notice of various updates to our terms of service or policies. These also include communications designed to educate and provide resources to both new and existing users on how to use the application, welcome emails, training sessions, and Responder Network updates.

Customer Support

We communicate with users on a regular basis to provide requested services, and in regard to issues relating to their account we reply via email or phone in accordance with the user's wishes.

Marketing Communications

We may from time to time send emails or mail to provide you with information regarding new product and service offerings, product and service notifications, and/or complimentary resources.

Generally, you may not opt-out of Customer Support or Core Communications. If you do not wish to receive them, you have the option to deactivate your account. If you do not wish to receive marketing communications you can simply not consent to receiving them (if your location requires consent), use the “Manage Your Preferences” and “Unsubscribe” links provided within each marketing email message, or contact Customer Support at Customer.Support@confirmation.com.

Sharing

We will share your personal data or legal confirmation attachments containing PHI with third parties only in the ways that are described in this privacy policy. We do not sell your personal data or legal confirmation attachments containing PHI to third parties.

Legal Disclaimer

In certain situations, Capital Confirmation may be required to disclose personal data or legal confirmation attachments containing PHI in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

Though we make every effort to preserve user privacy, we may also need to disclose personal data or legal confirmation attachments containing PHI when required by law such as to comply with a subpoena, bankruptcy proceedings, or similar legal process when we believe in good faith that disclosure is necessary to protect our rights, protect your safety or the safety of others, investigate fraud, or respond to a government request.

Aggregate Information (non-personal data)

We do not share aggregated demographic information with our partners and advertisers. These are the instances in which we will share users' personal data or legal confirmation attachments containing PHI:

Third Party Intermediaries

We use PCI-DSS compliant outside credit card processing companies to bill users for services. These companies do not retain, share, store, or use personal data for any secondary purposes.

Business Transitions

In the event Capital Confirmation goes through a business transition, such as a merger, being acquired by another company, or selling a portion of its assets, users' personal data or legal confirmation attachments containing PHI will, in most instances, be part of the assets transferred. Users will be notified via prominent notice on our website(s) for 30 days prior to a change of ownership or control of their personal data or legal confirmation attachments containing PHI. If as a result of the business transition, the users' personally identifiable

information or legal confirmation attachments containing PHI will be used in a manner different from that stated at the time of collection they will be given choice consistent with our notification of changes section prior to the information being used for the new purposes.

Surveys & Contests

From time-to-time our site requests information from users via surveys or contests. Participation in these surveys or contests is completely voluntary and the user therefore has a choice whether or not to disclose this information. The requested information typically includes contact information (such as name and shipping address), and demographic information (such as zip code). Contact information will be used to notify the winners and award prizes. Survey information will be used for purposes of monitoring or improving the use and satisfaction of this site. Users' personally identifiable information is not shared with third parties unless we give prior notice and choice. Though we may use an intermediary to conduct these surveys or contests, they may not use users' personal data for any secondary purposes.

Security

This Website(s) takes every precaution to protect our users' information. When users submit sensitive information via the Website(s), their information is protected both online and offline.

The Confirmation Website(s)s are entirely encrypted and protected using 256 bit encryption with a public RSA 2048 bit key for SSL Extended Validation Certificates with Server Gated Cryptography by DigiCert for internet communications. This means that when our registration/order form asks users to enter sensitive information (such as credit card number), that information is encrypted. While we use SSL encryption to protect sensitive information online, we also use appropriate technical and organizational measures to protect user-information offline. All of our users' information, not just the sensitive information mentioned above, is restricted in our offices. Only employees who need the information to perform a specific job (for example, our billing clerk or a Customer Support representative) are granted access to personal data. The servers that store personal data are in a secure environment, in a hardened hosting facility.

However, no method of transmission over the Internet, or method of electronic storage, is 100% secure. Therefore, we cannot guarantee its absolute security.

If users have any questions about the security at our Website(s), users can send an email to: Customer.Support@confirmation.com (www.confirmation.com, bba.confirmation.com, www.creditconfirm.com) or EDCustomer.Support@confirmation.com (edu.confirmation.com).

Supplementation of Information

In order for the website(s) to properly fulfill its obligation to users it is necessary for us to supplement the information we receive with information from 3rd party sources. We use outside sources to verify a user's accounting credentials to validate that user’s access to our system. If you provide us personal information about others, or if others give us your information, we will only use that information for the specific reason for which it was provided to us.

Personal Data Management and Inquiries

You have the following rights in relation to personal data relating to you that we process:

1. Upon request Capital Confirmation will provide you with information about whether we hold any of your personal information. You may also request a copy or access to the personal data concerned.
2. If your personal data changes (such as zip code, phone, email or postal address) you can update your data by editing your user profile on the Confirmation.com Website(s) or by contacting Customer Support.
3. Where we are processing personal data relating to you on the basis of your prior consent to that processing, you may withdraw your consent at any time, after which we shall stop the processing concerned.

4. If you have a complaint about the processing of your personal data by Capital Confirmation, please contact Customer Support. If we are unable to rectify the issue to your satisfaction, you are always able to lodge a formal complaint with the applicable Supervisory Authority.

Personal data inquiries can be submitted by contacting the Capital Confirmation Data Protection Officer at Customer.Support@confirmation.com (www.confirmation.com, bba.confirmation.com, www.creditconfirm.com) or EDCustomer.Support@confirmation.com (edu.confirmation.com). We will respond to your request within 30 days.

Social Media Widgets

Our website(s) includes social media features, such as the Facebook "Like" button, and Widgets, such as the "Share This" button or interactive mini-programs that run on our website(s). These features may collect your Internet Protocol (IP) address, which page you are visiting on our website(s) and may set a cookie to enable the feature to function properly. social media features and widgets are either hosted by a third party or hosted directly on our website(s). Your interactions with these features are governed by the privacy statement of the company providing it.

Testimonials

We display personal testimonials of satisfied customers on our site in addition to other endorsements. With your consent we may post your testimonial along with your name. If you wish to update or delete your testimonial, you can contact us at Customer.Support@confirmation.com (www.confirmation.com, bba.confirmation.com, www.creditconfirm.com) or EDCustomer.Support@confirmation.com (edu.confirmation.com).

Links to 3rd Party Sites

Our website includes links to other website(s) whose privacy practices may differ from those of Capital Confirmation. If you submit personal data to any of those sites, your information is governed by their privacy policies. We encourage you to carefully read the privacy statement of any website(s) you visit.

Notification of Changes

If we decide to change our privacy statement, we will post those changes to this privacy statement, the homepage, and other places we deem appropriate so our users are always aware of what information we collect, how we use it, and under what circumstances, if any, we disclose it. We will use information in accordance with the privacy statement under which the information was collected.

If, however, we are going to use a user's personal data in a manner different from that stated at the time of collection we will notify users via email prior to the change becoming effective. Users will have a choice as to whether or not we use their information in this different manner. However, if users have opted out of all communication with the site through deactivating their account, then they will not be contacted, nor will their personal data be used in this new manner. In addition, if we make any material changes in our privacy practices that do not affect user information already stored in our database, we will post a prominent notice on our website(s) prior to the changes taking effect. In some cases where we post a notice we will also email users, who have opted to receive communications from us, notifying them of the changes in our privacy practices.

Regional Privacy Requirements

EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield

The data that we process in relation to you may be transferred to, and stored at, a destination outside the European Economic Area ("EEA") and Switzerland, that may not be subject to equivalent data protection law. It may also be processed by staff situated outside these areas who work for us or for one of our suppliers. This includes staff engaged in activities such as the fulfilment of orders, the processing of payment details, and the provision of support services.

Where personal data is transferred in relation to providing our services, we will take all steps reasonably necessary to ensure that it is protected by appropriate safeguards. Capital Confirmation and its subsidiary companies (Capital Confirmation International LLC, Confirmation Technology Services LLC, Confirmation.com UK

Pvt. Ltd., Confirmation.com India Pvt. Ltd., Confirmation.com Japan Kabushiki Kaisha) participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss-U.S Privacy Shield Framework. Capital Confirmation is committed to subjecting all personal data received from European Union (EU) member countries and Switzerland, respectively, in reliance on the Privacy Shield Framework, to the Framework's applicable Principles. To learn more about the Privacy Shield Frameworks, and to view our certification, visit the U.S. Department of Commerce's Privacy Shield List. [https://www.privacyshield.gov/list]

Capital Confirmation is responsible for the processing of personal data it receives, under the Privacy Shield Framework, and subsequently transfers to a third party acting as an agent on its behalf. Capital Confirmation complies with the Privacy Shield Principles for all onward transfers of personal data from the EU and Switzerland, including the onward transfer liability provisions.

With respect to personal data received or transferred pursuant to the Privacy Shield Frameworks, Capital Confirmation is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, Capital Confirmation may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request.

Under certain conditions, more fully described on the Privacy Shield Website(s) [https://www.privacyshield.gov/article?id=How-toSubmit-a-Complaint] , you may invoke binding arbitration when other dispute resolution procedures have been exhausted.

EU General Data Protection Regulation (GDPR)

In providing our services, we act as a data processor on behalf of the users of our services in relation to personal data that is processed using the service, in which case we will process the relevant personal data only for the purpose(s) of providing the service and otherwise in accordance with our agreement with the users and the regulations that apply to us directly as a data processor.

Legal Basis for Personal Data Processing

Collecting, processing, and using personal data by Capital Confirmation occurs under the following legal bases:

- Legitimate Interest – User validation, transactional confirmation activities including authorization, user access permissions, user account management, core site communications, and customer support.
- Consent – Marketing communications.

[Intentionally Blank]

Data Protection Officer

Compliance with Capital Confirmation's privacy policy, and applicable data protection laws, is verified regularly with internal impact assessments and other controls. The coordination of these activities is the responsibility of the Data Protection Officer, who can be contacted in accordance with the contact information below.

Dan Zangwill
Data Protection Officer
DataInquiries@confirmation.com

Automated Decisions

Personal data processed by Capital Confirmation is never used to make automated decisions that would have negative consequences for its data subjects.

Supervisory Authority

The United Kingdom's Information Commissioner's Office is the lead supervisory authority for Capital Confirmation, Inc. in the EU and can provide further information about your rights and our obligations in relation to personal data, as well as to address any complaints that you have about our processing of your personal data.

Contact Information

If users have any questions or suggestions regarding our privacy statement, please contact us at:

Phone: (615) 844-6222 Fax: (615) 376-7971

Email: Customer.Support@confirmation.com (www.confirmation.com, bba.confirmation.com, www.creditconfirm.com) or EDCustomer.Support@confirmation.com (edu.confirmation.com)

Postal Address: 214 Centerview Drive, Suite 265 Brentwood, Tennessee – 37027