CONFIRMATION
Part of Thomson Reuters

CAPITAL CONFIRMATION, INC.

INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT

FOR THE CONFIRMATION.COM™ SYSTEM

FOR THE PERIOD OF DECEMBER 1, 2019, TO NOVEMBER 30, 2020

Attestation and Compliance Services

schellman
Quality, above all.

INDEPENDENT SERVICE AUDITOR'S REPORT

To Capital Confirmation, Inc.:

Scope

We have examined Capital Confirmation, Inc.'s ("Confirmation") accompanying assertion titled "Assertion of Capital Confirmation, Inc. Service Organization Management" ("assertion") that the controls within Confirmation's Confirmation.com™ system ("system") were effective throughout the period December 1, 2019, to November 30, 2020, to provide reasonable assurance that Confirmation's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Confirmation uses various subservice organizations for data center hosting and infrastructure monitoring and managed security services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Confirmation, to achieve Confirmation's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Confirmation is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Confirmation's service commitments and system requirements were achieved. Confirmation has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Confirmation is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and systems requirements were achieved based on the applicable trust services criteria. 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 our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.
Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that controls were not effective to achieve Confirmation's service commitments and system requirements based on the applicable trust services criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Confirmation's service commitments and system requirements based on the applicable trust services criteria.

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

Inherent Limitations

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

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

Opinion

In our opinion, management's assertion that the controls within Confirmation's Confirmation.com™ system were effective throughout the period December 1, 2019, through November 30, 2020, to provide reasonable assurance that Confirmation's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Emphasis of Matters

Confirmation's description of its Confirmation.com™ system states that incident response procedures are performed to detect and react to information security and privacy incidents; determine their scope and risk; respond appropriately to the incident; document and monitor incident response and resolution activities; communicate the results and risk to stakeholders; and reduce the likelihood of the incident from reoccurring. The system description also states that privacy inquiry, dispute, and complaint response and resolution activities are documented, tracked, and handled in accordance with the Confirmation's privacy policies. The system description also states that customer data is removed from databases and disposed of within 30 days upon receipt of written request; and privacy inquiry, dispute, and complaint response and resolution activities are documented, tracked, and handled in accordance with Confirmation's privacy policies. However, during the period, December 1, 2019, to November 30, 2020, there were no incidents related to security and privacy reported or identified; no requests for the removal and disposal of customer data; and no privacy inquiries, disputes, or complaints that would warrant the operation of the aforementioned controls. Because those controls did not operate during the period, the tests of operating effectiveness could not be performed for those controls using the following associated trust services criteria:

- CC7.3 which states, "The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures."
- CC7.4 which states, "The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate."
- CC7.5 which states, "The entity identifies, develops, and implements activities to recover from identified security incidents."
- C1.2 which states, "The entity disposes of confidential information to meet the entity's objectives related to confidentiality."
- P4.3 which states, "The entity securely disposes of personal information to meet the entity's objectives related to privacy."
- P6.6 which states, "The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy."
- P6.7 which states, "The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy."

Our opinion is not modified with respect to these matters.

Schellman & Company, LLC

Tampa, Florida
January 22, 2021

ASSERTION OF CONFIRMATION'S MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Capital Confirmation, Inc.'s ("Confirmation") Confirmation.com™ system ("system") throughout the period December 1, 2019, to November 30, 2020, to provide reasonable assurance that Confirmation's service commitments and system requirements relevant to security, availability, processing integrity, confidentiality, and privacy were achieved. Our description of the boundaries of the system is presented below and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period December 1, 2019, to November 30, 2020, to provide reasonable assurance that Confirmation's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. Confirmation's objectives for the system in applying the applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period December 1, 2019, to November 30, 2020, to provide reasonable assurance that Confirmation's service commitments and systems requirements were achieved based on the applicable trust services criteria.

Our description of our Confirmation.com™ system states that incident response procedures are performed to detect and react to information security and privacy incidents; determine their scope and risk; respond appropriately to the incident; document and monitor incident response and resolution activities; communicate the results and risk to stakeholders; and reduce the likelihood of the incident from reoccurring. The system description also states that customer data is removed from databases and disposed of within 30 days upon receipt of written request; and privacy inquiry, dispute, and complaint response and resolution activities are documented, tracked, and handled in accordance with Confirmation's privacy policies. However, during the period, December 1, 2019, to November 30, 2020, there were no incidents related to security and privacy reported or identified; no requests for the removal and disposal of customer data; and no privacy inquiries, disputes, or complaints that would warrant the operation of the aforementioned controls. Because those controls did not operate during the period, the tests of operating effectiveness could not be performed for those controls using the following associated trust services criteria:

- CC7.3 which states, "The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures."
- CC7.4 which states, "The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate."
- CC7.5 which states, "The entity identifies, develops, and implements activities to recover from identified security incidents."
- C1.2 which states, "The entity disposes of confidential information to meet the entity's objectives related to confidentiality."
- P4.3 which states, "The entity securely disposes of personal information to meet the entity's objectives related to privacy."

- P6.6 which states, “The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity’s objectives related to privacy.”
- P6.7 which states, “The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects’ personal information, upon the data subjects’ request, to meet the entity’s objectives related to privacy.”

DESCRIPTION OF THE BOUNDARIES OF THE CONFIRMATION.COM™ SYSTEM

Company Background

Confirmation, part of Thomson Reuters, is a provider of computerized audit confirmation services. Confirmation provides patented Software as a Service (SaaS) solution to over 1.5 million users for audit confirmations. Confirmation'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. Confirmation is a privately held company, headquartered in Brentwood, Tennessee. Confirmation's information technology (IT) division, based in Delray Beach, Florida, is responsible for the managing the IT systems that support Confirmation.com™.

In July 2019, Confirmation and its subsidiaries were acquired by Thomson Reuters Corporation (Thomson Reuters). As a wholly owned subsidiary of Thomson Reuters, the company continues to operate as a separate legal entity, Capital Confirmation, Inc.

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, Confirmation provides independent, third-party validated confirmation requests and responses.

Features include automatic document management, a secure 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™ helps ensure that both requestors and responders of confirmations are authorized and authenticated, providing control to both parties while they utilize the service to help improve and streamline 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. This solution provides authorization and authentication procedures that are designed to not only help requestors and responders detect fraud, but also serve as a deterrent or preventative measure against those hoping to circumvent the audit confirmation process.

Confirmation.com™ provides the following core capabilities:

- Multiple layers of authentication and security 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

[Intentionally Blank]

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

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives 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.

Principal Service Commitments and System Requirements

Confirmation designs its processes and procedures related to the Confirmation.com™ system to meet its objectives for providing its audit confirmation services. Those objectives are based on the service commitments that Confirmation makes to user entities, the laws and regulations that govern the provision of its Confirmation.com™ platform and audit confirmation services, and the financial, operational, and compliance requirements that Confirmation has established for the services. Confirmation's services are subject to the European Union (EU) General Data Protection Regulation (GDPR) applicable frameworks; Health Insurance Portability and Accountability Act (HIPAA) administrative simplification as amended, including relevant regulations, as well as the data privacy and security regulations in the jurisdictions in which Confirmation operates.

Security, confidentiality, availability, processing integrity, and privacy commitments to user entities are documented and communicated in Service Level Agreements (SLAs), contracts, and other customer agreements, as well as in the Privacy notice documentation related to the Confirmation.com™ service offering provided the company website. The principal security, confidentiality, availability, processing integrity, and privacy commitments are standardized and include, but are not limited to, the following:

- Personal data will be used only for the stated purposes and deleted after its primary use has expired.
- Data inquiries regarding the correction, deletion, or disclosure of user data will be handled in accordance with applicable regulations to include EU GDPR, EU and Swiss - U.S. Privacy Shield, HIPAA, and contracted service levels for data integrity and availability.
- The Confirmation.com™ platform will maintain compliance with applicable data privacy laws and regulations, including EU GDPR, EU and Swiss-U.S Privacy Shield Framework Principles for onward transfers of personal data from the EU and Switzerland and the onward transfer liability provisions; and applicable frameworks, and HIPAA.
- Confirmation users will be provided with a privacy notice outlining the following commitments for the handling and use of personal information, and users will be notified of any changes made to the privacy notice:
    - All customer financial information or legal confirmation attachments containing PHI residing within Confirmation's secure processing controls will be maintained and stored according to Confirmation's stated security and privacy policies.
    - All such collected information is used only for the conduct of the provision of Confirmation's service.

- Confirmation, and its production site, Confirmation.com™, use log files to track errors in the system.
- Confirmation will share personally identifiable information or legal confirmation attachments containing PHI with third parties only in the ways that are described in the privacy policy. Confirmation will not share aggregated demographic information with our partners and advertisers. Users' personally identifiable information is not shared with third parties unless we give prior notice and choice.
- The entire Confirmation website is encrypted and is protected using 256-bit encryption with a public RSA 2048-bit key for SSL Extended Validation Certificates.
- All of Confirmation's users' information, not just the sensitive information mentioned above, is restricted in Confirmation's offices. Only employees who need the information to perform a specific job are granted access to personal data.
- Every quarter as well as any time new policies are added, employees are notified and/or reminded about the importance placed on privacy, and what they can do to ensure user information is protected.

Confirmation establishes operational requirements that support the achievement of the principal service commitments, relevant laws and regulations, and other system requirements including the clear communication of the purposes for which data will be processed; the establishment of channels for the communication of user data inquiries to the appropriate resources at Confirmation; the implementation of multifactor authentication techniques to validate user identities before access is a granted to confidential data; periodic and continuous testing of the Confirmation.com™ platform to include automated and manual penetration tests, vulnerability scans, and code reviews; the implementation of a defense-in-depth security architecture to include multiple layers of firewalls with intrusion detection and prevention system (IDPS) capabilities; the encryption of data classified as confidential using industry standard encryption at-rest and in-transit methods; industry standard system downtime notification procedures and predefined intervals; the maintaining of a business resumption plan (BRP) which is tested quarterly from both a systems and staff perspective; continued compliance with all applicable data privacy laws and regulations; and the establishment of a change management process that ensures that confirmation transactions are processed in a complete, valid, accurate, timely, and authorized manner in accordance with approved and auditable procedures.

Such requirements are communicated in Confirmation's system policies and procedures, SLAs, contracts, contracts, and other customer agreements, as well as information describing the service offering provided on the company website. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired, trained, and managed. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Confirmation.com™ application.

In accordance with our assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

Infrastructure and Software

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

Confirmation utilizes a third-party data center hosting service provider, Equinix, for colocation and infrastructure monitoring services. The underlying production infrastructure for the Confirmation.com™ system is primarily at an Equinix data center located in Miami, Florida, with secondary production sites located in located in Equinix data centers in Culpeper, Virginia, and Dublin, Ireland. Confirmation 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. Confirmation is also responsible for the secure handling, storage, backup up, transmission, and destruction of application data and related media.

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

Primary Infrastructure			
Production Application	**Business Function Description**	**Operating System Platform**	**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.	Windows Server 2012 R2	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.	Windows Server 2012 R2	Equinix (Miami, FL)
Confirmation.com™ Databases	SQL Server databases containing information about Confirmation.com™ application users, transactional data, and logging activity, as well as distribution documents related to completed confirmations.	Windows Server 2016 / Windows SQL Server 2016 Enterprise	Equinix (Miami, FL / Culpeper, VA / Dublin, IE)
Iron Mountain Live Vault / SQL Management Studio	Automated backup system software and network of servers that provide backup and recovery for subscribing customers.	Windows Server 2012 R2 / Windows SQL Server 2016 Enterprise	Equinix (Miami, FL / Culpeper, VA)
Check Point firewalls / Imperva SecureSphere web application firewall (WAF)	Corporate Check Point firewall systems utilized to filter in-bound and out-bound network traffic with built-in intrusion prevention system (IPS) functionality / Imperva SecureSphere WAF protects the Confirmation.com™ web for cyberattacks.	Check Point IPSO / SecureSphere (proprietary)	Equinix (Miami, FL / Culpeper, VA)
Check Point SecuRemote VPN	Virtual private network (VPN) client software providing multi-factor authentication for remote client-to-site access via Check Point firewall systems	Check Point IPSO / Windows	Equinix (Miami, FL / Culpeper, VA)

Primary Infrastructure			
Production Application	**Business Function Description**	**Operating System Platform**	**Physical Location**
HP SiteScope / Site 24X7 Monitoring Applications	Enterprise monitoring applications that provides real time monitoring and alerts related to availability, capacity, performance of infrastructure hardware and IPS services. SiteScope monitors memory usage, CPU usage, concurrent database connections, disk space, page hits, queued requests, etc. Additionally, automated tools monitor logs for health or the external interfaces. SiteScope, automated log monitors, and firewall alarms page support staff with both warnings and severe events. Site 24x7 is used to monitor the Confirmation.com™ website via multiple node, alert IT operations for failures, and generate daily website reports.	Check Point IPSO / Windows Server 2012 R2	Equinix (Miami, FL / Culpeper, VA)
Event Log Analyzer / ManageEngine	Security information and event management (SIEM) solutions and centralized log servers utilized for the security event auditing and monitoring including inactive user account for disable.	Windows Server 2016	Equinix (Miami, FL)
ChangeNet	Automated ticketing software that provides centralized storage.	Windows Server 2012 R2	Equinix (Miami, FL)
Microsoft Team Foundation Server (TFS) / Planview LeanKit	Workflow utilized for version control, change management and infrastructure issue tracking and resolution / Kanban board software utilized for the software development project management workflows.	Windows Server 2012 R2	Confirmation (Delray Beach, FL)
Symantec EndPoint Protection	Automated antivirus protection software that provides updates of virus definitions and scanning for known viruses or infections on protected devices.	Windows Server 2012 R2	Equinix (Miami, FL) Confirmation (Delray Beach, FL)
Malwarebytes	Automated malware detection and removal of viruses, worms, trojans, rootkits, dialers and spyware software that provides access to malware database and heuristics updates and real-time active malware prevention; blocks known threats; and prevents new Zero Day malware infections.	Windows Server 2012 R2	Equinix (Miami, FL) Confirmation (Delray Beach, FL)

Primary Infrastructure			
Production Application	**Business Function Description**	**Operating System Platform**	**Physical Location**
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.	Windows Server 2012 R2	Equinix (Miami, FL) Confirmation (Delray Beach, FL)
Radware DDoS Protection Service	Cloud-based distributed denial of service (DDoS) attack prevention solution integrating DDoS and cyber-attack prevention solution including detection, mitigation, scrubbing, and support services.	Cloud SaaS	Third-party hosted (Radware SaaS)

People

Confirmation serves customers around the world with its U.S.-based employees supporting the business overall. Confirmation's IT teams and management personnel collaborate to support the Confirmation.com™ services system architecture and business processes, and are responsible for upholding the company's standard for quality assurance (QA) data security standards. 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

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

Access, Authentication and Authorization

Confirmation 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. Confirmation 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. Internal user access reviews, including privileged users, for the Confirmation.com™ application are performed by the executive committee on an annual basis to ensure that access to data is restricted and authorized.

Production 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.

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 180 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 workflow case ticket to document re-inspections for all active requestor entities and associated users with a registration or reinspection year equal to current date less five (5) years on an annual basis. Re-inspections are performed for each active requestor and responder entity and its associated users at least once every five years. These re-inspections are reviewed by a Confirmation director, Confirmation.com™ systems administrator, or officer.

Access Requests and Access Revocation

Confirmation's Operations and Security Policies and Procedures manual contains 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 Confirmation's IT operations personnel. IT operations personnel complete the ticket request by granting access to the Confirmation network and application systems for new hires and disabling user access to the network and application systems for terminated employees.

Authenticating proper source establishes the fundamental guidelines and practices for properly authenticating and authorizing users of Confirmation'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. Confirmation utilizes validation checklists, which are reviewed by a Confirmation director, officer, or Confirmation.com™ systems administrator to help ensure the required activities for requestor and user validation such as physical address and contact information are completed. In addition to validation, customer support agents complete a workflow case ticket to document re-inspections for all active requestor entities and associated users with a registration or reinspection year equal to current date less five years on an 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 Confirmation director, officer, or Confirmation.com™ systems administrator.

To enroll in 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.

Network and Web Application Security

Confirmation maintains a formally documented network diagram outlining the Confirmation production network. A demilitarized zone (DMZ) subnetwork separates the internal network from external Internet traffic; untrusted inbound Internet traffic terminates in the DMZ. A high-availability firewall system is in place to provide perimeter security for the internal network. The firewall is configured with parameters to mask internal IP addresses via network address translation (NAT) and to deny any type of network connection not explicitly authorized by a firewall rule. The ability to administer the firewall system is restricted to user account assigned to authorized IT personnel. Firewall logs are reviewed by operations personnel on a daily basis as a component of the daily IT operations checklists. Additionally, an IPS is utilized to monitor network segments with Internet connectivity.

Encrypted 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 Advanced Encryption Standard (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. A web application firewall is also 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.

Physical and Environmental Security

Physical access to IT computing resources is restricted by office suite doors secured by a badge access control system 24 hours per day at the Delray Beach, Florida, office facility and the Brentwood, Tennessee, corporate headquarters office facility. Badge access is controlled and limited to the current Confirmation employees in each respective location. 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's log maintained by Confirmation personnel. Visitors are not allowed badge access and are required to have an employee chaperone their access to the facility at all times. Upon termination of an employee, the physical access badge cards assigned to the employee are collected and deactivated by the employee's manager and human resources. Operations personnel are also notified to revoked physical badge access to the office facilities 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. Confirmation has contracted with Equinix to provide data center hosting and infrastructure monitoring services. Confirmation utilizes Equinix's Miami, Florida, location as their primary data center facility with a secondary production site located in Culpeper, Virginia. The Equinix data center was not included in the scope of this audit.

The Confirmation 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. Fire suppression equipment third-party inspections occur on an annual basis and are employed by the multi-tenant office building facility's operations team.

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.

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

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.

Confirmation safeguards source code within a version control application (Microsoft TFS) 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.

Data Backup and Disaster Recovery

Confirmation maintains formalized computer operations policies and procedures to guide personnel in the processes for data backup, data recovery, service level performance, incident management, and systems monitoring and maintenance. 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 systems 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 personnel. Backup recovery testing is also performed 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. Confirmation transaction data is 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 AES-256 encryption.

Confirmation has developed a 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 Confirmation 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. Confirmation 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 Confirmation, 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, recovery time objectives (RTOs), recovery point objectives (RPOs), and provides guidelines for ensuring that personnel and resources are available for disaster preparation and response.

Incident Response

Confirmation defines security and privacy incidents as a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. Additionally, Confirmation defines security events as an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant. Confirmation has established a formal information incident response procedure, which is documented and included in the IT operations and security policies and procedures manual. The documented procedure describes the overall plan for responding to information security and privacy incidents at Confirmation, including definition for roles and responsibilities of participants, characterization of incidents, relationships to other policies and procedures, and reporting requirements. The purpose of the incident response procedure is to detect and react to information security and privacy incidents, determine their scope and risk, respond appropriately to the incident, communicate the results and risk to stakeholders, and reduce the likelihood of the incident from reoccurring.

Confirmation personnel are instructed to report information security incidents immediately to the CIO, IT security team, or IT operations team. The chief security officer is responsible for assembling the data pertinent to an incident, communicating with appropriate parties, ensuring that the information is complete, and reporting on incident status both during and after the investigation. IT support staff has additional responsibilities for information security incident handling and reporting for the systems they manage. In the case of an information security incident, IT support will review to determine how the incident should be handled and take immediate action to stop the incident from continuing or recurring. Incidents involving the loss of confidential information are escalated to CIO, CSO, and VP of IT operations to investigate the incident in consultation with the IT support specialist and to develop response plan to address the incident. Confirmation's incident response process follows the National Institute of Standards and Technology Special Publication (NIST SP) 800-61 guidelines for incident response and encompasses a six-phase approach: preparation, detection, containment, investigation, remediation, and recovery.

Incident response activities are documented by the chief security officer and includes the artifacts obtained using methods consistent with chain of custody and confidentiality requirements. At minimum, information security incident records must contain the following:

- The date and time the incident occurred;
- The date and time it was discovered;
- Who/what reported the incident;
- Description of the incident;
- Details of any Confirmation systems involved in the incident; and
- Any other substantiating material.

The information security incidents are reviewed post-mortem by the information security team, chaired by the chief security officer, on a quarterly basis to assess whether the investigational process was successful and effective. Subsequent adjustments are made to methods and procedural documentation as a result of lessons learned or for purposes of process improvement. Deletion of artifacts obtained during the course of an investigation after its conclusion and post-mortem analysis required the approval by the CSO.

Continuous improvement of the information security incident response process implies that those processes are periodically reviewed, tested, and translated into recommendations for enhancements. All Confirmation employees receive training on properly identifying and reporting information security incidents. Members of the IT security team and support staff participate in an annual tabletop exercise for responding to incidents to ensure that there is a consistent and appropriate response to incidents and that post-incident finding are incorporated into procedural enhancements.

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.

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.

Information Security and Privacy

Confirmation's information sensitivity policy defines "personal data" as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The policy designates customer information that is considered private (e.g., credit card numbers, account numbers, user's personal information), that which relates to the privacy policies of the business, and trade secrets as "most sensitive" under the Confidential information classification.

The policy also provides guidelines for labeling, safeguarding (controls for access and distribution), storing, disposal / destruction, and penalties for deliberate or inadvertent disclosure of data classified as Confidential based on three sensitivity levels (minimally sensitive, more sensitive, and most sensitive).

The official responsible for directing, defining, and implementing the company's information security and privacy program, and overall strategy is the CSO. The CSO is also designated as the Data Protection Officer (DPO) for monitoring and enforcing data protection regulations applicable to Confirmation. The CSO / DPO performs the following:

- Considers developments in technology and the impact of applicable laws or regulations on the entity's related security policies.
- Monitors compliance with applicable regulations and standards, and review violations.
- Determines the scope that defines security and privacy incidents where the incident response plan procedures would be invoked.
- Evaluates reported events related to data security and privacy, investigate the event to determine the necessary course of action for responding to the event, including activation of the incident response plan, and coordinate response and resolution activities in accordance with documented incident response plan procedures.
- Coordinates the development and maintenance of information security and privacy policies and standards.
- Ensures implementation of security and privacy policies, and documentation of supporting process and procedures.
- Assists business owners in assessing their data for classification and advise them of available controls.
- Defines processes for assigning user access codes (using access profiles prepared for that use), revoking user access privileges, and setting file protection parameters.
- Maintains ongoing internal audit processes which record security and privacy incidents, control deficiencies, opportunities for improvement, and corrective action plans.
- Acts as the contact point for and fulfill any requests issued by data subjects or supervisory authorities.
- Conducts data protection impact assessments for the applicable organizational data processing.

- Establishes and maintains a risk-based internal audit plan to determine the priorities of internal audit resources and ensure they are consistent with the Confirmation's goals.
- Monitors progress in implementing agreed action plans and corrective action plans, by maintaining a register of audit findings and progress, and undertaking follow up audits based on the risks posed to the organization and report on progress to the Executive Committee.

The executive committee is responsible for governance and oversight of the Confirmation IT Operations and Security Policies and Procedures. The executive committee is chaired by the chief information officer, with standing members being the chief financial officer, chief security officer, and vice president of business integration. The executive committee meets at least annually and produces minutes of the outputs as permanent record. Specific functions of the executive committee include the following:

- Review and as needed, modify, current processes and to ensure the information security and privacy policies and procedures are in alignment, including changes made to the document since the last annual executive committee meeting; and modify policies and procedures.
- Review the risk assessment results including new risks and changes to existing risk ratings, and direct appropriate actions to mitigate the risk.
- Validate and approve Confirmation.com™ internal users and privilege assignments are restricted to authorized personnel, based on a need to know.
- Review critical contracts for consistency with Confirmation policies and ensure that data security and privacy controls, service definitions, and delivery levels included in third-party service delivery agreements are implemented, operated, and maintained to meet Confirmation's requirements.
- Monitor compliance to the security and privacy policies and procedures, industry security and privacy standards, and any new or existing legal and regulatory requirements.
- Review hardware inventory where access to USB support for removable media has been enabled.
- Ensure consistency in disciplinary processes for violation.
- Review business resumption plan.
- Monitor compliance to training requirements and review appropriateness of current policies. Any non-conformities will be noted, and a remediation plan must be submitted and completed within 60 days.

Data

Data provided by Confirmation 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, as well as distribution documents related to completed confirmations. 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 (PII). Legal confirmation requests could contain protected health information (PHI), and may be stored on Confirmation's systems as a document attachment. Confirmation 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	Confirmation	Confidential
Transactional and customer data and application activity logs, as well as distribution documents related to completed confirmations		
Customer data that could include PII		

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Legal confirmation requests that could contain PHI and may be stored on Confirmation's systems as document attachments		

Data utilized by Confirmation 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.

Subservice Organizations

Confirmation utilizes the data center hosting and infrastructure monitoring services provided by Equinix, Inc (Equinix). Confirmation also utilizes managed security services provided by Radware Ltd. (Radware) for Distributed Denial of Service (DDoS) and cyber-security threat detection monitoring, mitigation, and reporting. The data center hosting and infrastructure monitoring services provided by Equinix and the managed security services provided by Radware were not included within the scope of this examination.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at Equinix and Radware, alone or in combination with controls at Confirmation, and the types of controls expected to be implemented at Equinix and Radware to achieve Confirmation's service commitments and system requirements based on the applicable trust services criteria.

Control Activity Expected to be Implemented by Equinix and Radware	Applicable Trust Services Criteria
Equinix is responsible for implementing control activities to help ensure 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.	CC6.4, CC6.7
Radware is responsible for implementing control activities for aspects of threat detection and monitoring on Confirmation's network, including DDoS and cyber-security attack threat management and mitigation, and for alerting IT security personnel of potential security vulnerabilities.	CC6.6, CC7.2
Equinix is responsible for implementing control activities for the design, development, implementation, operations, maintenance, and monitoring of environmental security safeguards to meet availability commitments and requirements. Additionally, Equinix is responsible for implementing control activities that ensure 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

Confirmation has not delegated any responsibility of the personal information life cycle to Equinix or Radware.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security, availability, processing integrity, confidentiality, and privacy categories are applicable to the Confirmation.com™ system.

Privacy Notice

Confirmation provides the privacy notice to individuals about whom personal information is collected, used, retained, disclosed, and disposed of or anonymized. Confirmation 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/eu-en/legal-security-privacy/index.html.

Confirmation PRIVACY STATEMENT

Effective on: August 30, 2019

This privacy policy applies to www.confirmation.com, and learn.confirmation.com ("Confirmation Website(s)") owned and operated by Confirmation. This privacy policy describes how Confirmation collects, shares, secures 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 PHI Confirmation collects.
2. What personal data third parties collect through the website(s).
3. What organization collects the information.
4. How Confirmation uses the information.
5. With whom 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 the information under 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 e-mail 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, e-mail, 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 e-mail address. This information is used to validate the client users of the service. A welcome e-mail 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 e-mails are only used for the primary purpose of providing the service of the site and are not used for any secondary purposes.

Information Use

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

1. General Personal Data
2. Customer Financial Information
3. 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 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 Confirmation's secure processing controls will be maintained and stored according to our stated security and privacy policies. Confirmation takes no responsibility for Customer Financial Information once this data is no longer within Confirmation's control (e.g., data downloaded by the user, or mailed confirmations). The Confirmation website(s) serve the function of an online 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 the Internet Protocol (IP) address, browser type, Internet Service Provider (ISP) and access times. We do not store the 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, 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 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 IP addresses, browser type, and ISP, referring/exit pages, operating system and access time. Confirmation and its production 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 Client

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 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. 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 e-mail, 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 e-mails, 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 e-mail or phone in accordance with the user's wishes.

Marketing Communications

We may from time to time send e-mails or mail to provide you with information regarding new product and service offerings, product and service notifications, and/or complementary 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 receive them (if your location requires consent), use the "Manage Your Preferences" and "Unsubscribe" links provided within each marketing e-mail 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, 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 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 secure socket layer (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 e-mail to Customer.Support@confirmation.com (www.confirmation.com) or learn@confirmation.com (learn.confirmation.com/learn).

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:

Upon request, 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.

If your personal data changes (such as zip code, phone, e-mail or postal address) you can update your data by editing your user profile on the Confirmation.com Website(s) or by contacting Customer Support.

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.

If you have a complaint about the processing of your personal data by 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 Confirmation Data Protection Officer at Customer.Support@confirmation.com (www.confirmation.com) or (learn.confirmation.com/learn). 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 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) or learn@confirmation.com (https://learn.confirmation.com/learn).

Links to 3rd Party Sites

Our website includes links to other website(s) whose privacy practices may differ from those of 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 e-mail 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 e-mail 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 fulfillment 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. Confirmation and its subsidiary companies (Confirmation International LLC, and Confirmation Technology Services LLC) participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss-U.S Privacy Shield Framework. Confirmation is committed to subjecting all personal data received from the 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).

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. 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, Confirmation is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, 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-to-Submit-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 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.

Data Protection Officer

Compliance with 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 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 Confirmation 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
E-mail: Customer.Support@confirmation.com (www.confirmation.com)
or learn@confirmation.com (https://learn.confirmation.com/learn)
Postal Address: 214 Centerview Drive, Suite #100 Brentwood, Tennessee, 37027