Cross Commerce Media, Inc. d/b/a Collective[i] SOC 3 2020

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

October 1, 2019 to September 30, 2020

Table of Contents

SECTION 1

ASSERTION OF CROSS COMMERCE MEDIA, INC. D/B/A COLLECTIVE[I] MANAGEMENT

ASSERTION OF CROSS COMMERCE MEDIA, INC. D/B/A COLLECTIVE[I] MANAGEMENT

October 5, 2020

We are responsible for designing, implementing, operating, and maintaining effective controls within Cross Commerce Media, Inc. d/b/a Collective[i]'s ('Collective[i]' or 'the Company') Sales Compensation Software as a Service (SaaS) System throughout the period October 1, 2019 to September 30, 2020, to provide reasonable assurance that Collective[i]'s service commitments and system requirements relevant to Security (applicable trust services criteria) were achieved. Our description of the boundaries of the system is presented below in "Cross Commerce Media, Inc. d/b/a Collective[i]'s Description of Its Sales Compensation SaaS System throughout the period October 1, 2019 to September 30, 2020" 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 October 1, 2019 to September 30, 2020, to provide reasonable assurance that Collective[i]'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity and Privacy* (AICPA, *Trust Services Criteria*). Collective[i]'s objectives for the system in applying applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "Cross Commerce Media, Inc. d/b/a Collective[i]'s Description of Its Sales Compensation SaaS System throughout the period October 1, 2019 to September 30, 2020".

Collective[i] uses RagingWire to provide data center hosting services and Voonami to provide cloud hosting services (collectively, the 'subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Collective[i], to achieve Collective[i]'s service commitments and system requirements based on the applicable trust services criteria. The description presents Collective[i]'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Collective[i]'s controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Collective[i]'s service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of Collective[i]'s controls.

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 October 1, 2019 to September 30, 2020 to provide reasonable assurance that Collective[i]'s service commitments and system requirements were achieved based on the applicable trust services criteria.

Jacques Robert Gagnon
Chief Financial Officer
Cross Commerce Media, Inc. d/b/a Collective[i]

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Cross Commerce Media, Inc. d/b/a Collective[i]

Scope

We have examined Collective[i]'s accompanying description of Sales Compensation SaaS System titled "Cross Commerce Media, Inc. d/b/a Collective[i]'s Description of Its Sales Compensation SaaS System throughout the period October 1, 2019 to September 30, 2020" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2019 to September 30, 2020, to provide reasonable assurance that Collective[i]'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Collective[i] uses RagingWire to provide data center hosting services and Voonami to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Collective[i], to achieve Collective[i]'s service commitments and system requirements based on the applicable trust services criteria. The description presents Collective[i]'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Collective[i]'s controls. The description 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.

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

Service Organization's Responsibilities

Collective[i] 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 Collective[i]'s service commitments and system requirements were achieved. Collective[i] has provided the accompanying assertion titled "Assertion of Cross Commerce Media, Inc. d/b/a Collective[i] Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Collective[i] is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

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

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

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

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

Inherent Limitations

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

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

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

Opinion

In our opinion, management's assertion that the controls within Collective[i]'s Sales Compensation SaaS System were suitably designed and operating effectively throughout the period October 1, 2019 to September 30, 2020, to provide reasonable assurance that Collective[i]'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

The SOC logo for Service Organizations on Collective[i]'s website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of Collective[i], user entities of Collective[i]'s Sales Compensation SaaS System during some or all of the period October 1, 2019 to September 30, 2020, business partners of Collective[i] subject to risks arising from interactions with the Sales Compensation SaaS System, and those who have sufficient knowledge and understanding of the complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

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

A-LIGN ASSURANCE

Tampa, Florida
October 5, 2020

SECTION 3

CROSS COMMERCE MEDIA, INC. D/B/A COLLECTIVE[I]'S DESCRIPTON OF ITS SALES COMPENSATION SAAS SYSTEM THROUGHOUT THE PERIOD OCTOBER 1, 2019 TO SEPTEMBER 30, 2020

OVERVIEW OF OPERATIONS

Company Background

Cross Commerce Media, Inc. was incorporated in 2007 and began doing business as Collective[i] in 2011 after creating the largest global network to map enterprise buying behavior using data, artificial intelligence and predictive technologies. Collective[i]'s advanced technology for business-to-business sales management guides sales professionals from a variety of industries through the daily activities that lead directly to revenue. Collective[i] is a Delaware corporation with offices in New York City, New York and San Jose, California.

Description of Services Provided

Collective[i] provides a proprietary database network and applications to help augment internal business-to-business sales activities, management and people based on machine learning that processes aggregated data from various sources, including Collective[i]'s clients. Through applications that easily connect to clients' Customer Resource Management ('CRM') system and other relevant data sources, the technology transforms raw data into usable insight and intelligence. The technology removes the need for rigor, endless meetings, routine/manual analyses (such as forecasting) and research by offering real-time intelligence linking buyer behavior to seller activity. The intelligence presents aggregated data in a form that helps clients identify buyer specific opportunities, connections and potential connections, ongoing sales activities, time frames, forecasts and other information crucial to their sales and marketing efforts.

Principal Service Commitments and System Requirements

Collective[i] designs its processes and procedures related to its application to meet its objectives for its application services. Those objectives are based on the service commitments that Collective[i] makes to user entities, the laws and regulations that govern the provision of application services, and the financial, operational, and compliance requirements that Collective[i] has established for the services. The application services of Collective[i] are subject to the security and privacy requirements of Privacy Shield, as amended, including relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which Collective[i] operates.

Security commitments to user entities are documented and communicated in Service Level Agreements ('SLAs') and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the application that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role
- Use of encryption technologies to protect customer data both at rest and in transit

Collective[i] establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Collective[i]'s system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. 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 application.

Components of the System

Infrastructure

Primary infrastructure used to provide Collective[i]'s Sales Compensation SaaS System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Web Servers	[redacted]	Hosts files to support the client application.
Database Servers	[redacted]	Hosts files that contact application data.
Firewalls	[redacted]	Filters traffic into and out of the private network supporting the application.
Routers	[redacted]	Connects multiple networks and forward packets within the network and other networks.
Switches	[redacted]	Connects devices on the private network by sending packets to the specific devices that need to receive the messages.
Load Balancers	[redacted]	Connects multiple networks and distributes application traffic amongst various web and application servers.
Virtualization	[redacted]	Hosts servers in a virtual architecture that supports various infrastructure components in the client environment.
Virtual Private Network ('VPN') Concentrator	[redacted]	Authorizes and authenticates VPN connections from the public network to the private network.

Software

Primary software used to provide Collective[i]'s Sales Compensation SaaS System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
[redacted]	[redacted]	Provides ticketing functionality to document and track requests and issues related to the client environment.
[redacted]	[redacted]	Provides intranet web server to host and distribute internal system documentation.
[redacted]	[redacted]	Monitoring application used to provide monitoring, alerting and notification services for the client environment.
[redacted]	[redacted]	The operating system that hosts applications in the client environment.
[redacted]	[redacted]	A database application that stores application data in the client environment.

Primary Software		
Software	**Operating System**	**Purpose**
[redacted]	[redacted]	A database application that stores application data in the client environment.
[redacted]	[redacted]	A data processing system that processes and stores application data in the client environment.
[redacted]	[redacted]	A database application that stores data in the client environment.
[redacted]	[redacted]	Web server system that provides interface for application dashboards and other features.
[redacted]	[redacted]	Web server system that provides interface for application data and other features.
[redacted]	[redacted]	Perform scheduled jobs like backups and application tasks of client data according to the requirements defined by the Backup Policy and documented in the Recovery Point Objective/ Recovery Time Objective ('RPO/RTO') Inventory.
[redacted]	[redacted]	Virtualization system that operates various servers and applications that run in the client environment.
[redacted]	[redacted]	Provides code versioning and application for teams to plan projects, collaborate on code, test and deploy.
[redacted]	[redacted]	Continuous integration automation system that provides a system to support building, deploying and automating software projects.
[redacted]	[redacted]	Configuration management system that provides a system to support building, deploying and automating infrastructure projects.

People

The Collective[i] staff provides support for the above services in each of the following functional areas:

- Executive Management - provides general oversight and strategic planning of operations
- Information Security team - responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines
- Development team - responsible for delivering a responsive system that complies with the functional specification
- Quality Assurance team - verifies that the system complies with the functional specification through functional testing procedures
- System administrators - responsible for effective provisioning, installation/configuration, operation, and maintenance of systems hardware and software relevant to the system
- Client Services - serves clients by providing product and service information that includes resolving product and service issues
- Audit and Compliance - performs regularly scheduled audits relative to defined standards, provides continuous improvement feedback, and assesses legal and regulatory requirements

Data

Client data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in client contracts. Client data is captured which is utilized by Collective[i] in delivering its Intelligence system. Such data includes, but is not limited to, the following:

- Alert notifications and monitoring reports generated from the commercial monitoring applications
- Alert notifications received from automated backup systems
- Vulnerability or security alerts received from various sources including security subscriptions, scanning tools, Intrusion Detection System ('IDS') alerts, or automated patching systems
- Incident reports documented via the ticketing systems
- Client CRM source data from commercial CRM systems
- Client Workplace Productivity source data from commercial e-mail, calendar, Voice over Internet Protocol ('VOIP') and other productivity systems

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Collective[i] policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any Collective[i] team member.

Physical Security

Occupied company facilities are protected by appropriate perimeter boundary protection. Where necessary, as in data center facilities, walls and fencing define the boundary area. Access to the reception area can be unlocked from 8am to 5pm on business days and is locked at all other times. When locked, a visitor presses a buzzer to call the visitor guard at the visitor desk who can release the lock. The door may also be unlocked through the use of an access card/ID that has been assigned general access to the facility. Access beyond the reception area is controlled through the access card system.

All remaining exterior ingress doors are restricted to users possessing an access card/ID that has been assigned access to use the door. The access card/ID system is zones to control access. Each exterior door and doors to restricted areas within the facilities is assigned to door zones. Access to zones is restricted through the use of access control lists. Employees and vendors granted access cards are assigned to roles based on their job responsibilities.

Visitors check in with the receptionist or security guard stationed in the reception area. Visitors must present a valid, government-issued photo ID. The visitor's name, employer, and purpose for visit are recorded in a visitor log and his or her visit must be approved by a Collective[i] employee who is authorized to sign non-employees into the facility. The visitor is issued a temporary ID badge to be worn throughout his or her visit. This temporary badge does not permit users access through any secured doors within the facility.

Entrances to data centers are restricted by two doors; access through the first door is gained by using a key card to deactivate the locking mechanism, and access through the second door is granted by using a biometric hand reader and Personal Identification Number ('PIN'). Where possible, retinal verification is used as a secondary form of identification verification.

Upon an employee's termination of employment, the Human Resource ('HR') system automatically generates an access revocation record in the event management system on the last day of employment. This record is routed to the access administrators for access revocation. In addition, terminated employees turn over their access cards/IDs during their exit interview.

On a quarterly basis, zone owners review access to their zones. Access listings are generated by security and distributed to the zone owners via the ticket management system. Zone owners review the listings and indicate the required changes in the ticket management record. The record is routed back to the access administrators for processing. The physical security manager identifies any records not returned within two weeks and follows up with the zone owner.

On a semi-annual basis, the Chief Information Security Officer ('CISO') sends a list of each vendor's employees who have been granted access to the vendor contact to review appropriateness of employee access. Vendors are required to return the confirmation of access within two weeks. The CISO follows up on any access lists not returned.

Logical Access

Collective[i] uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists. In situations in which incompatible responsibilities cannot be segregated, Collective[i] implements monitoring of one or more of the responsibilities. Monitoring must be performed by a superior without responsibility for performing the conflicting activities or by personnel from a separate department.

All resources are managed in the asset inventory system and each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing reviews of access by role.

Employees and approved vendor personnel sign on to the Collective[i] network using a Lightweight Directory Access Protocol ('LDAP') user ID and password. Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality of LDAP or Linux-based Public Key Infrastructure ('PKI'). Passwords must conform to defined password standards and are enforced through parameter settings in the Centralized Authentication and/or Linux-based Operating System. In accordance with the National Institute of Standards and Technology ('NIST') digital identity guidelines, these settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts, and mask workstation screens, requiring reentry of the user ID and password after a period of inactivity.

Employees accessing the system from outside the Collective[i] network are required to use a token-based two-factor authentication system. Employees are issued electronic tokens upon employment and are expired during their exit interview. Vendor personnel are not permitted to access the system from outside the Collective[i] network.

Client employees access Intelligence services through the Internet using the Secure Socket Layer ('SSL') functionality of their web-browser. These client employees must supply a valid user ID and password to gain access to client cloud resources. Passwords must conform to password configuration requirements configured through the application administration portal account.

Upon hire, employees are assigned to a position in the HR management system. Two days prior to the employees' start date, the HR management system creates a JIRA ticket report that identifies the employee user IDs to be created and access to be granted. The report is used by the security help desk to create user IDs and access rules. Access rules have been pre-defined based on the defined roles. The system lists also include employees with position changes and the associated roles to be changed within the access rules.

On an annual basis, access rules for each role are reviewed by a working group composed of security help desk, data center, client services, and HR personnel. In evaluating role access, group members consider job description, duties requiring segregation, and risks associated with access. Completed rules are reviewed and approved by the CISO. As part of this process, the CISO reviews access by privileged roles and requests modifications based on this review.

The HR system generates a list of terminated employees on a regular basis. Upon termination, a JIRA ticket report is created to be used by the security help desk to delete or freeze employee access. On an annual basis, HR runs a list of active employees. The security help desk uses this list to suspend user IDs and delete all access roles from IDs belonging to terminated employees.

On a quarterly basis, an access review is performed whereby managers review roles assigned to their direct reports. Role lists are generated by security and distributed to the managers via the event management system. Managers review the lists and indicate the required changes in the event management record. The record is routed back to the security help desk for processing. The security help desk manager identifies any records not returned within two weeks and follows up with the manager. As part of this process, the CISO reviews employees with access to privileged roles and requests modifications through the event management system.

Computer Operations - Backups

Client data is backed up and monitored by operations personnel for completion and exceptions. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job depending on client indicated preference within the documented work instructions.

Backup infrastructure and on-site backup media are physically secured in locked cabinets and/or caged environments within the third-party data centers. The backup infrastructure resides on private networks logically secured from other networks.

On an annual basis, a backup review is performed to confirm the successful restoration and compliance of backups sufficient to meet the requirements of clients and the business. As part of this process, the CISO reviews backups in accordance with the RTO/RPO inventory and updates the SLA as necessary to comply with Business Continuity Planning (‘BCP’) and Disaster Recovery (‘DR’) standards.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

Collective[i] monitors the capacity utilization of physical and computing infrastructure both internally and for clients to ensure that service delivery matches service level agreements. Collective[i] evaluates the need for additional infrastructure capacity in response to growth of existing clients and/or the addition of new clients. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Data center space, power and cooling
- Disk storage
- Backup media storage
- Network bandwidth
- Server resources
- Application availability and performance

Collective[i] has implemented a patch management process to ensure contracted client and infrastructure systems are patched in accordance with vendor recommended operating system patches. Collective[i] system owners and Information Security review proposed operating system patches to determine whether the patches are applied. Collective[i] systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Collective[i] staff validate that all patches have been installed and if applicable that reboots have been completed.

Change Control

Collective[i] maintains documented Systems Development Life Cycle ('SDLC') policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures. A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance ('QA') testing and User Acceptance Testing ('UAT') results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Collective[i] has implemented a patch management process to ensure contracted client and infrastructure systems are patched in accordance with vendor recommended operating system patches. Collective[i] system owners review proposed operating system patches to determine whether the patches are applied. Collective[i] systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Collective[i] staff validate that all patches have been installed and if applicable that reboots have been completed.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network Address Translation ('NAT') functionality is utilized to manage internal Internet Protocol (IP) addresses. Administrative access to the firewall is restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by Collective[i]. The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed by a third-party vendor on a quarterly basis in accordance with Collective[i] policy. The third-party vendor uses industry standard scanning technologies and a formal methodology specified by Collective[i]. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during non-peak windows. Tools requiring installation in the Collective[i] system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Authorized employees may access the system from the Internet through the use of industry standard VPN technology. Employees are authenticated through the use of a token-based two-factor authentication system.

Boundaries of the System

The scope of this report includes the Sales Compensation SaaS System performed in the New York City, New York and San Jose, California facilities.

This report does not include the data center hosting services provided by RagingWire or the cloud hosting services provided by Voonami at multiple locations.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Collective[i]'s control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Collective[i]'s ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook
- Background checks are performed as needed for employees as a component of the hiring process

Commitment to Competence

Collective[i]'s management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements
- Training is provided to maintain the skill level of personnel in certain positions

Management's Philosophy and Operating Style

Collective[i]'s management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

Specific control activities that the service organization has implemented in this area are described below:

- Management is briefed on regulatory and industry changes affecting the services provided
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole

Organizational Structure and Assignment of Authority and Responsibility

Collective[i]'s organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Collective[i]'s assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Organizational charts are in place to communicate key areas of authority and responsibility. These charts are communicated to employees and updated as needed.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility
- Organizational charts are communicated to employees and updated as needed

Human Resource Policies and Practices

Collective[i]'s success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Collective[i]'s human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment
- Evaluations for each employee are performed on an annual basis
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist

Risk Assessment Process

Collective[i]’s risk assessment process identifies and manages risks that could potentially affect Collective[i]’s ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. Collective[i] identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process continuously seeks to identify risks resulting from the nature of the services provided by Collective[i], and management has implemented various measures designed to manage these risks.

Risks identified in this process include the following:

- Operational risk - changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance - legal and regulatory changes

Collective[i] has established an independent organizational business unit that is responsible for identifying risks to the entity and monitoring the operation of the firm’s internal controls. The approach is intended to align the entity’s strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. Collective[i] attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Collective[i]’s system; as well as the nature of the components of the system result in risks that the criteria will not be met. Collective[i] addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Collective[i]’s management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communications Systems

Communication is an integral component of Collective[i]’s internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity’s operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Collective[i], information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various routine calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, town hall meetings are held in each geographic location to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead the town hall meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to entity-wide security policies and procedures are usually communicated to the appropriate Collective[i] personnel via e-mail messages.

Specific information systems used to support Collective[i]’s Sales Compensation SaaS System are described in the Description of Services section above.

Monitoring Controls

Collective[i]’s risk assessment process identifies and manages risks that could potentially affect Collective[i]’s ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. Collective[i] identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process continuously seeks to identify risks resulting from the nature of the services provided by Collective[i], and management has implemented various measures designed to manage these risks.

Risks identified in this process include the following:

- Operational risk - changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance - legal and regulatory changes

Collective[i] has established an independent organizational business unit that is responsible for identifying risks to the entity and monitoring the operation of the firm’s internal controls. The approach is intended to align the entity’s strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. Collective[i] attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

On-Going Monitoring

Collective[i]’s management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management’s close involvement in Collective[i]’s operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control’s weakness is made based on whether the incident was isolated or requires a change in the company’s procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Collective[i]’s personnel.

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of ongoing monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Incident in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Criteria Not Applicable to the System

All Common criteria was applicable to Collective[i]'s Sales Compensation SaaS System.

Subservice Organizations

This report does not include the data center hosting services provided by RagingWire or the cloud hosting services provided by Voonami at multiple locations.

Subservice Description of Services

RagingWire delivers colocation services through enterprise data center facilities engineered to offer a 100% uptime SLA even during maintenance windows. Based on client space and power needs, RagingWire configures custom colocation dedicated suites, cages or high-density cabinets that will accommodate a wide array of free-standing equipment. Client assets reside within RagingWire's data center.

Voonami provides colocation, cloud computing, hosting, virtualized servers, managed services, dedicated servers, Internet Service Provider ('ISP') services, VOIP solutions, and a full suite of other data center products and services tailored specifically to meet the high demand of corporate computing.

Complementary Subservice Organization Controls

Collective[i]'s services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called subservice organization controls. It is not feasible for all of the trust services criteria related to Collective[i]'s services to be solely achieved by Collective[i] control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Collective[i].

The following subservice organization controls should be implemented by RagingWire and Voonami to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - RagingWire		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.4	Physical access controls are in place to restrict access to and within the corporate and data center facilities.
		Physical access requests are documented on a standard access request form and require approval of a manager.
		Digital Surveillance cameras are in place to monitor the following facility areas: • Building entrances • Datacenter lobbies • Datacenter floors Building exteriors
		Video archives of surveillance cameras are retained for a minimum 90 days.
		Security personnel are positioned at various locations throughout the facility 24 hours per day and performs patrols twice daily. Security events occurring during the shift are recorded on a shift activity report.
		Facilities personnel conduct an audit of access groups and badge holders on at least an annual basis to verify that access is appropriate.

Subservice Organization - RagingWire		
Category	**Criteria**	**Control**
		A termination checklist is completed and physical access is revoked for employees as a component of the employee termination process.
		Visitors to the facility require continuous escort by either authorized facility personnel or authorized client personnel while on facility property.
		Security personnel maintain a client access li to guide security personnel in granting access into the facility.
		Datacenter hosting services clients are required to provide government issued identification and sigh a key log in order to check out the physical key for their respective cage.
		Visitors are required to provide government issued identification and sign a visitor's log prior to gaining access to the facility.
		Visitors are required to surrender their badges upon exit. The badges are disabled when returned.

Subservice Organization - Voonami		
Category	**Criteria**	**Applicable Controls**
Common Criteria/Security	CC6.4	Physical access controls are in place to restrict access to and within the corporate and data center facilities.
		Datacenter facilities require two-factor authentication to gain access. Biometric authentication and key-card/badge control authentication to electromechanical locks restrict access to the datacenters facilities.
		The Chief Technology Officer and Facilities Manager perform a quarterly access review to validate access levels and ensure access is restricted to designated Voonami personnel and customers.
		New Customers and Voonami employees sign the Access Card Agreement before receiving access to the datacenters. Only the President/Chief Technology Officer, Facilities Manager or a member of the Network Operations Center ('NOC') have rights to provision data center access.
		The Facilities Manager or a member of the NOC removes access to the datacenter for terminated employees through the use of an exit checklist, and for inactive customers upon the notification from the customer as tracked in the ticketing system.
		Voonami requires potential customers and other visitors touring the datacenter to sign the visitor log and to provide a photo ID, which is retained during the visit.
		Combination and/or keyed locks secure customer equipment, which is maintained in separate cages or cabinets.

Subservice Organization - Voonami		
Category	**Criteria**	**Applicable Controls**
		Closed-circuit video surveillance records activity at the entrance points on the interior and exterior of the datacenter buildings. The NOC monitors the video feeds.
		A Voonami NOC employee is present 24 hours a day, 7 days a week and 365 days a year.

Collective[i] management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Collective[i] performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing and reconciling output reports
- Holding discussions with vendors and subservice organizations
- Making regular site visits to vendor and subservice organizations’ facilities
- Testing controls performed by vendors and subservice organizations
- Reviewing attestation reports over services provided by vendors and subservice organizations
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organizations

COMPLEMENTARY USER ENTITY CONTROLS

Collective[i]’s services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to Collective[i]’s services to be solely achieved by Collective[i] control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Collective[i]’s.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities’ locations, user entities’ auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Collective[i].
2. User entities are responsible for notifying Collective[i] of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own systems of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Collective[i] services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Collective[i] services.
6. User entities are responsible for providing Collective[i] with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Collective[i] of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.