System and Organization Controls Report (SOC 2® Type 2)

Report on Fragment Foundries Inc.'s Description of Its Ledger API Platform and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security Throughout the Period February 10, 2025, to May 10, 2025

FRAGMENT

Insight Assurance

Delivering Quality, Assuring Trust.

+1 877.607.7727

www.InsightAssurance.com

TABLE OF CONTENTS

SECTION 1:
INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Fragment Foundries Inc.

Scope

We have examined Fragment Foundries Inc.'s ("Fragment" or "the service organization") accompanying description of its Ledger API Platform found in Section 3 titled "Fragment Foundries Inc.'s description of its Ledger API Platform" throughout the period February 10, 2025, to May 10, 2025, ("description") based on the criteria for a description of a service organization's system set forth in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)* in AICPA, *Description Criteria*, (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period February 10, 2025, to May 10, 2025, to provide reasonable assurance that Fragment'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 (With Revised Points of Focus—2022)* in AICPA*, Trust Services Criteria.*

Fragment uses Amazon Web Services (AWS) ("subservice organization") to provide hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Fragment, to achieve Fragment's service commitments and system requirements based on the applicable trust services criteria. The description presents Fragment's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Fragment's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

Fragment is responsible for its service commitments and system requirements and designing, implementing, and operating effective controls within the system to provide reasonable assurance that Fragment's service commitments and system requirements were achieved. In Section 2, Fragment has provided the accompanying assertion titled "Fragment Foundries Inc.'s

Management Assertion" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. Fragment 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.

We are required to be independent and meet our other ethical responsibilities in accordance with ethical requirements relating to the examination engagement.

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

- 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 report users may consider important to meet their informational needs. There are inherent limitations in 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 or 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.

Emphasis of Matter – Controls Did Not Operate During the Period Covered by the Report

The service organization's description of its system discusses new hires acknowledging the Code of Conduct, information security policies, confidentiality agreement, background checks and completing the security awareness training upon hire. However, during the period February 10, 2025, to May 10, 2025, the service organization did not have any new hires, where acknowledgement of the Code of Conduct, information security policies, and confidentiality agreement, background checks and security awareness training for new hires. Because these controls did not operate during the period, we were unable to test, and did not test, the operating effectiveness of those controls as evaluated using the following trust services criteria:

- CC1.1*, The entity demonstrates a commitment to integrity and ethical values*

The service organization's description of its system discusses its Risk Assessment process, which includes the controls implemented and operated to perform the risk assessment of the identified risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. However, during the period February 10, 2025, to May 10, 2025, the service organization did not conduct the risk assessment because the latest risk assessment was performed in January 2025. Because those controls did not operate during the period, we were unable to test, and did not test, the operating effectiveness of those controls as evaluated using trust services criteria:

- CC3.1, *The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.*
- CC3.2, *The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives*
- CC3.3, *The entity considers the potential for fraud in assessing risks to the achievement of objectives.*
- CC3.4, *The entity identifies and assesses changes that could significantly impact the system of internal control.*

The service organization's description of its system discusses its vendor management program, which includes the controls implemented and operated to perform security reviews on vendors. However, during the period February 10, 2025, to May 10, 2025, the service organization did not perform security reviews of its critical and high-risk vendors because the latest vendor security review was done in January 2025. Because those controls did not operate during the period, we

were unable to test, and did not test, the operating effectiveness of those controls as evaluated using trust services criteria:

- CC9.2, *The entity assesses and manages risks associated with vendors and business partners.*

Our opinion is not modified with respect to the matter emphasized.

Description of Test of Controls

The specific controls we tested, and the nature, timing, and results of those tests are listed in Section 4.

Opinion

In our opinion, in all material respects,

- the description presents Fragment's Ledger API Platform that was designed and implemented throughout the period February 10, 2025, to May 10, 2025, in accordance with the description criteria.
- the controls stated in the description were suitably designed throughout the period February 10, 2025, to May 10, 2025, to provide reasonable assurance that Fragment's service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of Fragment's controls throughout that period.
- the controls stated in the description operated effectively throughout the period February 10, 2025, to May 10, 2025, to provide reasonable assurance that Fragment's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and user entity controls assumed in the design of Fragment's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of management of Fragment; user entities of Fragment's Ledger API Platform during some or all of the period February 10, 2025, to May 10, 2025; business partners of Fragment subject to risks arising from interactions with the Ledger API Platform; practitioners providing services to such user entities and business partners; prospective user entities and business partners; and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, and other parties.
- Internal control and its limitations.

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

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

Insight Assurance LLC

Tampa, Florida
July 23, 2025

SECTION 2:
FRAGMENT FOUNDRIES INC.'S MANAGEMENT ASSERTION

FRAGMENT FOUNDRIES INC.'S MANAGEMENT ASSERTION

We have prepared the description of Fragment Foundries Inc.'s ("Fragment" or "the service organization") Ledger API Platform entitled "Fragment Foundries Inc.'s description of its Ledger API Platform" throughout the period February 10, 2025, to May 10, 2025, ("description") based on the criteria for a description of a service organization's system set forth in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)* in AICPA, *Description Criteria*, (description criteria). The description is intended to provide report users with information about the Ledger API Platform that may be useful when assessing the risks arising from interactions with Fragment's system, particularly information about system controls that Fragment has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA*, Trust Services Criteria.*

Fragment uses Amazon Web Services (AWS) (the "subservice organization") to provide hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Fragment, to achieve Fragment's service commitments and system requirements based on the applicable trust services criteria. The description presents Fragment's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Fragment's controls. The description does not disclose the actual controls at the subservice organization.

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

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

- the description presents Fragment's Ledger API Platform that was designed and implemented throughout the period February 10, 2025, to May 10, 2025, in accordance with the description criteria.
- the controls stated in the description were suitably designed throughout the period February 10, 2025, to May 10, 2025, to provide reasonable assurance that Fragment's service commitments and system requirements would be achieved based on the applicable trust services criteria, and if the subservice organization and user entities applied the complementary controls assumed in the design of Fragment's controls.

- the controls stated in the description operated effectively throughout the period February 10, 2025, to May 10, 2025, to provide reasonable assurance that Fragment's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Fragment's controls operated effectively throughout that period.

Fragment Foundries Inc.
July 23, 2025

SECTION 3:
FRAGMENT FOUNDRIES INC.'S DESCRIPTION OF ITS LEDGER API PLATFORM

FRAGMENT FOUNDRIES INC.'S DESCRIPTION OF ITS LEDGER API PLATFORM

COMPANY BACKGROUND

Fragment Foundries Inc ("Fragment") is a financial technology company building a ledger API and developer tools to support companies building products that move money. Fragment is fully remote with employees in New York, San Francisco, Vancouver, and Sydney.

DESCRIPTION OF SERVICES OVERVIEW

The Fragment Platform provides customers with a Ledger API, language specific SDKs, and user-facing Dashboard to build and manage their Ledger data.

The Fragment Platform facilitates user onboarding, API client management, permission, ledger schema design, and data retrieval. In addition, Fragment works closely with customers to help translate their product funds flow into the Fragment Platform during their onboarding process.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Fragment designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Fragment makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Fragment has established for the services. The system services are subject to the Security commitments established internally for its services.

Fragment's commitments to users are communicated through Service Level Agreements (SLAs) or Master Service Agreements (MSAs), online Privacy Policy, and in the description of the service offering provided online at fragment.dev.

SECURITY COMMITMENTS

Security commitments include, but are not limited to, the following:

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role.
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system.
- Continuous vulnerability scans over the system and network, and at least annual penetration tests over the production environment.
- Operational procedures for managing security incidents and breaches, including notification procedures.
- Use of encryption technologies to protect customer data both at rest and in transit.
- Use of data retention and data disposal.
- Up-time availability of production systems.

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

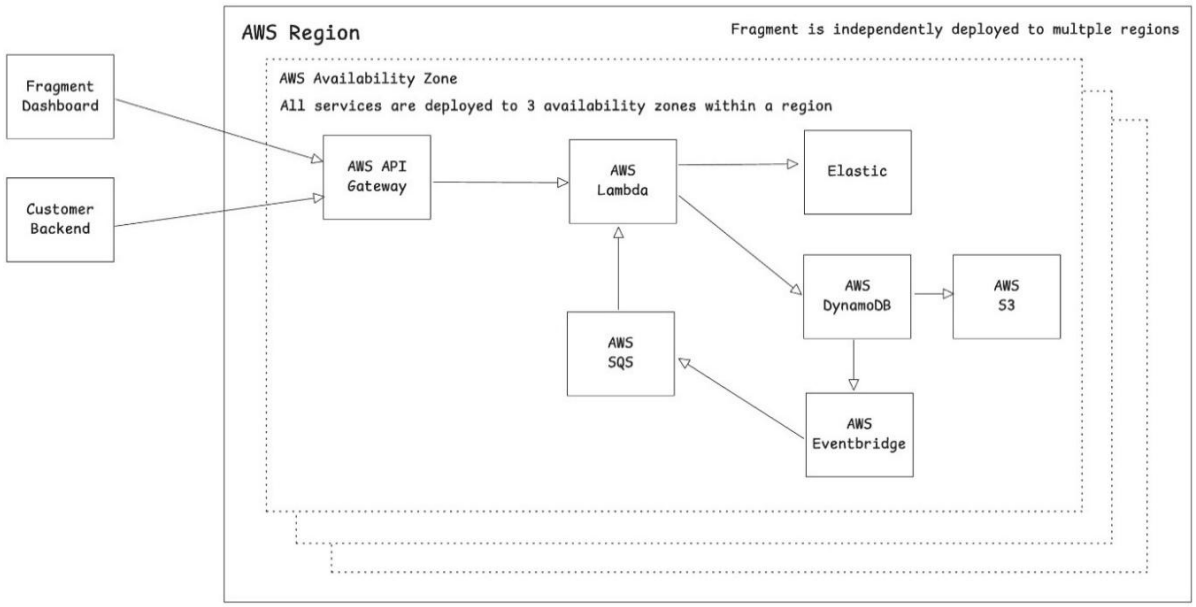
The system description is comprised of the following components:

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

INFRASTRUCTURE

Fragment maintains a system inventory that includes virtual machines, computers (desktops and laptops), and networking devices (switches and routers). The inventory documents device name, inventory type, description, and owner.

To outline the topology of its network, the organization maintains the following network diagram.



Primary infrastructure used to provide Fragment's Platform includes the following:

Infrastructure		
Hardware	**Type**	**Purpose**
AWS Lambda	AWS	Executes Fragment's core business logic in response to API calls and events across availability zones.
AWS API Gateway	AWS	Serves as the public HTTP endpoint ("front door") for Fragment's dashboard and customer backend, routing requests to the appropriate Lambda.
AWS DynamoDB	AWS	Stores core ledger data for transactional processing.
AWS EventBridge	AWS	Routes events from data changes and other services, enabling decoupled, event-driven workflows.
AWS SQS	AWS	Buffers asynchronous tasks or workflows, decoupling Lambda processes and smoothing traffic spikes.
AWS S3	AWS	Stores backups and logs
Elastic Cloud	AWS	Provides search for data replicated from AWS DynamoDB

SOFTWARE

Fragment is responsible for managing the development and operation of the Fragment Platform system including infrastructure components such as servers, databases, and storage systems. The in-scope Fragment software components are shown in the table provided below:

Software	
System/Application	**Purpose**
GuardDuty	Security application used for automated intrusion detection (IDS)
AWS CloudWatch	Monitoring application used to provide monitoring, alter, and notification services for Fragment platform.
Amazon Web Services	Cloud computing platform providing core infrastructure including compute, storage, networking, and databases.
Certn (Partner)	Employment background screening and identity verification partner.
GitHub	Source code repository and version control system used for software development and collaboration.
Notion	Knowledge management and documentation platform used for internal wikis, notes, and project planning.
Google Workspace	Productivity suite used for email (Gmail), file storage (Drive), and collaboration (Docs, Sheets, etc.).
Justworks	HR platform used for payroll, benefits administration, and compliance.

Software	
System/Application	**Purpose**
Linear	Project management and issue tracking tool used for software development workflows.
Slack	Communication and collaboration platform used for internal team messaging and coordination.
Vanta	Compliance automation platform used to manage and monitor security controls (e.g., SOC 2, ISO 27001)

PEOPLE

The company employs dedicated team members to handle major product functions, including operations, and support. The IT/Engineering Team monitors the environment, as well as manages data backups and recovery. The company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep the company and its data secure.

Management: Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment. This includes CEO and Head of Engineering.

Engineering: Responsible for the development, testing, deployment, and maintenance of the source code for the system. Responsible for the product life cycle, including adding additional product functionality. Responsible for maintaining the availability of production infrastructure and managing access and security for production infrastructure.

DATA

Data, as defined by Fragment, constitutes the following:

User and account data - this includes Personally Identifiable Information (PII) and other data from employees, customers, users (customers' employees), and other third parties such as suppliers, vendors, business partners, and contractors. This collection is permitted under the Terms of Service and Privacy Policy (as well as other separate agreements with vendors, partners, suppliers, and other relevant third parties). Access to PII is controlled through processes for provisioning system permissions, as well as ongoing monitoring activities, to ensure that sensitive data is restricted to employees based on job function.

Data is categorized in the following major types of data used by Fragment.

Data		
Category	**Description**	**Examples**
Public	Public information is not confidential and can be made public without any implications for Fragment.	• Press releases • Public website

Data		
Category	**Description**	**Examples**
Internal	Access to internal information is approved by management and is protected from external access.	• Internal memos • Design documents • Product specifications • Correspondences
Customer data	Information received from customers for processing or storage by Fragment. Fragment must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Customer operating data • Customer PII • Customers' customers' PII • Anything subject to a confidentiality agreement with a customer
Company data	Information collected and used by Fragment to operate the business. Fragment must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Legal documents • Contractual agreements • Employee PII • Employee salaries

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements, if any. Customer data is captured which is utilized by the company in delivering its services.

All personnel and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, Fragment has policies and procedures in place to proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

PROCESSES AND PROCEDURES

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by management, the executive team, and control owners. These procedures cover the following key security life cycle areas:

- Logical access
- Change control
- Data communications
- Risk assessment
- Data retention
- Third-party management

Logical Access

Fragment provides employees and contracts access to infrastructure via a role-based access control system, to ensure uniform, least privileged access to identified users and to maintain simple and reportable user provisioning and deprovisioning processes.

Access to these systems is split into admin roles, user roles, and no access roles. User access and roles are reviewed on a quarterly basis to ensure the least privilege of access.

Operations, Management is responsible for provisioning access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing Fragment's policies, completing security training. These steps must be completed at the time of hire.

When an employee is terminated, Operations Management is responsible for deprovisioning access to all in scope systems within 24 business hours for that employee's termination.

Computer Operations - Backups

Customer data is backed up and monitored by the Engineering, Head of Engineering for completion and exceptions. If there is an exception, Engineering, Head of Engineering will perform troubleshooting to identify the root cause and either rerun the backup or as part of the next scheduled backup job.

Backup infrastructure is maintained in AWS with physical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

Change Management

Fragment 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 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.

Data Communications

Fragment has elected to use a platform-as-a-service (PaaS) to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. The PaaS simplifies our logical network configuration by providing an effective firewall around all the Fragment application containers, with the only ingress from the network via HTTPS connections to designated web frontend endpoints.

The PaaS provider also automates the provisioning and deprovisioning of containers to match the desired configuration; if an application container fails, it will be automatically replaced, regardless of whether that failure is in the application or on underlying hardware.

Fragment uses an automated monitoring service to perform vulnerability scans and engages an external firm to perform annual penetration testing to look for unidentified vulnerabilities, and the product engineering team responds to any issues identified via the regular incident response and change management process.

Boundaries of the System

The boundaries of the Fragment Platform are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the Fragment Platform.

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities.

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 Fragment's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Fragment'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 for employees as a component of the hiring process.

Commitment to Competence

Fragment'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 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

The Fragment management team must balance two competing interests: continuing to grow and develop in a cutting edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly sensitive data and workflows our customers entrust to us.

The management team meets frequently to be briefed on technology changes that impact the way Fragment can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally any regulatory changes that may require Fragment to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and duties to new and existing customers.

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

- Management is periodically 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.

Organizational Structure and Assignment of Authority and Responsibility

Fragment'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.

Fragment'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.

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 Resources Policies and Practices

Fragment'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 ensure the service organization is operating at maximum efficiency. Fragment'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 acknowledgment 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.
- Personnel termination procedures are in place to guide the termination process and are documented in a termination checklist.

RISK ASSESSMENT PROCESS

Fragment's risk assessment process identifies and manages risks that could potentially affect Fragment's ability to provide reliable and secure services to our customers. As part of this process, Fragment maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular Fragment's product development process so they can be dealt with predictably and iteratively.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Fragment Platform; as well as the nature of the components of the system result in risks that the criteria will not be met. Fragment 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, Fragment's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

CONTROL ACTIVITIES

Control activities are the actions established by policies and procedures to help ensure that management directives to mitigate risks to the achievement of objectives are executed. Control activities are performed at all levels of the organization and various stages within business processes, and over the technology environment.

INFORMATION AND COMMUNICATION SYSTEMS

Information and communication are an integral component of Fragment'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.

Fragment uses several information and communication channels internally to share information with management, employees, contractors, and customers. Fragment uses chat systems and email as the primary internal and external communications channels.

Structured data is communicated internally via SaaS applications and project management tools. Finally, Fragment uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

MONITORING CONTROLS

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Fragment management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures are also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

Ongoing Monitoring

Fragment'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 Fragment'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 to address 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 Fragment's personnel.

Monitoring of the Subservice Organization

Fragment uses Amazon Web Services (AWS) to provide hosting services.

Management of Fragment receives and reviews the SOC 2 report of Amazon Web Services (AWS) on an annual basis. In addition, through its daily operational activities, Fragment's management monitors the services performed by Amazon Web Services (AWS) to gain comfort that operations and controls expected to be implemented at the subservice organization are functioning effectively.

Reporting Deficiencies

Our internal risk management tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. 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 DURING THE PERIOD

No significant changes have occurred to the services provided to user entities during the examination period.

SYSTEM INCIDENTS DURING THE PERIOD

No significant system incidents have occurred to the services provided to user entities during the examination period.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOCs)

Fragment's controls related to the system cover only a portion of overall internal control for each user entity of Fragment. It is not feasible for the trust services criteria related to the system to be achieved solely by Fragment. Therefore, each user entity's internal controls should be evaluated in conjunction with Fragment's controls and the related tests and results described in Section 4 of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

#	Complementary Subservice Organization Controls (CSOC)	Related Criteria
1	Amazon Web Services (AWS) is responsible for maintaining physical security and environmental protection controls over the data centers hosting the Fragment infrastructure.	CC6.4

#	Complementary Subservice Organization Controls (CSOC)	Related Criteria
2	Amazon Web Services (AWS) is responsible for the destruction of physical assets hosting the production environment.	CC6.5

COMPLEMENTARY USER ENTITY CONTROLS (CUECs)

Fragment's controls related to the Ledger API Platform only cover a portion of the overall internal controls for each user entity. It is not feasible for the applicable trust services criteria related to the system to be achieved solely by Fragment's control procedures. Accordingly, user entities, in conjunction with the services, should establish their internal controls or procedures to complement those of Fragment.

User auditors should determine whether the following controls have been in place in operation at the user organization:

1. User entities should have controls in place to provide reasonable assurance that user access including the provisioning and de-provisioning are designed appropriately and operating effectively.
2. User entities are responsible for reporting issues with Fragment systems and platforms.
3. User entities are responsible for understanding and complying with their contractual obligations to Fragment.
4. User entities are responsible for notifying Fragment of changes made to the administrative contact information.

TRUST SERVICES CATEGORY, CRITERIA, AND RELATED CONTROLS

The Security category and applicable trust services criteria were used to evaluate the suitability of the design of controls stated in the description. The criteria and controls designed, implemented, and operated to meet them ensure that information, systems, and access (physical and logical) are protected against unauthorized access, and systems are available for operation and use. The controls supporting the applicable trust services criteria are included in Section 4 of this report and are an integral part of the description of the system.

For specific criteria, which were deemed not relevant to the system, see Section 4 for the related explanation.

SECTION 4:
TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS AND TESTS OF CONTROLS

TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

This SOC 2 Type 2 report was prepared in accordance with the AICPA attestation standards and has been performed to examine the suitability of the design and operating effectiveness of controls to meet the criteria for the Security category set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*With Revised Points of Focus—2022)* in AICPA*, Trust Services Criteria* throughout the period February 10, 2025, to May 10, 2025.

The applicable trust services criteria and related controls specified by Fragment are presented in Section 4 of this report.

Test procedures performed in connection with determining the operating effectiveness of controls detailed here in Section 4 are described below:

- Inquiries – Inquiry of appropriate personnel and corroboration with management.
- Observation – Observation of the application, performance, or existence of the control.
- Inspection – Inspection of documents and reports indicating the performance of the control.
- Reperformance – Reperformance of the control.

FOOTNOTES FOR TEST RESULTS WHEN NO TESTS OF OPERATING EFFECTIVENESS WERE PERFORMED

1. The circumstances that warranted the operation of the control did not occur during the examination period; therefore, no tests of operating effectiveness were performed.
2. The operation of the control was performed outside the examination period; therefore, no tests of operating effectiveness were performed.

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	The company performs background checks on new employees.	Per inquiry with management and inspection of the compliance tool, there were no new employees during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.
CC1.1.2	The company requires contractor/employee agreements to include a Code of Conduct or reference to the company Code of Conduct.	Inspected the contractor or employment agreement document to determine it included a reference to the company Code of Conduct.	No exceptions noted.
CC1.1.3	The company requires employees/contractors to acknowledge a code of conduct at the time of hire. Employees who violate the Code of Conduct are subject to disciplinary actions in accordance with a Disciplinary Policy.	Per inquiry with management and inspection of the employee listing, there were no new hires during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.
		Inspected the company's Code of Conduct and Human Resource Security Policy to determine that employees who violated the Code of Conduct were subject to disciplinary actions in accordance with the Disciplinary Policy.	No exceptions noted.
CC1.1.4	The company requires contractors to sign a confidentiality agreement at the time of engagement.	Per inquiry with management and inspection of the employee listing, there were no new contractors during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.1.5	The company requires employees to sign a confidentiality agreement during onboarding.	Per inquiry with management and inspection of the employee listing, there were no new employees during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.
CC1.1.6	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected the completed performance evaluation for a sample of active employees to determine that the company's managers were required to complete performance evaluations for direct reports annually.	No exceptions noted.
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected the company's Information Security Roles and Responsibilities Policy to determine the company's management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	No exceptions noted.
CC1.3.2	The company maintains an organizational chart that describes the organizational structure and reporting lines.	Inspected the company's organizational chart to determine that the company maintains an organizational chart that described the organizational structure and reporting lines.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.3.3	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Information Security Roles and Responsibilities Policy.	Inspected the company's Information Security Roles and Responsibilities Policy to determine the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy.	No exceptions noted.
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Information Security Roles and Responsibilities Policy.	Inspected the company's Information Security Roles and Responsibilities Policy to determine the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy.	No exceptions noted.
CC1.4.2	The company performs background checks on new employees.	Per inquiry with management and inspection of the compliance tool, there were no new employees during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.
CC1.4.3	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected the completed performance evaluation for a sample of active employees to determine that the company's managers were required to complete performance evaluations for direct reports annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.4.4	The company requires employees to complete security awareness training at the time of hire and at least annually thereafter.	Inspected the security awareness training topics to determine that the security awareness training covered areas to educate personnel on information security topics and the latest trends to protect sensitive data.	No exceptions noted.
		Per inquiry with management and inspection of the employee listing, there were no new hires during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.
		Per inquiry with management and inspection of sample for active employees, security awareness training was conducted in January 2025; therefore, no testing was performed.	No testing performed. See footnote 2 above.
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Information Security Roles and Responsibilities Policy.	Inspected the company's Information Security Roles and Responsibilities Policy to determine the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC1.5.2	The company requires employees/contractors to acknowledge a code of conduct at the time of hire. Employees who violate the Code of Conduct are subject to disciplinary actions in accordance with a Disciplinary Policy.	Per inquiry with management and inspection of the employee listing, there were no new hires during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.
		Inspected the company's Code of Conduct and Human Resource Security Policy to determine that employees who violated the Code of Conduct were subject to disciplinary actions in accordance with the Disciplinary Policy.	No exceptions noted.
CC1.5.3	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected the completed performance evaluation for a sample of active employees to determine that the company’s managers were required to complete performance evaluations for direct reports annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
COMMUNICATION AND INFORMATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.	Inspected the company's compliance platform to determine that control self-assessments were performed annually.	No exceptions noted.
CC2.1.2	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected the log management tool configurations to determine that the company utilized a log management tool to identify events that may potentially impact on the company's ability to achieve its security objectives.	No exceptions noted.
CC2.1.3	Host-based vulnerability scans are performed continuously. Critical and high vulnerabilities are tracked to remediation.	Inspected the vulnerability scan report from the compliance tool to determine that vulnerability scans were performed continuously on in-scope systems.	No exceptions noted.
		Inspected the remediation ticket/notes from the compliance tool to determine that the critical and high vulnerabilities are tracked to remediation.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
COMMUNICATION AND INFORMATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns.	Inspected the company's whistleblower policy to determine that company has established a formalized and an anonymous communication channel for users to report potential issues or fraud concerns.	No exceptions noted.
CC2.2.2	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected the company's Information Security Roles and Responsibilities Policy to determine the company's management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	No exceptions noted.
CC2.2.3	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Information Security Roles and Responsibilities Policy.	Inspected the company's Information Security Roles and Responsibilities Policy to determine the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy.	No exceptions noted.
CC2.2.4	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were documented and reviewed annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
COMMUNICATION AND INFORMATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC2.2.5	The company communicates system changes to authorized internal users.	Inspected the internal communication channel to determine that the company communicated system changes to authorized internal users.	No exceptions noted.
CC2.2.6	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's Incident Response Plan and the compliance platform to determine the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.
CC2.2.7	The company provides a description of its products and services to internal and external users.	Inspected the company's website to determine that the company provides a description of its products and services to internal and external users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
COMMUNICATION AND INFORMATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC2.2.8	The company requires employees to complete security awareness training at the time of hire and at least annually thereafter.	Inspected the security awareness training topics to determine that the security awareness training covered areas to educate personnel on information security topics and the latest trends to protect sensitive data.	No exceptions noted.
		Per inquiry with management and inspection of the employee listing, there were no new hires during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.
		Per inquiry with management and inspection of sample for active employees, security awareness training was conducted in January 2025; therefore, no testing was performed.	No testing performed. See footnote 2 above.
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	The company notifies customers of critical system changes that may affect their processing.	Inspected the company's website to determine the customers are notified of critical system changes that could affect their processing.	No exceptions noted.
CC2.3.2	The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	Inspected the company's website to determine the company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
COMMUNICATION AND INFORMATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC2.3.3	The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).	Inspected the company's terms of services from the website to determine the company communicated its security commitments to customers.	No exceptions noted.
CC2.3.4	The company provides guidelines and technical support resources relating to system operations to customers.	Inspected the company's website to determine that the company provides guidelines and technical support resources relating to system operations to customers.	No exceptions noted.
CC2.3.5	The company provides a description of its products and services to internal and external users.	Inspected the company's website to determine that the company provides a description of its products and services to internal and external users.	No exceptions noted.
CC2.3.6	The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected the written agreements for the vendors to determine they were in place and included confidentiality and privacy commitments.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the Risk Management Policy to determine that the company specified its objectives to enable the identification and assessment of risk related to the objectives.	No exceptions noted.
CC3.1.2	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company's Risk Management Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2.1	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the company's Business Continuity and Disaster Recovery Plan to determine the company has a documented business continuity/disaster recovery (BC/DR) plan in place.	No exceptions noted.
		Inspected the company's BC/DR Plan Tabletop Disaster Recovery Exercise to determine the company has tested the business continuity/disaster recovery (BC/DR) plan annually.	No exceptions noted.
CC3.2.2	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Per inquiry with management and inspection of the latest risk assessment performed in the compliance tool, the latest annual security risk assessment was performed in January 2025; therefore, no testing was performed.	No testing performed. See footnote 2 above.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC3.2.3	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company's Risk Management Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC3.2.4	The company has a vendor management program in place. Components of this program include: - critical vendor inventory; - vendor's security and privacy requirements; and - review of critical vendors at least annually.	Inspected the company's Third-Party Management Policy to determine that the company had a vendor management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the vendor listing to determine that all the critical vendors inventory was in place.	No exceptions noted.
		Per inquiry with management and inspection of vendor reviews, the vendor reviews were conducted in January 2025; therefore, no testing was performed.	No testing performed. See footnote 2 above.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Per inquiry with management and inspection of the latest risk assessment performed in the compliance tool, the latest annual security risk assessment was performed in January 2025; therefore, no testing was performed.	No testing performed. See footnote 2 above.
CC3.3.2	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company’s Risk Management Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected the company's Operations Security Policy to determine the company had a configuration management procedure in place to ensure that system configurations were deployed consistently throughout the environment.	No exceptions noted.
CC3.4.2	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate high and critical vulnerabilities in accordance with SLAs.	Inspected the latest penetration testing report to determine the company's penetration testing is performed at least annually.	No exceptions noted.
		Per inquiry with management and inspection of the latest penetration testing report, there were no critical or high vulnerabilities identified; therefore, no testing was performed.	No testing performed. See footnote 1 above.
CC3.4.3	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Per inquiry with management and inspection of the latest risk assessment performed in the compliance tool, the latest annual security risk assessment was performed in January 2025; therefore, no testing was performed.	No testing performed. See footnote 2 above.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC3.4.4	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company's Risk Management Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
MONITORING ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.	Inspected the company's compliance platform to determine that control self-assessments were performed annually.	No exceptions noted.
CC4.1.2	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate high and critical vulnerabilities in accordance with SLAs.	Inspected the latest penetration testing report to determine the company's penetration testing is performed at least annually.	No exceptions noted.
		Per inquiry with management and inspection of the latest penetration testing report, there were no critical or high vulnerabilities identified; therefore, no testing was performed.	No testing performed. See footnote 1 above.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
MONITORING ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC4.1.3	The company has a vendor management program in place. Components of this program include: - critical vendor inventory; - vendor's security and privacy requirements; and - review of critical vendors at least annually.	Inspected the vendor listing to determine that all the critical vendors inventory was in place.	No exceptions noted.
		Inspected the company's Third-Party Management Policy to determine that the company had a vendor management program in place that included the security requirements for vendors.	No exceptions noted.
		Per inquiry with management and inspection of vendor reviews, the vendor reviews were conducted in January 2025; therefore, no testing was performed.	No testing performed. See footnote 2 above.
CC4.1.4	Host-based vulnerability scans are performed continuously. Critical and high vulnerabilities are tracked to remediation.	Inspected the vulnerability scan report from the compliance tool to determine that vulnerability scans were performed continuously on in-scope systems.	No exceptions noted.
		Inspected the remediation ticket/notes from the compliance tool to determine that the critical and high vulnerabilities are tracked to remediation.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
MONITORING ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC4.2.1	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.	Inspected the company's compliance platform to determine that control self-assessments were performed annually.	No exceptions noted.
CC4.2.2	The company has a vendor management program in place. Components of this program include: - critical vendor inventory; - vendor's security and privacy requirements; and - review of critical vendors at least annually.	Inspected the company's Third-Party Management Policy to determine that the company had a vendor management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the vendor listing to determine that all the critical vendors inventory was in place.	No exceptions noted.
		Per inquiry with management and inspection of vendor reviews, the vendor reviews were conducted in January 2025; therefore, no testing was performed.	No testing performed. See footnote 2 above.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1.1	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were documented and reviewed annually.	No exceptions noted.
CC5.1.2	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company's Risk Management Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's Operations Security and Secure Development policies to determine that the company had a formal SDLC methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC5.2.2	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were documented and reviewed annually.	No exceptions noted.
CC5.2.3	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the company's Access Control Policy to determine the Access Control Policy has documented the requirements for adding, modifying, and removing user access.	No exceptions noted.
CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's Information Security Policies and Procedures to determine that the company's Information Security Policies and procedures were documented and reviewed annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC5.3.2	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the company's Operations Security Policy to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, Inspected, and approved before being implemented in the production environment.	No exceptions noted.
		Inspected the change management documentation for a sample of changes to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
CC5.3.3	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's Operations Security and Secure Development policies to determine that the company had a formal SDLC methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC5.3.4	The company's data backup policy documents requirements for backup and recovery of customer data.	Inspected the company's Operations Security Policy and Internal Retention and Disposal Procedure to determine that the company has documented requirements for backup and recovery of customer data.	No exceptions noted.
CC5.3.5	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Information Security Roles and Responsibilities Policy.	Inspected the company's Information Security Roles and Responsibilities Policy to determine the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Roles and Responsibilities Policy.	No exceptions noted.
CC5.3.6	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were documented and reviewed annually.	No exceptions noted.
CC5.3.7	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's Incident Response Plan and the compliance platform to determine the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC5.3.8	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the Risk Management Policy to determine that the company specified its objectives to enable the identification and assessment of risk related to the objectives.	No exceptions noted.
CC5.3.9	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company's Risk Management Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC5.3.10	The company has a vendor management program in place. Components of this program include: - critical vendor inventory; - vendor's security and privacy requirements; and - review of critical vendors at least annually.	Inspected the company's Third-Party Management Policy to determine that the company had a vendor management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the vendor listing to determine that all the critical vendors inventory was in place.	No exceptions noted.
		Per inquiry with management and inspection of vendor reviews, the vendor reviews were conducted in January 2025; therefore, no testing was performed.	No testing performed. See footnote 2 above.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.1.1	The company maintains a formal inventory of production system assets.	Inspected an inventory listing of information assets to determine that the company maintained a formal inventory of production system assets.	No exceptions noted.
CC6.1.2	The company restricts access to migrate changes to production to authorized personnel.	Inspected the list of users with access to production to determine that the company restricts access to migrate changes to production to authorized personnel.	No exceptions noted.
CC6.1.3	The company requires authentication to production datastores to use authorized secure authentication mechanisms, such as unique SSH key.	Inspected the access list from the production environment datastores of AWS and GitHub to determine that authorized secure authentication mechanisms were used.	No exceptions noted.
CC6.1.4	The company restricts privileged access to encryption keys to authorized users with a business need.	Inspected the company's Cryptography Policy to determine that the company restricted privileged access to encryption keys to authorized users with a business need.	No exceptions noted.
		Inspected the list of users with privileged access to encryption keys to determine that the company restricted privileged access to authorized users with a business need.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.1.5	The company's datastores housing sensitive customer data are encrypted at rest.	Inspected the compliance tool to determine the company's datastores housing sensitive customer data are encrypted at rest.	No exceptions noted.
CC6.1.6	The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.	Inspected the list of users with privileged access to the systems and applications to determine that the company requires authentication into systems and applications to use unique username and password.	No exceptions noted.
CC6.1.7	The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the company’s Data Management Policy to determine that the company has data classification in place to help ensure that confidential data was properly secured and restricted to authorized personnel.	No exceptions noted.
CC6.1.8	System access restricted to authorized access only	Inspected system configuration for the in-scope systems to determine that system access is restricted to authorized personnel only.	No exceptions noted.
CC6.1.9	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the company’s Access Control Policy to determine the Access Control Policy has documented the requirements for adding, modifying, and removing user access.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.1.10	The company restricts privileged access to databases to authorized users with a business need.	Inspected the production environment user groups to determine that the company restricts privileged access to databases to authorized users with a business need.	No exceptions noted.
CC6.1.11	The company restricts privileged access to the security groups to authorized users with a business need.	Inspected the AWS security groups in the compliance tool to determine that company privileged access was restricted to the security groups to authorized users with a business need.	No exceptions noted.
CC6.1.12	The company restricts privileged access to the operating system to authorized users with a business need.	Inspected AWS users list to determine that privileged access to operating system was restricted to authorized users with a business need.	No exceptions noted.
CC6.1.13	The company restricts privileged access to the production network to authorized users with a business need.	Inspected the list of users with privileged access to determine that privileged access was restricted to the production network and granted to authorized users with a business need.	No exceptions noted.
CC6.1.14	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected the in-scope user listings for a sample of active employee listing to determine that the company ensured that user access to in-scope system components was based on job role and function.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.1.15	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the list of users with privileged access to the production network to determine that the company requires authentication into the "production network" to use unique usernames and passwords.	No exceptions noted.
CC6.1.16	The company requires passwords for in-scope system components to be configured according to the company's policy.	Inspected the password configurations and written password policy to determine that the company required passwords for in-scope system components to be configured according to the company's policy.	No exceptions noted.
CC6.1.17	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Inspected the MFA configurations to determine that the company's production systems could only be remotely accessed by authorized employees possessing a valid MFA method.	No exceptions noted.
CC6.1.18	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the company's Infrastructure as a Service provider's SSL/TLS certificate to determine that the company's production systems could only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
CC6.1.19	The company's network is segmented to prevent unauthorized access to customer data.	Inspected the network configurations to determine that the company's network was segmented to prevent unauthorized access to customer data.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC6.2.1	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the company's Access Control Policy to determine the Access Control Policy has documented the requirements for adding, modifying, and removing user access.	No exceptions noted.
CC6.2.2	The company conducts quarterly access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the user access review documentation to determine that the company conducted quarterly access reviews for the in-scope system components to help ensure that access was restricted appropriately, and required changes are tracked to completion.	No exceptions noted.
CC6.2.3	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Per inquiry with management and inspection of the user listing, there were no terminated employees during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.
CC6.2.4	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected the in-scope user listings for a sample of active employee listing to determine that the company ensured that user access to in-scope system components was based on job role and function.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.2.5	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the list of users with privileged access to the production network to determine that the company requires authentication into the "production network" to use unique usernames and passwords.	No exceptions noted.
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.3.1	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the company's Access Control Policy to determine the Access Control Policy has documented the requirements for adding, modifying, and removing user access.	No exceptions noted.
CC6.3.2	The company conducts quarterly access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the user access review documentation to determine that the company conducted quarterly access reviews for the in-scope system components to help ensure that access was restricted appropriately, and required changes are tracked to completion.	No exceptions noted.
CC6.3.3	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Per inquiry with management and inspection of the user listing, there were no terminated employees during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.3.4	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected the in-scope user listings for a sample of active employee listing to determine that the company ensured that user access to in-scope system components was based on job role and function.	No exceptions noted.
CC6.3.5	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the list of users with privileged access to the production network to determine that the company requires authentication into the "production network" to use unique usernames and passwords.	No exceptions noted.
CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
CC6.4.1	The company conducts quarterly access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	This control activity is the responsibility of the subservice organization. Refer to the Subservice Organization section above for controls managed by the subservice organization.	

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
CC6.5.1a	The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	Per inquiry with management and inspection of compliance tool, there were no disposals during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.
CC6.5.2	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's Information Security Policies and Procedures to determine that the company's Information Security Policies and procedures were documented and reviewed annually.	No exceptions noted.
CC6.5.3	The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	Inspected the company's Data Management Policy to determine the company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	No exceptions noted.
CC6.5.4	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Per inquiry with management and inspection of the user listing, there were no terminated employees during the examination period; therefore, no testing was performed.	No testing performed. See footnote 1 above.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.5.1b	The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	This control activity is the responsibility of the subservice organization. Refer to the Subservice Organization section above for controls managed by the subservice organization.	
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the list of users with privileged access to the production network to determine that the company requires authentication into the "production network" to use unique usernames and passwords.	No exceptions noted.
CC6.6.2	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Inspected the MFA configurations to determine that the company’s production systems could only be remotely accessed by authorized employees possessing a valid MFA method.	No exceptions noted.
CC6.6.3	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the company’s Infrastructure as a Service provider’s SSL/TLS certificate to determine that the company’s production systems could only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.6.4	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the IDS configurations to determine that the company uses IDS to provide continuous monitoring of the company's network and early detection of potential security breaches.	No exceptions noted.
CC6.6.5	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the company's website and TLS certificates to determine that the company used secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.
CC6.6.6	The company uses security groups and configures them to prevent unauthorized access.	Inspected the AWS security groups in the compliance tool to determine that the company used security groups and configured them to prevent unauthorized access.	No exceptions noted.
CC6.6.7	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Inspected the company's Configuration and Hardening Standards to determine the company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.6.8	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the Operations Security Policy, Configuration and Hardening Standard to determine that the company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
CC6.7.1	The company encrypts portable devices when used.	Inspected the company's Cryptography Policy to determine that the company encrypted portable media devices when used.	No exceptions noted.
		Inspected the encryption configurations for a sample of devices from the user listing to determine that the company encrypted portable media devices when used.	No exceptions noted.
CC6.7.2	The company has a mobile device monitoring (MDM) system in place to centrally manage mobile devices supporting the service.	Inspected the company’s compliance tool to determine that the company had a mobile device monitoring system in place to centrally monitor mobile devices supporting the service.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.7.3	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the company's website and TLS certificates to determine that the company used secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.
CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC6.8.1	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's Operations Security and Secure Development policies to determine that the company had a formal SDLC methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.
CC6.8.2	The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.	Inspected the anti-malware configurations for a sample of workstations to determine that the company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC6.8.3	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the Operations Security Policy, Configuration and Hardening Standard to determine that the company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
CC7.1.1	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected the company's Operations Security Policy to determine the company had a configuration management procedure in place to ensure that system configurations were deployed consistently throughout the environment.	No exceptions noted.
CC7.1.2	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the company's Operations Security Policy to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, Inspected, and approved before being implemented in the production environment.	No exceptions noted.
		Inspected the change management documentation for a sample of changes to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.1.3	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the company's Operations Security Policy to determine that the company's formal policies outlined the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	No exceptions noted.
CC7.1.4	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Per inquiry with management and inspection of the latest risk assessment performed in the compliance tool, the latest annual security risk assessment was performed in January 2025; therefore, no testing was performed.	No testing performed. See footnote 2 above.
CC7.1.5	Host-based vulnerability scans are performed continuously. Critical and high vulnerabilities are tracked to remediation.	Inspected the vulnerability scan report from the compliance tool to determine that vulnerability scans were performed continuously on in-scope systems.	No exceptions noted.
		Inspected the remediation ticket/notes from the compliance tool to determine that the critical and high vulnerabilities are tracked to remediation.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.2.1	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate high and critical vulnerabilities in accordance with SLAs.	Inspected the latest penetration testing report to determine the company's penetration testing is performed at least annually.	No exceptions noted.
		Per inquiry with management and inspection of the latest penetration testing report, there were no critical or high vulnerabilities identified; therefore, no testing was performed.	No testing performed. See footnote 1 above.
CC7.2.2	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the IDS configurations to determine that the company uses IDS to provide continuous monitoring of the company's network and early detection of potential security breaches.	No exceptions noted.
CC7.2.3	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected the log management tool configurations to determine that the company utilized a log management tool to identify events that may potentially impact on the company's ability to achieve its security objectives.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.2.4	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Inspected the monitoring tool configurations to determine that an infrastructure monitoring tool was utilized to monitor systems, infrastructure, and performance and generated alerts when specific predefined thresholds were met.	No exceptions noted.
CC7.2.5	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the company's Operations Security Policy to determine that the company's formal policies outlined the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	No exceptions noted.
CC7.2.6	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the Operations Security Policy, Configuration and Hardening Standard to determine that the company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.2.7	Host-based vulnerability scans are performed continuously. Critical and high vulnerabilities are tracked to remediation.	Inspected the vulnerability scan report from the compliance tool to determine that vulnerability scans were performed continuously on in-scope systems.	No exceptions noted.
		Inspected the remediation ticket/notes from the compliance tool to determine that the critical and high vulnerabilities are tracked to remediation.	No exceptions noted.
CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.3.1	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's Incident Response Plan and the compliance platform to determine the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.3.2	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the company's Incident Response Plan to determine the company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
		Inspected the incident listing to determine that the company's security and privacy incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
CC7.4 - The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.4.1	The company tests their incident response plan at least annually.	Inspected a sample incident report to determine that company tested their incident response plan at least annually.	No exceptions noted.
CC7.4.2	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's Incident Response Plan and the compliance platform to determine the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.4.3	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the company's Incident Response Plan to determine the company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
		Inspected the incident listing to determine that the company's security and privacy incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
CC7.4.4	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the Operations Security Policy, Configuration and Hardening Standard to determine that the company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.4.5	Host-based vulnerability scans are performed continuously. Critical and high vulnerabilities are tracked to remediation.	Inspected the vulnerability scan report from the compliance tool to determine that vulnerability scans were performed continuously on in-scope systems.	No exceptions noted.
		Inspected the remediation ticket/notes from the compliance tool to determine that the critical and high vulnerabilities are tracked to remediation.	No exceptions noted.
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the company's Business Continuity and Disaster Recovery Plan to determine the company has a documented business continuity/disaster recovery (BC/DR) plan in place.	No exceptions noted.
CC7.5.2	The company tests their incident response plan at least annually.	Inspected a sample incident report to determine that company tested their incident response plan at least annually.	No exceptions noted.
CC7.5.3	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's Incident Response Plan and the compliance platform to determine the company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC7.5.4	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the company's Incident Response Plan to determine the company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
		Inspected the incident listing to determine that the company's security and privacy incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CHANGE MANAGEMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1.1	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the company's Operations Security Policy to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, Inspected, and approved before being implemented in the production environment.	No exceptions noted.
		Inspected the change management documentation for a sample of changes to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
CC8.1.2	The company restricts access to migrate changes to production to authorized personnel.	Inspected the list of users with access to production to determine that the company restricts access to migrate changes to production to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CHANGE MANAGEMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC8.1.3	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's Operations Security and Secure Development policies to determine that the company had a formal SDLC methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.
CC8.1.4	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate high and critical vulnerabilities in accordance with SLAs.	Inspected the latest penetration testing report to determine the company's penetration testing is performed at least annually.	No exceptions noted.
		Per inquiry with management and inspection of the latest penetration testing report, there were no critical or high vulnerabilities identified; therefore, no testing was performed.	No testing performed. See footnote 1 above.
CC8.1.5	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Inspected the company's Configuration and Hardening Standards to determine the company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CHANGE MANAGEMENT			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC8.1.6	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the Operations Security Policy, Configuration and Hardening Standard to determine that the company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	No exceptions noted.
CC8.1.7	Host-based vulnerability scans are performed continuously. Critical and high vulnerabilities are tracked to remediation.	Inspected the vulnerability scan report from the compliance tool to determine that vulnerability scans were performed continuously on in-scope systems.	No exceptions noted.
		Inspected the remediation ticket/notes from the compliance tool to determine that the critical and high vulnerabilities are tracked to remediation.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK MITIGATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	Inspected the Business Continuity and Disaster Recovery plans to determine the company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	No exceptions noted.
CC9.1.2	The company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	Inspected company's cybersecurity insurance document to determine the company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	No exceptions noted.
CC9.1.3	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Per inquiry with management and inspection of the latest risk assessment performed in the compliance tool, the latest annual security risk assessment was performed in January 2025; therefore, no testing was performed.	No testing performed. See footnote 2 above.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK MITIGATION			
Control Number	**Controls**	**Detailed Tests of Controls**	**Test Results**
CC9.1.4	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the company's Risk Management Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected the written agreements for the vendors to determine they were in place and included confidentiality and privacy commitments.	No exceptions noted.
CC9.2.2	The company has a vendor management program in place. Components of this program include: - critical vendor inventory; - vendor's security and privacy requirements; and - review of critical vendors at least annually.	Inspected the company's Third-Party Management Policy to determine that the company had a vendor management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the vendor listing to determine that all the critical vendors inventory was in place.	No exceptions noted.
		Per inquiry with management and inspection of vendor reviews, the vendor reviews were conducted in January 2025; therefore, no testing was performed.	No testing performed. See footnote 2 above.