# Report on Stripe, Inc.'s Description of Its Stripe Payment Processing System and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security, Availability, Processing Integrity, and Confidentiality Throughout the Period October 1, 2021 to September 30, 2022

SOC 2® - SOC for Service Organizations: Trust Services Criteria – Integrated Type 2 Report Prepared in Accordance with the AICPA SSAE No. 18 and 21 and IAASB ISAE 3000 Standards

# Table of Contents

# Section 1

# Independent Service Auditor’s Report

# Independent Service Auditor's Report

To: Stripe, Inc. ("Stripe")

## Scope

We have examined Stripe's accompanying description in Section 3 titled "Stripe, Inc.'s Description of Its Stripe Payment Processing System Throughout the Period October 1, 2021 to September 30, 2022" (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* (AICPA, *Description Criteria*) (description criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that Stripe's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

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

Stripe uses subservice organizations to provide data center colocation services and security alerts. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Stripe, to achieve Stripe's service commitments and system requirements based on the applicable trust services criteria. The description presents Stripe's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Stripe's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The information included in Section 5, "Other Information Provided by Stripe, Inc. That Is Not Covered by the Service Auditor's Report," is presented by Stripe's management to provide additional information and is not a part of Stripe's description of its Stripe Payment Processing System made available to user entities during the period October 1, 2021 to September 30, 2022. Information included in Stripe's responses to testing exceptions has not been subjected to the procedures applied in the examination and, accordingly, we express no opinion on it.

## Service Organization's Responsibilities

Stripe is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Stripe's service commitments and system requirements were achieved. In Section 2, Stripe has provided the accompanying assertion titled "Assertion of Stripe, Inc. Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Stripe 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 (AICPA) and in accordance with International Standard on Assurance Engagements (ISAE) 3000 (Revised), *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board (IAASB). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of 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.

## Service Auditor's Independence and Quality Control

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA.

We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

## 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.

## Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in Section 4, "Trust Services Criteria, Related Controls and Tests of Controls Relevant to the Security, Availability, Processing Integrity, and Confidentiality Categories" of this report.

## Controls That Were Not Tested During the Period

Stripe's description of its Stripe Payment Processing System discusses its incident response and recovery plan, which includes the controls implemented and operated to respond to and recover from security incidents. Stripe's incident response and recovery plan includes procedures to help understand, contain, monitor, or eradicate a security incident; restore normal business operations in a timely manner with minimal, or no, business interruption or loss of data; and communicate with affected parties. However, during the period October 1, 2021 to September 30, 2022, Stripe did not experience a security incident that would warrant the operation of the response and recovery processes and controls.

Because the controls described above were not required to operate during the period, we did not test the operating effectiveness of those controls as evaluated using the following trust services criteria:

- 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.*
- CC7.5 - *The entity identifies, develops, and implements activities to recover from identified security incidents.*

## Opinion

In our opinion, in all material respects—

a. The description presents the Stripe Payment Processing System that was designed and implemented throughout the period October 1, 2021 to September 30, 2022, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that Stripe'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 organizations and user entities applied the complementary controls assumed in the design of Stripe's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that Stripe'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 Stripe'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 Stripe, user entities of the Stripe Payment Processing System during some or all of the period October 1, 2021 to September 30, 2022, business partners of Stripe subject to risks arising from interactions with the Stripe Payment Processing System, 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, subservice organizations, 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 these specified parties. If a report recipient is not a specified party as defined above and has obtained this report, or has access to it, use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Coalfire Controls, LLC as a result of such access. Further, Coalfire Controls, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Coalfire Controls LLC

Westminster, Colorado
December 9, 2022

# Section 2

# Assertion of Stripe, Inc. Management

## Assertion of Stripe, Inc. ("Stripe") Management

We have prepared the accompanying description in Section 3 titled "Stripe, Inc.'s Description of Its Stripe Payment Processing System Throughout the Period October 1, 2021 to September 30, 2022" (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* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the Stripe Payment Processing System that may be useful when assessing the risks arising from interactions with Stripe's system, particularly information about system controls that Stripe 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, availability, processing integrity, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Stripe uses subservice organizations for data center colocation services and security alerts. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Stripe, to achieve Stripe's service commitments and system requirements based on the applicable trust services criteria. The description presents Stripe's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Stripe's controls. The description does not disclose the actual controls at the subservice organizations.

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

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

a. The description presents the Stripe Payment Processing System that was designed and implemented throughout the period October 1, 2021 to September 30, 2022, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that Stripe'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 organizations and user entities applied the complementary controls assumed in the design of Stripe's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that Stripe'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 Stripe's controls operated effectively throughout that period.

d. Our description of the Stripe Payment Processing System discusses Stripe's incident response and recovery plan, which includes the controls implemented and operated to respond to and recover from security incidents. Stripe's incident response and recovery plan includes procedures to help understand, contain, monitor, or eradicate a security incident; restore normal business operations in a timely manner with minimal, or no, business interruption or loss of data; and communicate with affected parties. During the period October 1, 2021 to September 30, 2022, Stripe did not experience a security incident that would warrant the operation of the response and recovery processes and controls.

Stripe, Inc.

# Section 3

# Stripe, Inc.’s Description of Its Stripe Payment Processing System Throughout the Period October 1, 2021 to September 30, 2022

# Type of Services Provided

Since launching in 2011, Stripe, Inc. (“Stripe” or “the Company”) has provided software tools for building and running Internet businesses to organizations of all sizes. Stripe’s software tools are designed to help businesses securely accept payments, expand globally, and create new revenue streams.

## Overview of Stripe Services

Stripe offers developer-oriented payment processing technologies and services that can be integrated to accept online payments. An overview of Stripe’s offerings is provided in the subsections below.

### Integration Methods

Stripe has several tools that enable customers to integrate with and connect to the Stripe application programming interface (API). This helps customers build purchasing experiences through a single connection to Stripe rather than needing to integrate separately with different payment gateways, payment methods, or merchant services from banks. Each of the following integration methods enable the tokenization of sensitive data so that payment details are sent from the customer's browser directly to Stripe and do not touch the customer’s servers. Customers can build interfaces for consumers using their own style and workflow and utilize the security of Stripe’s infrastructure without having to handle consumers’ credit card information.

#### Stripe.js (v2 and v3)

Stripe.js v2 and v3 are JavaScript libraries used for collecting information including, but not limited to, credit card details, bank account details, and personally identifiable information. Built-in validators are included to check the format of credit card, CVV bank account, and routing numbers, as well as a credit card’s type and expiration date.

#### Checkout

Stripe Checkout (“Checkout”) is a modal opinionated payment form. The payment form is embeddable for desktop, tablet, and mobile devices to work within users’ sites. It allows customers to pay instantly without being redirected away to complete the transaction. It is built on top of Stripe.js v2.

#### Elements

Stripe Elements (“Elements”) is a set platform for building pre-built modular user interface (UI) components that users can leverage to build payments and other flows. It is built on top of Stripe.js v3 and includes Elements for iDeal and International Bank Account Number (IBAN) payments in addition to cards. Using Elements, payment forms can be customized to meet customer needs. Elements also makes collecting payment details more secure by generating a secure Inline Frame (IFrame) and isolating sensitive information from users’ sites.

#### Mobile Libraries

Stripe mobile libraries are software development kits (SDKs) that help enable customers to integrate their iOS or Android application with the Stripe API.

#### Stripe Connect

Stripe Connect (“Connect”) is a full-stack solution for businesses that need to process payments and pay out to multiple parties, known as platforms. Connect provides a powerful API and other tools that platforms need to make charges, as well as onboard, verify, and pay sellers, contractors, service providers, and other platform users. Connect is a combination of features designed to support a wide range of use cases,

including crowdfunding services, e-commerce platforms, marketplaces, on-demand services, booking platforms, and travel and event providers.

**Stripe Dashboard**

Stripe Dashboard ("Dashboard") is a tool that simplifies administrative control over a user's account and enables a user to access transaction information and reports. From within the Dashboard, users can view and manage incoming payments, customers, and refunds. They can also create subscriptions for customers, submit evidence for disputes, and administer partial or full refunds. All reporting can be accessed in CSV format for reconciliation purposes.

**Stripe Billing**

*Subscriptions*

Stripe Subscriptions is a set of tools that helps users build and scale businesses based on a recurring business model. Stripe Billing includes functionality that enables users to create subscriptions (via the Dashboard and API), in combination with features that enhance customer conversion (e.g., smart retries for unpaid invoices) and provide business intelligence.

*Invoicing*

Stripe Invoicing provides businesses with invoice management, payment collection and processing, and automated accounts receivable workflows (through the Dashboard and an API). Invoicing enables businesses to get paid in 135+ currencies, dynamically show optimized payment methods, and automate payment reconciliation and invoice collections.

**Stripe Sigma**

Stripe Sigma makes transactional data available via an interactive SQL environment in the Dashboard. Users can write queries that leverage various schema, allowing them to generate customized reports about payments, subscriptions, customers, payouts, and more. Users can also browse and use Stripe's collection of example queries to answer common questions and serve as a starting point for their own explorations.

Query results are displayed directly in the browser and can be downloaded in CSV format for use in users' own reporting tools or spreadsheet applications. Users can also automate reporting with scheduled queries that repeat regularly and send results via email or notifications via webhook events.

**Stripe Radar**

Stripe Radar ("Radar") is a proprietary suite of tools that helps users identify and prevent fraud and is powered by advanced machine learning algorithms. The system uses data across Stripe's network of businesses to evaluate the level of risk for each payment a user processes to help protect businesses from attempted fraudulent payments. Radar includes machine-learning algorithms, real-time insights about fraud for users, rules to block or flag payments for review by users, and granular information about why payments were blocked or flagged.

**Stripe Issuing**

Stripe Issuing ("Issuing") is an end-to-end platform to create and distribute physical and virtual cards. Using Issuing, users can create rules based on their business logic to manage which types of transactions are approved or declined on the cards. Issuing is currently certified with Visa as an issuer processor and is built on the same core payments acceptance platform.

**Stripe Corporate Card**

Stripe Corporate Card ("Corporate Card") is a commercial charge card offered via a partnership between Stripe and Celtic Bank and is built on Issuing. Stripe markets the charge card to startups and merchant payment processing customers. Celtic Bank evaluates the applicants, offers the credit, and issues the

charge card. Stripe supports the partnership by acting as a servicer and collections agent for the card program.

**Stripe Capital**
Stripe Capital ("Capital") is Stripe's financing program, and currently offers access to merchant cash advances and commercial term loans. Term loans are provided by Celtic Bank, in partnership with Stripe. Similar to the Corporate Card partnership, Stripe acts as the servicer and collections agent for the term loans. Merchant cash advances are offered directly by Stripe. Participants in the program fulfill their payment obligations by having a percentage of the participant's daily payment processing proceeds withheld by Stripe.

**Stripe Terminal**
Stripe Terminal ("Terminal") is an in-person payments solution that provides global reach, large-scale fleet management, deep customization, flexible integration modes, and multiple low-cost reader hardware options for software-as-a-service (SaaS) platforms and modern internet-first retailers.

The system description in this section of the report details the Stripe Payment Processing System. Any other Stripe services are not within the scope of this report. The accompanying description includes only the policies, procedures, and control activities at Stripe and does not include the policies, procedures, and control activities at any subservice organizations (see below for further discussion of subservice organizations). Infrastructure that sits outside of Stripe (e.g., Visa, MasterCard, other financial partners, and payment methods) are out of scope of this report, as they are not run or managed by Stripe.

# Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of the Stripe Payment Processing System. Commitments are communicated in written individualized agreements, standardized contracts, and service-level agreements (SLAs).

System requirements are specifications regarding how the Stripe Payment Processing System should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures.

The Company's principal service commitments and system requirements related to the Stripe Payment Processing System include the following:

| Trust Services Category | Service Commitments | System Requirements |
|---|---|---|
| **Security** | • Stripe will maintain administrative, organizational, and technical controls to protect customer data from unauthorized access, destruction, accidental loss, unauthorized modification, alteration or misuse. | • Employee provisioning and deprovisioning standards<br>• User access reviews<br>• Logical access controls<br>• Risk assessment standards<br>• Change management controls |

| Trust Services Category | Service Commitments | System Requirements |
|---|---|---|
| **Availability** | • Stripe will operate and maintain measures designed to maintain system availability.<br>• Stripe will provide 99.9% system uptime/availability. | • Incident handling policies and procedures<br>• Incident response plan<br>• Business continuity and disaster recovery plan |
| **Confidentiality** | • Stripe will protect and keep confidential customer's confidential information.<br>• Stripe will not disclose customers' confidential information to any third party without the customer's consent.<br>• Stripe will only use customer data for the purposes of providing the services. | • Data input, output, and processing controls.<br>• Encryption standards for data at rest and in transit |
| **Processing Integrity** | • Stripe will operate and maintain measures designed to maintain the integrity of data.<br>• Stripe will make reasonable efforts to ensure a level of security appropriate to the risk associated with the processing of data. | • Financial Reconciliations<br>• System and transaction monitoring controls |

# The Components of the System Used to Provide the Services

The boundaries of the Stripe Payment Processing System 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 Stripe Payment Processing System.

The components that directly support the services provided to customers are described in the subsections below.

## Infrastructure

Stripe utilizes AWS and Equinix Data Centers (Equinix) to provide the resources to host the Stripe Payment Processing System. The Company leverages the experience and resources of AWS and Equinix to scale quickly and securely as necessary to meet current and future demand. However, the Company is responsible for designing and configuring the Stripe Payment Processing architecture within AWS and Equinix to ensure the availability, security, and resiliency requirements are met.

The in-scope hosted infrastructure also consists of multiple supporting tools, as shown in the table below:

| Infrastructure | | | |
|---|---|---|---|
| **Production Tool** | **Business Function** | **Operating System** | **Hosted Location** |
| Databases | Customer Data Storage | MongoDB | AWS and Equinix |
| Firewalls | Network Protection | Juniper | AWS and Equinix |

| Infrastructure | | | |
|---|---|---|---|
| **Production Tool** | **Business Function** | **Operating System** | **Hosted Location** |
| Switches | Network Traffic | Juniper | AWS and Equinix |
| Computers | Productivity | Linux | N/A |

## Software

Software consists of the programs and software that support the Stripe Payment Processing System (operating systems [OSs], middleware, and utilities). The list of software and ancillary software used to build, support, secure, maintain, and monitor the Stripe Payment Processing System include the following applications, as shown in the table below:

| Software | |
|---|---|
| **Production Application** | **Business Function** |
| SignalFX, Sentry, PagerDuty, Splunk | Application monitoring |
| AWS Elastic Block Storage (EBS) | Backup and replication |
| Splunk, AWS CloudTrail | Security information and event management (SIEM), logging system |
| SignalFX, Splunk, osquery | Infrastructure monitoring |
| Ruby Bundler (Scan) & Puppet (Deployments) | Patch management |
| OSSEC | File integrity monitoring, intrusion detection |
| Uptycs | Antivirus |
| JIRA | Help desk, ticketing system |

## People

The Company develops, manages, and secures the Stripe Payment Processing System via separate departments. The responsibilities of these departments are defined in the following table:

| People | |
|---|---|
| **Group/Role Name** | **Function** |
| Executive Management | Responsible for overseeing company-wide activities, establishing and accomplishing goals, and managing objectives. |
| Engineering (e.g., Payments, Security) | Responsible for operational efficiencies, development, testing and implementation of changes, incident response, and overall security at Stripe. |
| Compliance and Legal | Responsible for facilitating compliance across various regulatory bodies and requirements (e.g., financial, payment, SOC, Anti-Money Laundering/Counter Financing Terrorism (AML/CFT). |
| IT | Responsible for supporting and monitoring internal Stripe systems, maintaining a physical inventory of hardware, and identifying, addressing, and supporting technical issues. |

| People | |
|---|---|
| **Group/Role Name** | **Function** |
| Human Resources (HR) | Responsible for facilitating day-to-day activities, including onboarding and offboarding relevant personnel to the corporate environment, workplace health, discipline, security awareness training, and performance evaluations. |

## Procedures

Procedures include the automated and manual procedures involved in the operation of the Stripe Payment Processing System. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, information technology (IT), and HR. These procedures are drafted in alignment with the overall information security policies and are updated and approved as necessary for changes in the business, but no less than annually. The following table details the procedures as they relate to the operation of Stripe Payment Processing System:

| Procedures | |
|---|---|
| **Procedure** | **Description** |
| Incident Management | Stripe maintains an incident management process that: (a) Identifies root cause to prevent future incidents; (b) Posts incident root-cause analysis; (c) Develops and implements future preventative measures and controls through appropriate control procedures; and (d) Retains known occurrences and resolutions that allow for reactive incident management. |
| Backup and Offsite Storage | Stripe maintains a backup and offsite storage process that backs up all of Stripe's core databases hourly and replicates those backup snapshots to a different geographic region. Real-time monitoring and alerting ensure that the backup process is successful. Stripe regularly tests and restores backups weekly to prove their validity. |
| Information Security | Stripe maintains an internal access control system for data, servers, and internal procedures. The security team has procedures for maintaining and updating access control systems.<br>Every quarter, Stripe performs a recertification of the permissions granted to users. Stripe validates that all users have appropriate assigned permission that are still required based on job title and responsibilities. Inappropriate access is flagged and immediately removed. |
| Change Management and System Development | Stripe maintains documented policies and procedures for making changes to Stripe's software and infrastructure. These policies dictate how changes are tested, reviewed, and approved and, for individual services, prescribe what specific metrics should be monitored as a change is being deployed. They also ensure changes are communicated before being deployed.<br>Engineers develop in a segregated environment that is separate from the production environment. Engineers submit changes to a code review process and select a reviewer with appropriate context. Tests are run automatically as part of the code review pipeline. After the tests have succeeded and the reviewer has approved the change, the engineer can then deploy the change, typically in a staged rollout.<br>Engineers closely monitor deployments and follow documented rollback procedures to restore the previous state if a problem is detected. Deploys are triggered multiple times each workday, and (outside of an emergency) are avoided outside of working hours. |

## Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. Through the application programming interface (API), the customer or end-user defines and controls the data they load into and store in the Stripe Payment Processing System production network. Once stored in the environment, the data is accessed remotely from customer systems via the Internet.

Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts.

The Company has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Encryption is enabled for data stores housing sensitive customer data.

# System Incidents

There were no identified significant system incidents that (a) were the result of controls that were not suitably designed or operating effectively to achieve one or more of the service commitments and system requirements or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements from October 1, 2021 to September 30, 2022.

# The Applicable Trust Services Criteria and Related Controls

## Applicable Trust Services Criteria

The Trust Services Categories that are in scope for the purposes of this report are as follows:

- *Security*: Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, processing integrity, or confidentiality of information or systems and affect the entity's ability to meet its objectives.
- *Availability:* Information and systems are available for operation and use to meet the entity's objectives.
- *Processing Integrity:* System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.
- *Confidentiality*: Information designated as confidential is protected to meet the entity's objectives.

Many of the criteria used to evaluate a system are shared amongst all in-scope categories; for example, the criteria related to risk assessment apply to the security, availability, processing integrity, and confidentiality categories. As a result, the criteria for the security, availability, processing integrity, and confidentiality categories are organized into (a) the criteria that are applicable to all categories (common criteria) and (b) criteria applicable only to a single category. The common criteria constitute the complete set of criteria for the security category. For the categories of availability, processing integrity, and confidentiality, a complete set of criteria is comprised of all the common criteria and all the criteria applicable to the category being reported on.

The common criteria are organized as follows:

1. *Control environment:* The criteria relevant to how the entity is structured and the processes the entity has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values, qualifications of personnel, and the environment in which they function.
2. *Communication and information:* The criteria relevant to how the entity communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.
3. *Risk assessment:* The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.
4. *Monitoring activities:* The criteria relevant to how the entity monitors the system, including the suitability and design and operating effectiveness of the controls, and acts to address deficiencies identified.
5. *Control activities:* The criteria relevant to the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out.
6. *Logical and physical access controls:* The criteria relevant to how the entity restricts logical and physical access, provides and removes that access, and prevents unauthorized access.
7. *System operations:* The criteria relevant to how the entity manages the operation of system(s) and detects and mitigates processing deviations, including logical and physical security deviations.
8. *Change management:* The criteria relevant to how the entity identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
9. *Risk mitigation:* The criteria relevant to how the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

This report is focused solely on the security, availability, processing integrity, and confidentiality categories. The Company has elected to exclude the privacy category.

# Control Environment

## Integrity and Ethical Values

The control environment is the foundation for all other areas of internal control. As such, the control environment of the Company sets the tone for the organization and influences the control consciousness and discipline of employees. Management emphasizes the importance of controls and ethical behavior throughout the organization.

## Board of Directors

The Company has a board of directors that meets annually and is consulted and involved in all significant business decisions.

### Organizational Structure

The Company has established appropriate lines of reporting, which facilitate the flow of information to the appropriate people in a timely manner. Roles and responsibilities are segregated based on functional requirements. The Company has an organization chart that sets forth the Company's lines of reporting, which is updated as necessary.

Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective internal control.

### Human Resources

The Company maintains formal hiring policies and procedures. The Company maintains current job descriptions and roles for key personnel. The Company also has a process to ensure that the correct personnel are responsible for key processes and technology.

## Communication and Information

The Company has implemented various methods of communication to ensure that all employees understand their individual roles and responsibilities. These methods include periodic training programs for educating employees on internal developments, industry trends, and organizational development activities.

Communication is the continual, iterative process of providing, sharing, and obtaining necessary information. Internal communication is the means by which information is disseminated throughout the organization, flowing up, down, and across the Company. It enables personnel to receive a clear message from senior management that control responsibilities must be taken seriously. External communication is twofold: it enables inbound communication of relevant external information and provides information to external parties in response to requirements and expectations.

The Company obtains or generates and uses relevant, quality information to support the functioning of internal control. The Company maintains data flow diagrams, flowcharts, narratives, and procedural documentation to allow easy identification of data sources, responsible personnel, and other relevant information. The Company has methods in place to help ensure information systems maintain and produce information that is timely, current, accurate, and complete.

## Risk Assessment and Mitigation

The Company has a risk assessment process to identify and manage risks that could affect the Company's ability to provide reliable services to its clients. This process requires management to identify significant risks in their areas of responsibility and corresponding measures to address those risks. In designing its controls, the Company has considered the risks that could prevent it from effectively achieving its objectives.

Key risks that the Company has identified and is focused on controlling include but are not limited to:

- Fraud and Financial Crimes
- Regulatory Compliance
- Data Security
- Reliability
- Partnerships
- Organizational Design

Risk assessment is a dynamic and iterative process for identifying and assessing risks to the achievement of objectives. Management specifies objectives with enough clarity to identify and analyze risks to those objectives, the Company identifies risks to the achievement of its objectives across the entity, and the Company analyzes risks as a basis for determining how the risks should be managed. Appropriate levels of management are involved in the risk assessment process.

The risk identification and control effectiveness assessment includes a consideration of both internal and external factors and their impact on the achievement of the objectives and the effectiveness of existing controls. Identified risks are analyzed through a process that includes estimating the potential significance of the risk.

The Company considers the potential for fraud in assessing risks to the achievement of objectives. The assessment of fraud risk considers fraudulent reporting, possible loss of assets or data, and corruption resulting from the various ways that fraud and misconduct can occur. It also considers opportunities for unauthorized acquisition, use, or disposal of assets; altering of the entity's reporting records; or committing other inappropriate acts and how management and other personnel might engage in or undertake inappropriate actions.

The risk assessment process includes identification and assessment of changes that could significantly impact the effectiveness of existing controls. Risk identification involves a broad consultative process with knowledgeable stakeholders to ensure the completeness and materiality of the overall risk taxonomy in regard to the Company's objectives and relevant business environment factors.

Where appropriate, the Company uses the risk assessment process to help inform treatment strategies for the risks that have been identified.

## Monitoring

Members of the Company regularly participate in security and risk-based groups to monitor the impact of emerging technologies. Additionally, the Company holds weekly team meetings to discuss current projects and any potential security concerns.

Ongoing evaluations, built into business processes at different levels of the Company, provide timely information. Separate evaluations, conducted periodically, vary in scope and frequency depending on assessment of risks, effectiveness of ongoing evaluations, and other management considerations. Findings are evaluated against criteria established by senior management and the board of directors, and deficiencies are communicated to management and the board of directors as appropriate.

The Company selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. The Company's management and supervisory personnel monitor the quality of internal control performance as a routine part of their activities.

The Company 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.

The Company monitors the controls of subservice organizations by periodically obtaining and reviewing SOC reports (or, if not available, other security documentation). In addition, through its daily operational activities, Company management monitors the services performed by the subservice organizations to ensure that operations and controls expected to be implemented at the subservice organizations are functioning effectively. Management also holds periodic calls with the subservice organizations that have access to Stripe data (as opposed to subservice organizations that perform operations without sensitive

data) to monitor compliance with their SLAs, stay informed of changes planned at the hosting facilities, and relay any issues or concerns to subservice organization management.

## Control Activities

The Company's control activities are defined through its established policies and procedures. Policies are dictated through management or board member statements of what should be done to effect control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. Policies serve as the basis for procedures. Control activities are deployed through policies that establish what is expected and procedures that put policies into action.

### Logical Access

Access to in-scope system components requires a documented access request form and group owner approval prior to access being provisioned. A termination checklist is completed, and access is revoked for employees within 24 hours as part of the termination process.

The following in-scope system components require unique username and authorized SSH keys prior to authenticating users:

- Network
- Application (admin.stripe.com)
- Operating system (OS)
- Data Stores
- AWS Management Console
- Firewalls
- Log data

Privileged access to the following in-scope system components is restricted to authorized users with a business need:

- Network
- Application (admin.stripe.com)
- OS
- Data Stores
- AWS Management Console
- Firewalls
- Log data

AWS security groups are used and configured to prevent unauthorized access. Infrastructure and applications supporting the service are patched in a timely manner to help ensure that infrastructure and applications supporting the service are hardened against security threats. The Company has deployed Transport Layer Security (TLS) for transmission of confidential or sensitive information over public networks. The Company has also deployed anti-malware technology for environments commonly susceptible to malicious attack and updates the definitions routinely.

## System Operations

All system incidents are logged, tracked, and communicated to affected parties by management until resolved. Management tests the incident response plan at least annually. Penetration testing is performed at least annually. A remediation plan is developed, and changes are implemented to remediate all critical and high vulnerabilities at a minimum. Logging and monitoring tools are used to identify errors and issues with the Stripe management dashboard and to monitor uptime. The tools are configured to send alerts when issues occur. A vendor risk assessment is performed annually for all vendors that have access to confidential data or impact the security of the system. A configuration management system is in place, monitors for configuration changes, and alerts administrators on what changes occurred.

## Change Management

Formally documented change management procedures are in place to govern the modification and maintenance of production systems. The Company has adopted a formal systems development life cycle (SDLC) methodology that governs the development, acquisition, implementation, and maintenance of computerized information systems and related technology requirements. Stripe's software and infrastructure change management process requires that change requests are authorized, formally documented, tested, peer reviewed by an appropriate owner, and approved prior to migration to production.

## Availability

The availability category refers to the accessibility of the system or services as committed by the Company's service agreements. The availability of the Stripe Payment Processing System is dependent on many aspects of the Company's operations. The risks that would prevent the Company from meeting its availability commitments and requirements are diverse. Availability includes consideration of risks during normal business operations, risks during routine failure of elements of the system, and risks related to the continuity of business operations during a natural or man-made disaster.

The Company has designed its controls to address the following availability risks:

- Insufficient processing capacity
- Insufficient Internet response time
- Loss of processing capability due to a power outage
- Loss of communication with user entities due to a break in telecommunication services
- Loss of key processing equipment, facilities, or personnel due to a natural disaster

Availability risks are addressed through the use and testing of various monitoring tools, replication setup, and backup and disaster recovery plans and procedures.

In evaluating the suitability of the design of availability controls, the Company considers the likely causes of data loss, the commitments and requirements related to availability, the timeliness of backup procedures, the reliability of the backup process, and the ability to restore backed up data. In evaluating the design of data availability controls, the Company considers that most data loss does not result from disasters but, rather, from routine processing errors and failures of system elements.

## Processing Integrity

Processing integrity refers to the completeness, validity, accuracy, timeliness, and authorization of system processing. Processing integrity addresses whether the Stripe Payment Processing System achieves the purpose for which it exists and whether it performs its intended function, which is to process customer transactions in an unimpaired manner, free from unauthorized or inadvertent manipulation. The processing

integrity criteria address input, processing, output, and storage of data within the Stripe Payment Processing System.

The Company has designed its controls to address the following processing integrity risks:

- Current processing capacity is not sufficient to meet processing requirements, resulting in processing errors
- Inputs are captured incorrectly
- Inputs are not captured in a timely manner
- Data is lost during processing
- Data is inaccurately modified during processing
- Processing is not complete within required timeframe
- System output in not accurate
- System output is provided to unauthorized recipients

### Confidentiality

Confidentiality refers to the protection of customer information as committed by the Company's service agreements. The confidentiality of the Stripe Payment Processing System is dependent on many aspects of the Company's operations. The risks that would prevent the Company from meeting its confidentiality commitments and requirements are diverse. The Company has designed its controls to address both internal and external confidentiality risks specifically related to protection from improper use and disclosure (including monitoring of vendor services), as well as the proper retention and disposal of confidential customer information.

Confidentiality risks are addressed through policies regarding the use, retention, and disposal of confidential data, data classification policies and procedures, network segmentation, confidentiality and information sharing agreements, remote access and transmission restrictions, and vendor risk assessments.

In evaluating the suitability of the design of confidentiality controls, the Company considers the likely causes of improper disclosure or handling of confidential information, and the commitments and requirements related to confidentiality.

# Complementary User Entity Controls (CUECs)

The Company's controls related to Stripe Payment Processing System cover only a portion of overall internal control for each user entity of Stripe Payment Processing System. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by the Company. Therefore, each user entity's internal control should be evaluated in conjunction with the Company's controls and the related tests and results described in Section 4 of this report, taking into account the related CUECs identified for the specific criterion. In order for user entities to rely on the controls reported herein, each user entity must evaluate its own internal control to determine whether the identified CUECs have been implemented and are operating effectively.

The CUECs presented should not be regarded as a comprehensive list of all controls that should be employed by user entities. Management of user entities is responsible for the following:

| Criteria | Complementary User Entity Controls |
|---|---|
| CC2.1 | • User entities have policies and procedures to report any material changes to their overall control environment that may adversely affect services being performed by the Company according to contractually specified time frames.<br>• Controls to provide reasonable assurance that the Company is notified of changes in:<br>– User entity vendor security requirements<br>– The authorized users list |
| CC2.3 | • It is the responsibility of the user entity to have policies and procedures to:<br>– Inform their employees and users that their information or data is being used and stored by the Company.<br>– Determine how to file inquiries, complaints, and disputes to be passed on to the Company. |
| CC6.1 | • User entities grant access to the Company's system to authorized and trained personnel. |
| CC6.4 | • User entities deploy physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity. |
| CC6.6 | • Controls to provide reasonable assurance that policies and procedures are deployed over user IDs and passwords that are used to access services provided by the Company. |

# Subservice Organizations and Complementary Subservice Organization Controls (CSOCs)

The Company uses AWS and Equinix as subservice organizations for data center colocation services and security alerts. Stripe's controls related to the Stripe Payment Processing System cover only a portion of the overall internal control for each user entity of the Stripe Payment Processing System. The description does not extend to the colocation services for IT infrastructure provided by the subservice organizations. Section 4 of this report and the description of the system only cover the Trust Services Criteria and related controls of the Company and exclude the related controls of AWS and Equinix.

Although the subservice organizations have been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organizations. CSOCs are expected to be in place at AWS and Equinix related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. AWS and Equinix physical security controls should mitigate the risk of fires, power loss, climate, and temperature variabilities.

Company management receives and reviews AWS and Equinix SOC reports annually. In addition, through its operational activities, Company management monitors the services performed by AWS and Equinix to determine whether operations and controls expected to be implemented at the subservice organizations are functioning effectively. Management also communicates with the subservice organizations to monitor compliance with service agreements, stay informed of changes planned at the hosting facility, and relay any issues or concerns to AWS and Equinix management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to the Stripe Payment Processing System to be achieved solely by Stripe. Therefore, each user entity's internal

control must be evaluated in conjunction with Stripe's controls and related tests and results described in Section 4 of this report, accounting for the related CSOCs expected to be implemented at the subservice organizations as described below.

| Criteria | Complementary Subservice Organization Controls |
|---|---|
| CC6.1 | • AWS and Equinix are responsible for ensuring data stores are encrypted at rest. |
| CC6.4 | • AWS and Equinix are responsible for restricting data center access to authorized personnel.<br>• AWS and Equinix are responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel. |
| CC6.5<br>CC6.7 | • AWS and Equinix are responsible for securely decommissioning and physically destroying production assets in its control. |
| A1.2<br>CC7.2 | • AWS and Equinix are responsible for the installation of fire suppression and detection, and environmental monitoring systems at the data centers.<br>• AWS and Equinix are responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS).<br>• AWS and Equinix are responsible for overseeing the regular maintenance of environmental protections at data centers. |

# Specific Criteria Not Relevant to the System

There were no specific security, availability, processing integrity, or confidentiality Trust Services Criteria as set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria) that were not relevant to the system as presented in this report.

# Significant Changes to the System

There were no changes that are likely to affect report users' understanding of how the Stripe Payment Processing System is used to provide the service from October 1, 2021 to September 30, 2022.

# Report Use

The description does not omit or distort information relevant to the Stripe Payment Processing System while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to their own particular needs.

# Section 4

# Trust Services Criteria, Related Controls and Tests of Controls Relevant to the Security, Availability, Processing Integrity, and Confidentiality Categories

## Control Environment Elements

The control environment represents the collective effect of various elements in establishing, enhancing or mitigating the effectiveness of specific controls. The control environment elements as described in the description of the system include, but are not limited to, the Code of Conduct, Policies and Procedures and Human Resources.

Our tests of the control environment included the following procedures, to the extent we considered necessary; (a) an inspection of Stripe's organizational structure including segregation of functional responsibilities and policies and procedures; (b) inquiries with management, operations, administrative and other personnel who are responsible for developing, ensuring adherence to and applying controls; (c) observations of personnel in the performance of their assigned duties; and (d) inspection of documents and records pertaining to controls.

## Description of Tests Performed by Coalfire Controls, LLC

Our tests of operating effectiveness of controls included such tests as were considered necessary in the circumstances to evaluate whether those controls, and the extent of compliance with them, were sufficient to provide reasonable, but not absolute, assurance that the trust services security, availability, processing integrity, and confidentiality categories and criteria were achieved throughout the period October 1, 2021 to September 30, 2022. In selecting particular tests of the operating effectiveness of the controls, we considered (i) the nature of the controls being tested; (ii) the types of available evidential matter; (iii) the nature of the criteria to be achieved; (iv) the assessed level of control risk; and (v) the expected efficiency and effectiveness of the test. Such tests were used to evaluate fairness of the presentation of the description of the Stripe Payment Processing System and to evaluate the operating effectiveness of specified controls.

Additionally, observation and inspection procedures were performed as it relates to system generated reports, queries, and listings within management's description of the system to assess the completeness and accuracy (reliability) of the information utilized in the performance of our testing of the control activities.

# Trust Services Criteria, Related Controls and Tests of Controls Relevant to the Security, Availability, Processing Integrity, and Confidentiality Categories

| Control Environment | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| **CC1.1** | The entity demonstrates a commitment to integrity and ethical values. | | |
| | Upon hire, employees must acknowledge an employee handbook that describes their responsibilities and expected behavior regarding data and information system usage. | Inspected the employee handbook to determine that it described employee responsibilities and expected behavior regarding data and information system usage. | No exceptions noted. |
| | | Inspected acknowledgements for a sample of new hires to determine that new hires acknowledged that they had read and agreed to the employee handbook upon hire. | Exceptions noted. 2 out of a sample of 44 employees did not acknowledge that they had read and agreed to the employee handbook upon hire. |
| | Employees are required to sign a confidentiality agreement upon hire. This agreement prohibits the disclosure of information and other data to which the employee has been granted access. | Inspected the confidentiality agreement to determine that it prohibited the disclosure of information and other data to which the employee had been granted access. | No exceptions noted. |
| | | Inspected signed confidentiality agreements for a sample of new hires to determine that new hires were provided and signed the agreement upon hire. | No exceptions noted. |

| Control Environment | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | Managers are required to complete performance appraisals for direct reports at least annually. | Inspected performance appraisal documentation for a sample of employees to determine that performance appraisals were completed by management during the period. | No exceptions noted. |
| | Employees and contractors who violate the code of conduct are subject to disciplinary actions documented in a formalized sanctions policy. | Inspected the employee handbook to determine that the Company had documented disciplinary actions in a formalized sanctions policy for employees and contractors who violated the code of conduct. | No exceptions noted. |
| | New personnel offered employment are subject to background checks upon hire. | Inspected background check completion evidence for a sample of new hires to determine that new hires were subject to background checks upon hire. | Exceptions noted. 5 out of a sample of 44 new hires did not have their background checks initiated within 30 days of hire. |
| **CC1.2** | The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control. | | |
| | The board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the Company. | Inspected the board of directors meeting minutes to determine that the board met during the period and maintained formal meeting minutes. | No exceptions noted. |
| | | Inspected a listing of the board of directors to determine that the board included directors that were independent of the Company. | No exceptions noted. |
| | The audit committee has a documented charter that outlines its oversight responsibilities relative to internal control. | Inspected the audit committee charter to determine that oversight responsibilities of the audit committee relative to internal control were documented. | No exceptions noted. |

| Control Environment | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| **CC1.3** | Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. | | |
| | An organization chart is documented and defines the organizational structure and reporting lines. | Inspected the organization chart to determine that it was documented and defined the organizational structure and reporting lines. | No exceptions noted. |
| | The audit committee has a documented charter that outlines its oversight responsibilities relative to internal control. | Inspected the audit committee charter to determine that oversight responsibilities of the audit committee relative to internal control were documented. | No exceptions noted. |
| | Management has established defined roles and responsibilities to oversee the implementation of the security and control environment and report any issues to the board of directors. | Inspected security policies to determine that management had established defined roles and responsibilities to oversee the implementation of the security and control environment and report issues to the board of directors. | No exceptions noted. |
| | Job descriptions (including roles and responsibilities) are documented for employees supporting the service and include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system. | Inspected job descriptions for a sample of employees supporting the service to determine that job descriptions were formally documented and included authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system. | No exceptions noted. |

| Control Environment | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| **CC1.4** | The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. | | |
| | Employees complete security awareness training upon hire and annually thereafter. | Inspected training completion evidence for a sample of new hires to determine that security awareness training was completed upon hire. | No exceptions noted. |
| | | Inspected training completion evidence for a sample of employees to determine that security awareness training was completed during the period. | No exceptions noted. |
| | Job descriptions (including roles and responsibilities) are documented for employees supporting the service and include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system. | Inspected job descriptions for a sample of employees supporting the service to determine that job descriptions were formally documented and included authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system. | No exceptions noted. |
| | Managers are required to complete performance appraisals for direct reports at least annually. | Inspected performance appraisal documentation for a sample of employees to determine that performance appraisals were completed by management during the period. | No exceptions noted. |
| **CC1.5** | The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives. | | |
| | Managers are required to complete performance appraisals for direct reports at least annually. | Inspected performance appraisal documentation for a sample of employees to determine that performance appraisals were completed by management during the period. | No exceptions noted. |

| Control Environment | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | Upon hire, employees must acknowledge an employee handbook that describes their responsibilities and expected behavior regarding data and information system usage. | Inspected the employee handbook to determine that it described employee responsibilities and expected behavior regarding data and information system usage. | No exceptions noted. |
| | | Inspected acknowledgements for a sample of new hires to determine that new hires acknowledged that they had read and agreed to the employee handbook upon hire. | Exceptions noted. 2 out of a sample of 44 employees did not acknowledge that they had read and agreed to the employee handbook upon hire. |
| | Employees and contractors who violate the code of conduct are subject to disciplinary actions documented in a formalized sanctions policy. | Inspected the employee handbook to determine that the Company had documented disciplinary actions in a formalized sanctions policy for employees and contractors who violated the code of conduct. | No exceptions noted. |
| | Job descriptions (including roles and responsibilities) are documented for employees supporting the service and include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system. | Inspected job descriptions for a sample of employees supporting the service to determine that job descriptions were formally documented and included authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system. | No exceptions noted. |

| Communication and Information | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| **CC2.1** | The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. | | |
| | Control self-assessments are performed by management at least annually to gain assurance that controls related to the in-scope Trust Services Categories are in place and operating effectively. Corrective actions are taken based on relevant findings and tracked to resolution. | Inspected control self-assessment documentation to determine that control self-assessments were performed by management during the period and corrective actions were taken based on relevant findings and tracked to resolution. | No exceptions noted. |
| | Internal and external network vulnerability scans are performed quarterly to identify, quantify, and prioritize vulnerabilities. | Inspected internal and external network vulnerability scans for a sample of quarters to determine that internal and external network vulnerability scans were performed to identify, quantify, and prioritize vulnerabilities. | No exceptions noted. |
| | A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during quarterly internal and external network vulnerability scans.<br><br>The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No critical or high vulnerabilities were discovered during the internal and external vulnerability scans. | Inquired of management and inspected vulnerability scans to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether a remediation plan was developed and changes were implemented to remediate all critical and high vulnerabilities identified during quarterly external network vulnerability scans. | Not tested. No critical or high vulnerabilities were discovered during the internal and external vulnerability scans. |
| | A log management tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its security objectives. | Inspected the log management tool to determine that logs were analyzed for trends that may have had a potential impact on the Company's ability to achieve its security objectives. | No exceptions noted. |

| Communication and Information | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | The security owner subscribes to industry security bulletins and email alerts and uses them to monitor the impact of emerging technologies and security to the production systems. | Inspected example security bulletins and email alerts subscribed to by the security owner to determine that the security owner subscribed to industry security bulletins and email alerts and used them to monitor the impact of emerging technologies and security to the production systems. | No exceptions noted. |
| | A file integrity monitoring (FIM) tool is used to notify system administrators of potential unauthorized changes to the production system. | Inspected alert configuration settings and example alerts to determine that the Company utilized a FIM tool that notified system administrators of potential unauthorized changes to the production systems. | No exceptions noted. |
| **CC2.2** | The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. | | |
| | Employees complete security awareness training upon hire and annually thereafter. | Inspected training completion evidence for a sample of new hires to determine that security awareness training was completed upon hire. | No exceptions noted. |
| | | Inspected training completion evidence for a sample of employees to determine that security awareness training was completed during the period. | No exceptions noted. |
| | Management has established defined roles and responsibilities to oversee the implementation of the security and control environment and report any issues to the board of directors. | Inspected security policies to determine that management had established defined roles and responsibilities to oversee the implementation of the security and control environment and report issues to the board of directors. | No exceptions noted. |

| Communication and Information | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | Job descriptions (including roles and responsibilities) are documented for employees supporting the service and include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system. | Inspected job descriptions for a sample of employees supporting the service to determine that job descriptions were formally documented and included authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system. | No exceptions noted. |
| | System changes are communicated to authorized internal users. | Inspected tickets for a sample of system changes to determine that system change information was communicated to authorized internal users. | No exceptions noted. |
| | A formalized whistleblower policy is established and an anonymous communication channel is available for employees to report potential security issues or fraud concerns. | Inspected the formal whistleblower policy to determine that a formalized whistleblower policy was established and an anonymous communication channel was available to all employees to report potential security issues or fraud concerns. | No exceptions noted. |
| **CC2.3** | The entity communicates with external parties regarding matters affecting the functioning of internal control. | | |
| | Customer agreements, contracts, and service-level agreements (SLAs) include the communication of the Company's commitments to its customers. | Inspected template customer agreements, contracts, and SLAs to determine that the Company's commitments were communicated to customers. | No exceptions noted. |
| | Formal information sharing agreements are in place with critical vendors. These agreements include confidentiality commitments applicable to that entity. | Inspected contracts for a sample of critical vendors to determine that a formal information sharing agreement was in place and included applicable confidentiality agreements. | No exceptions noted. |
| | Customers are notified of critical changes that may affect their processing. | Inspected release notes for a sample of critical changes to determine that the Company communicated critical changes to customers that could have affected their processing. | No exceptions noted. |

| Communication and Information | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | An external-facing support system is in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel. | Inspected the customer reporting portal to determine that an external-facing support system was in place that allowed users to report system information on failures, incidents, concerns, and other complaints to the appropriate personnel. | No exceptions noted. |
| | Guidelines and technical support resources relating to system operations are provided on the Company's website. | Inspected evidence of guidelines and resources posted on the Company's website to determine that guidelines and technical support resources related to system operations were provided. | No exceptions noted. |

| Risk Assessment | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| **CC3.1** | The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. | | |
| | The Company specifies its objectives in its annual risk assessment to enable the identification and assessment of risk related to the objectives. | Inspected the risk assessment to determine that the Company specified its objectives in its annual risk assessment to enable the identification and assessment of risk related to the objectives. | No exceptions noted. |
| | A documented risk management program is 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. The program considers the following:<br>- Compliance objectives<br>- External laws and regulations<br>- Tolerance for risk<br>- Establishment of sub-objectives to support primary objectives | Inspected the risk management policy to determine that a program had been established around the identification of potential threats, rating the significance of the risks associated with the identified threats, mitigation strategies for those risks, and that the program considered the following:<br>- Compliance objectives<br>- External laws and regulations<br>- Tolerance for risk<br>- Establishment of sub-objectives to support primary objectives | No exceptions noted. |
| **CC3.2** | 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. | | |
| | A documented risk management program is 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. The program considers the following:<br>- Compliance objectives<br>- External laws and regulations<br>- Tolerance for risk<br>- Establishment of sub-objectives to support primary objectives | Inspected the risk management policy to determine that a program had been established around the identification of potential threats, rating the significance of the risks associated with the identified threats, mitigation strategies for those risks, and that the program considered the following:<br>- Compliance objectives<br>- External laws and regulations<br>- Tolerance for risk<br>- Establishment of sub-objectives to support primary objectives | No exceptions noted. |

| Risk Assessment | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | Risk assessments are performed by management 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. | Inspected risk assessment documentation to determine that a risk assessment was performed during the period and, as part of this process, threats and changes to service commitments were identified and the risks were formally assessed. | No exceptions noted. |
| | | Inspected risk assessment documentation to determine that the risk assessment included a consideration of the potential for fraud and how fraud may have impacted the achievement of objectives. | No exceptions noted. |
| | A documented business continuity/disaster recovery (BC/DR) plan is in place and tested annually. | Inspected the BC/DR plan to determine that a documented BC/DR plan was in place. | No exceptions noted. |
| | | Inspected results from the BC/DR plan testing to determine that testing was performed during the period. | No exceptions noted. |
| **CC3.3** | The entity considers the potential for fraud in assessing risks to the achievement of objectives. | | |
| | A documented risk management program is 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. The program considers the following:<br>- Compliance objectives<br>- External laws and regulations<br>- Tolerance for risk<br>- Establishment of sub-objectives to support primary objectives | Inspected the risk management policy to determine that a program had been established around the identification of potential threats, rating the significance of the risks associated with the identified threats, mitigation strategies for those risks, and that the program considered the following:<br>- Compliance objectives<br>- External laws and regulations<br>- Tolerance for risk<br>- Establishment of sub-objectives to support primary objectives | No exceptions noted. |

| Risk Assessment | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | Risk assessments are performed by management 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. | Inspected risk assessment documentation to determine that a risk assessment was performed during the period and, as part of this process, threats and changes to service commitments were identified and the risks were formally assessed. | No exceptions noted. |
| | | Inspected risk assessment documentation to determine that the risk assessment included a consideration of the potential for fraud and how fraud may have impacted the achievement of objectives. | No exceptions noted. |
| **CC3.4** | The entity identifies and assesses changes that could significantly impact the system of internal control. | | |
| | A documented risk management program is 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. The program considers the following:<br>- Compliance objectives<br>- External laws and regulations<br>- Tolerance for risk<br>- Establishment of sub-objectives to support primary objectives | Inspected the risk management policy to determine that a program had been established around the identification of potential threats, rating the significance of the risks associated with the identified threats, mitigation strategies for those risks, and that the program considered the following:<br>- Compliance objectives<br>- External laws and regulations<br>- Tolerance for risk<br>- Establishment of sub-objectives to support primary objectives | No exceptions noted. |
| | Risk assessments are performed by management 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. | Inspected risk assessment documentation to determine that a risk assessment was performed during the period and, as part of this process, threats and changes to service commitments were identified and the risks were formally assessed. | No exceptions noted. |

| Risk Assessment | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | | Inspected risk assessment documentation to determine that the risk assessment included a consideration of the potential for fraud and how fraud may have impacted the achievement of objectives. | No exceptions noted. |
| | A configuration management system is in place to ensure that system configurations are deployed consistently throughout the environment. | Inspected the configuration management tool configuration to determine that a configuration management system was in place to ensure that system configurations were deployed consistently throughout the environment. | No exceptions noted. |
| | A file integrity monitoring (FIM) tool is used to notify system administrators of potential unauthorized changes to the production system. | Inspected alert configuration settings and example alerts to determine that the Company utilized a FIM tool that notified system administrators of potential unauthorized changes to the production systems. | No exceptions noted. |
| | Penetration testing is performed at least annually. | Inspected the penetration test report to determine that penetration testing was performed during the period to identify vulnerabilities that could have been exploited to gain access to the production environment. | No exceptions noted. |
| | A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during the annual penetration test.<br><br>The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No critical or high vulnerabilities were discovered as a result of the penetration test. | Inquired of management and inspected penetration tests for vulnerabilities identified during the penetration test to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether a remediation plan was developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during the annual penetration test. | Not tested. No critical or high vulnerabilities were discovered as a result of the penetration test. |

| Monitoring Activities | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| **CC4.1** | The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. | | |
| | Control self-assessments are performed by management at least annually to gain assurance that controls related to the in-scope Trust Services Categories are in place and operating effectively. Corrective actions are taken based on relevant findings and tracked to resolution. | Inspected control self-assessment documentation to determine that control self-assessments were performed by management during the period and corrective actions were taken based on relevant findings and tracked to resolution. | No exceptions noted. |
| | Penetration testing is performed at least annually. | Inspected the penetration test report to determine that penetration testing was performed during the period to identify vulnerabilities that could have been exploited to gain access to the production environment. | No exceptions noted. |
| | A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during the annual penetration test.<br><br>The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No critical or high vulnerabilities were discovered as a result of the penetration test. | Inquired of management and inspected penetration tests for vulnerabilities identified during the penetration test to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether a remediation plan was developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during the annual penetration test. | Not tested. No critical or high vulnerabilities were discovered as a result of the penetration test. |

| Monitoring Activities | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | Internal and external network vulnerability scans are performed quarterly to identify, quantify, and prioritize vulnerabilities. | Inspected internal and external network vulnerability scans for a sample of quarters to determine that internal and external network vulnerability scans were performed to identify, quantify, and prioritize vulnerabilities. | No exceptions noted. |
| | A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during quarterly internal and external network vulnerability scans.<br><br>The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No critical or high vulnerabilities were discovered during the internal and external vulnerability scans. | Inquired of management and inspected vulnerability scans to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether a remediation plan was developed and changes were implemented to remediate all critical and high vulnerabilities identified during quarterly external network vulnerability scans. | Not tested. No critical or high vulnerabilities were discovered during the internal and external vulnerability scans. |
| | Third-party providers are reviewed to ensure that they meet Stripe requirements based on their risk ranking. | Inspected third-party attestation report review or vendor risk assessment documentation for a sample of vendors to determine that third-party providers are reviewed to ensure that they meet Stripe requirements based on their risk ranking. | No exceptions noted. |
| **CC4.2** | 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. | | |
| | Control self-assessments are performed by management at least annually to gain assurance that controls related to the in-scope Trust Services Categories are in place and operating effectively. Corrective actions are taken based on relevant findings and tracked to resolution. | Inspected control self-assessment documentation to determine that control self-assessments were performed by management during the period and corrective actions were taken based on relevant findings and tracked to resolution. | No exceptions noted. |

| Monitoring Activities | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | Third-party providers are reviewed to ensure that they meet Stripe requirements based on their risk ranking. | Inspected third-party attestation report review or vendor risk assessment documentation for a sample of vendors to determine that third-party providers are reviewed to ensure that they meet Stripe requirements based on their risk ranking. | No exceptions noted. |

| Control Activities | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| **CC5.1** | The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. | | |
| | As part of its annual risk assessment, management selects and develops manual and IT general control activities that contribute to the mitigation of identified risks. | Inspected the risk assessment documentation to determine that, as part of its annual risk assessment, management selected and developed manual and IT general control activities that contributed to the mitigation of identified risks. | No exceptions noted. |
| | A documented risk management program is 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. The program considers the following:<br>- Compliance objectives<br>- External laws and regulations<br>- Tolerance for risk<br>- Establishment of sub-objectives to support primary objectives | Inspected the risk management policy to determine that a program had been established around the identification of potential threats, rating the significance of the risks associated with the identified threats, mitigation strategies for those risks, and that the program considered the following:<br>- Compliance objectives<br>- External laws and regulations<br>- Tolerance for risk<br>- Establishment of sub-objectives to support primary objectives | No exceptions noted. |
| **CC5.2** | The entity also selects and develops general control activities over technology to support the achievement of objectives. | | |
| | As part of its annual risk assessment, management selects and develops manual and IT general control activities that contribute to the mitigation of identified risks. | Inspected the risk assessment documentation to determine that, as part of its annual risk assessment, management selected and developed manual and IT general control activities that contributed to the mitigation of identified risks. | No exceptions noted. |

| Control Activities | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | A documented risk management program is 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. The program considers the following:<br>- Compliance objectives<br>- External laws and regulations<br>- Tolerance for risk<br>- Establishment of sub-objectives to support primary objectives | Inspected the risk management policy to determine that a program had been established around the identification of potential threats, rating the significance of the risks associated with the identified threats, mitigation strategies for those risks, and that the program considered the following:<br>- Compliance objectives<br>- External laws and regulations<br>- Tolerance for risk<br>- Establishment of sub-objectives to support primary objectives | No exceptions noted. |
| **CC5.3** | The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action. | | |
| | Security incident response policies and procedures are documented and provide guidance for detecting, responding to, and recovering from security events and incidents. The policies and procedures are communicated to authorized users. | Inspected the security incident response policies and procedures to determine that they were documented and provided guidance to Company personnel for detecting, responding to, and recovering from security events and incidents. | No exceptions noted. |
| | | Inspected the Company intranet to determine that the security incident response policies and procedures were communicated to authorized users. | No exceptions noted. |
| | Formal procedures are documented that outline the process the Company's staff follows to perform the following access control functions:<br>- Adding new users<br>- Modifying an existing user's access<br>- Removing an existing user's access<br>The procedures are reviewed at least annually. | Inspected formal access control procedures to determine that they were documented, were reviewed during the period, and outlined the following processes:<br>- Adding new users<br>- Modifying an existing user's access<br>- Removing an existing user's access | No exceptions noted. |

| Control Activities | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | Information security policies and procedures are documented and define the information security rules and requirements for the service environment. These policies and procedures are reviewed by management at least annually and updated as needed. | Inspected the Company's information security policies and procedures to determine that they defined applicable information security rules and requirements for the service environment and that they were reviewed by management during the period and updated as needed. | No exceptions noted. |
| | A documented risk management program is 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. The program considers the following:<br>- Compliance objectives<br>- External laws and regulations<br>- Tolerance for risk<br>- Establishment of sub-objectives to support primary objectives | Inspected the risk management policy to determine that a program had been established around the identification of potential threats, rating the significance of the risks associated with the identified threats, mitigation strategies for those risks, and that the program considered the following:<br>- Compliance objectives<br>- External laws and regulations<br>- Tolerance for risk<br>- Establishment of sub-objectives to support primary objectives | No exceptions noted. |
| | Formal procedures are documented that outline the process the Company's staff follows to back up and recover customer data. | Inspected formal backup and recovery procedures to determine that they were documented and outlined the process the Company's staff followed to back up and recover customer data. | No exceptions noted. |
| | A data classification policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel. | Inspected the data classification policy to determine that a policy was in place to help ensure that confidential data was properly secured and restricted to authorized personnel. | No exceptions noted. |

| Control Activities | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | Formal procedures are documented that outline requirements for vulnerability management and system monitoring. The procedures are reviewed at least annually. | Inspected formal vulnerability management and system monitoring procedures to determine that they were documented, were reviewed during the period, and outlined the requirements for vulnerability management and system monitoring. | No exceptions noted. |
| | A vendor management program is in place. Components of this program include:<br>- Maintaining a list of critical third-party vendors<br>- Requirements for third-party vendors to maintain their own security practices and procedures<br>- Annually reviewing critical third-party attestation reports or performing a vendor risk assessment | Inspected the vendor management policy to determine that a vendor management program was in place and components of this program included:<br>- Maintaining a list of critical third-party vendors<br>- Requirements for third-party vendors to maintain their own security practices and procedures<br>- Annually reviewing critical third-party attestation reports or performing a vendor risk assessment | No exceptions noted. |
| | A formal systems development life cycle (SDLC) methodology is in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements. | Inspected formal SDLC methodology to determine that it governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements. | No exceptions noted. |
| | Network and system hardening standards are documented and reviewed by management at least annually. | Inspected network and system hardening standards to determine that they were documented and reviewed by management. | No exceptions noted. |
| | Formal data retention and disposal procedures are documented to guide the secure retention and disposal of Company and customer data. | Inspected the data retention and disposal procedures to determine that data retention and disposal procedures were documented to guide the secure retention and disposal of Company and customer data. | No exceptions noted. |

| Logical and Physical Access Controls | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| **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. | | |
| | Remote access to production systems is restricted to authorized employees with a valid multi-factor authentication (MFA) token over an encrypted virtual private network (VPN) connection. | Observed a remote login session to determine that only authorized employees with valid MFA tokens over encrypted VPN connections could remotely access production systems. | No exceptions noted. |
| | Authentication to the following in-scope production system components requires unique usernames and authorized Secure Shell (SSH) keys:<br>- Network<br>- Applications<br>- Operating system (OS)<br>- Data stores<br>- AWS console<br>- Firewalls<br>- Log data | Observed login attempts to determine that authentication to the following in-scope production system components required unique usernames and authorized SSH keys:<br>- Network<br>- Applications<br>- OS<br>- Data stores<br>- AWS console<br>- Firewalls<br>- Log data | No exceptions noted. |
| | Access to in-scope system components only supports public key authentication and explicitly disallows passwords. Authentication methods are configured according to the Company's policy. | Inspected the authentication policy and authentication configurations for in-scope system components to determine that public key authentication was configured for access and that passwords were explicitly disallowed and that authentication methods were configured according to the Company's policy. | No exceptions noted. |
| | The network is segmented to prevent unauthorized access to customer data. | Inspected the network configurations to determine that the network was segmented to prevent unauthorized access. | No exceptions noted. |

| Logical and Physical Access Controls | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | A formal inventory of production system assets is maintained. | Inspected a system-generated list of assets to determine that a formal inventory of production system assets was maintained. | No exceptions noted. |
| | Encryption is enabled for data stores housing sensitive customer data. | Inspected encryption configurations to determine that encryption was enabled for data stores housing sensitive customer data. | No exceptions noted. |
| **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. | | |
| | User access to in-scope system components is based on job role and function and requires a documented access request form and manager approval prior to access being provisioned. | Inspected access request forms for a sample of users that received access to the in-scope system components to determine that user access to in-scope system components was based on job role and function and required a documented access request form and manager approval prior to access being provisioned. | No exceptions noted. |
| | Termination checklists are completed to track employee terminations, and access is revoked for employees within 24 business hours of termination as part of the termination process. | Inspected termination tickets for a sample of employees terminated during the period to determine that a termination checklist was completed and access was revoked within 24 business hours of termination. | Exceptions noted. 3 out of a sample of 25 terminated employees retained their access beyond 24 business hours after termination. |
| | | Inspected a listing of terminated employees and compared the listing to the active user listings to determine that terminated employees did not retain access to the in-scope systems after their separation. | No exceptions noted. |

| Logical and Physical Access Controls | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | Quarterly access reviews are conducted by management for the in-scope system components to help ensure that access is restricted appropriately. Tickets are created to remove or modify access as necessary in a timely manner. | Inspected access review documentation for a sample of quarters to determine that an access review for in-scope system components was conducted by management quarterly and that tickets were created to remove or modify access as necessary in a timely manner. | 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. | | |
| | Privileged access to the following in-scope production system components is restricted to authorized users with a business need:<br>- Network<br>- Applications<br>- OS<br>- Data stores<br>- AWS console<br>- Encryption keys<br>- Firewalls<br>- Log data | Inspected the access listings, inquired of management, and compared each user's level of access to their job role to determine that privileged access to the following in-scope production system components was restricted to authorized users with a business need:<br>- Network<br>- Applications<br>- OS<br>- Data stores<br>- AWS console<br>- Encryption keys<br>- Firewalls<br>- Log data | No exceptions noted. |

| Logical and Physical Access Controls | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | User access to in-scope system components is based on job role and function and requires a documented access request form and manager approval prior to access being provisioned. | Inspected access request forms for a sample of users that received access to the in-scope system components to determine that user access to in-scope system components was based on job role and function and required a documented access request form and manager approval prior to access being provisioned. | No exceptions noted. |
| | Termination checklists are completed to track employee terminations, and access is revoked for employees within 24 business hours of termination as part of the termination process. | Inspected termination tickets for a sample of employees terminated during the period to determine that a termination checklist was completed and access was revoked within 24 business hours of termination. | Exceptions noted. 3 out of a sample of 25 terminated employees retained their access beyond 24 business hours after termination. |
| | | Inspected a listing of terminated employees and compared the listing to the active user listings to determine that terminated employees did not retain access to the in-scope systems after their separation. | No exceptions noted. |
| | Quarterly access reviews are conducted by management for the in-scope system components to help ensure that access is restricted appropriately. Tickets are created to remove or modify access as necessary in a timely manner. | Inspected access review documentation for a sample of quarters to determine that an access review for in-scope system components was conducted by management quarterly and that tickets were created to remove or modify access as necessary in a timely manner. | No exceptions noted. |
| | Access to migrate changes to production is restricted to authorized personnel. Developers are not granted access to the production environment and cannot deploy code. | Inspected system access listings to determine that access to migrate changes to production was restricted to authorized personnel and did not include personnel with development responsibilities. | No exceptions noted. |

| Logical and Physical Access Controls | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| **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. | | |
| | The Company's production environment is hosted at third-party data centers, which are carved out for the purposes of this report. | Not applicable. | Not applicable. |
| **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. | | |
| | Electronic media containing confidential information is purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.<br><br>The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No electronic media was purged or destroyed. | Inquired of management and inspected media destruction evidence to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether electronic media containing confidential information was purged or destroyed in accordance with best practices or whether certificates of destruction were issued for each device destroyed. | Not tested. No electronic media was purged or destroyed. |
| | A formal inventory of production system assets is maintained. | Inspected a system-generated list of assets to determine that a formal inventory of production system assets was maintained. | No exceptions noted. |
| | Formal data retention and disposal procedures are documented to guide the secure retention and disposal of Company and customer data. | Inspected the data retention and disposal procedures to determine that data retention and disposal procedures were documented to guide the secure retention and disposal of Company and customer data. | No exceptions noted. |

| Logical and Physical Access Controls | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| **CC6.6** | The entity implements logical access security measures to protect against threats from sources outside its system boundaries. | | |
| | Remote access to production systems is restricted to authorized employees with a valid multi-factor authentication (MFA) token over an encrypted virtual private network (VPN) connection. | Observed a remote login session to determine that only authorized employees with valid MFA tokens over encrypted VPN connections could remotely access production systems. | No exceptions noted. |
| | AWS security groups are used and configured to prevent unauthorized access to the production environment. | Inspected security group configurations to determine that security groups were used and configured to prevent unauthorized access to the production environment. | No exceptions noted. |
| | Secure data transmission protocols are used to encrypt confidential and sensitive data when transmitted over public networks. | Inspected transmission protocol configurations to determine that secure data transmission protocols were used to encrypt confidential and sensitive data when transmitted over public networks. | No exceptions noted. |
| | An intrusion detection system (IDS) is used to provide continuous monitoring of the Company's network and early detection of potential security breaches. | Inspected IDS configurations to determine that an IDS was used to provide continuous monitoring of the Company's network and early detection of potential security breaches. | No exceptions noted. |
| | Infrastructure supporting the service is 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 patching auto-deployment configurations in the production environment to determine that infrastructure supporting the service was patched as a part of routine maintenance and as a result of identified vulnerabilities. | No exceptions noted. |

| Logical and Physical Access Controls | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| **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. | | |
| | Secure data transmission protocols are used to encrypt confidential and sensitive data when transmitted over public networks. | Inspected transmission protocol configurations to determine that secure data transmission protocols were used to encrypt confidential and sensitive data when transmitted over public networks. | No exceptions noted. |
| | A mobile device management (MDM) system is in place to centrally manage mobile devices supporting the service. | Inspected the MDM system to determine that it was in place to centrally manage mobile devices supporting the service. | No exceptions noted. |
| | Portable and removable media devices are 'read only' when used. | Inspected configurations for portable and removable media devices to determine that portable and removable media devices were 'read only' when used. | 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. | | |
| | Anti-malware technology is deployed for environments commonly susceptible to malicious attack and is configured to be updated routinely, logged, and installed on all endpoints. | Inspected antimalware configurations to determine anti-malware technology was deployed for environments commonly susceptible to malicious attack and configured to be updated routinely, logged, and installed on all endpoints. | No exceptions noted. |
| | Infrastructure supporting the service is 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 patching auto-deployment configurations in the production environment to determine that infrastructure supporting the service was patched as a part of routine maintenance and as a result of identified vulnerabilities. | No exceptions noted. |

| Logical and Physical Access Controls | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | A file integrity monitoring (FIM) tool is used to notify system administrators of potential unauthorized changes to the production system. | Inspected alert configuration settings and example alerts to determine that the Company utilized a FIM tool that notified system administrators of potential unauthorized changes to the production systems. | No exceptions noted. |

| System Operations | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| **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. | | |
| | Internal and external network vulnerability scans are performed quarterly to identify, quantify, and prioritize vulnerabilities. | Inspected internal and external network vulnerability scans for a sample of quarters to determine that internal and external network vulnerability scans were performed to identify, quantify, and prioritize vulnerabilities. | No exceptions noted. |
| | A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during quarterly internal and external network vulnerability scans.<br>The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No critical or high vulnerabilities were discovered during the internal and external vulnerability scans. | Inquired of management and inspected vulnerability scans to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether a remediation plan was developed and changes were implemented to remediate all critical and high vulnerabilities identified during quarterly external network vulnerability scans. | Not tested. No critical or high vulnerabilities were discovered during the internal and external vulnerability scans. |
| | Risk assessments are performed by management 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. | Inspected risk assessment documentation to determine that a risk assessment was performed during the period and, as part of this process, threats and changes to service commitments were identified and the risks were formally assessed. | No exceptions noted. |
| | | Inspected risk assessment documentation to determine that the risk assessment included a consideration of the potential for fraud and how fraud may have impacted the achievement of objectives. | No exceptions noted. |

| System Operations | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | A configuration management system is in place to ensure that system configurations are deployed consistently throughout the environment. | Inspected the configuration management tool configuration to determine that a configuration management system was in place to ensure that system configurations were deployed consistently throughout the environment. | No exceptions noted. |
| | A file integrity monitoring (FIM) tool is used to notify system administrators of potential unauthorized changes to the production system. | Inspected alert configuration settings and example alerts to determine that the Company utilized a FIM tool that notified system administrators of potential unauthorized changes to the production systems. | No exceptions noted. |
| **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. | | |
| | A log management tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its security objectives. | Inspected the log management tool to determine that logs were analyzed for trends that may have had a potential impact on the Company's ability to achieve its security objectives. | No exceptions noted. |
| | Internal and external network vulnerability scans are performed quarterly to identify, quantify, and prioritize vulnerabilities. | Inspected internal and external network vulnerability scans for a sample of quarters to determine that internal and external network vulnerability scans were performed to identify, quantify, and prioritize vulnerabilities. | No exceptions noted. |

| System Operations | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during quarterly internal and external network vulnerability scans.<br><br>The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No critical or high vulnerabilities were discovered during the internal and external vulnerability scans. | Inquired of management and inspected vulnerability scans to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether a remediation plan was developed and changes were implemented to remediate all critical and high vulnerabilities identified during quarterly external network vulnerability scans. | Not tested. No critical or high vulnerabilities were discovered during the internal and external vulnerability scans. |
| | An intrusion detection system (IDS) is used to provide continuous monitoring of the Company's network and early detection of potential security breaches. | Inspected IDS configurations to determine that an IDS was used to provide continuous monitoring of the Company's network and early detection of potential security breaches. | No exceptions noted. |
| | An infrastructure monitoring tool is utilized to monitor system or infrastructure availability and performance and generates alerts when specific, predefined thresholds are met. | Inspected the infrastructure monitoring tool configurations and an example notification to determine that an infrastructure monitoring tool was utilized to monitor system or infrastructure availability and performance and generated alerts when specific, predefined thresholds were met. | No exceptions noted. |
| | Penetration testing is performed at least annually. | Inspected the penetration test report to determine that penetration testing was performed during the period to identify vulnerabilities that could have been exploited to gain access to the production environment. | No exceptions noted. |

| System Operations | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during the annual penetration test.<br><br>The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No critical or high vulnerabilities were discovered as a result of the penetration test. | Inquired of management and inspected penetration tests for vulnerabilities identified during the penetration test to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether a remediation plan was developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during the annual penetration test. | Not tested. No critical or high vulnerabilities were discovered as a result of the penetration test. |
| | Infrastructure supporting the service is 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 patching auto-deployment configurations in the production environment to determine that infrastructure supporting the service was patched as a part of routine maintenance and as a result of identified vulnerabilities. | 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. | | |
| | Security incident response policies and procedures are documented and provide guidance for detecting, responding to, and recovering from security events and incidents. The policies and procedures are communicated to authorized users. | Inspected the security incident response policies and procedures to determine that they were documented and provided guidance to Company personnel for detecting, responding to, and recovering from security events and incidents. | No exceptions noted. |
| | | Inspected the Company intranet to determine that the security incident response policies and procedures were communicated to authorized users. | No exceptions noted. |

| System Operations | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | Security events are logged, tracked, resolved, and communicated to affected parties by management according to the Company's security incident response policies and procedures. All events are evaluated to determine whether they could have resulted in a failure to meet security commitments and objectives. | Inspected a sample of security event tickets to determine that security events were logged, tracked, resolved, evaluated to determine whether they could have resulted in a failure to meet security commitments and objectives, and communicated to affected parties by management according to the Company's security incident response policies and procedures. | No exceptions noted. |
| | Penetration testing is performed at least annually. | Inspected the penetration test report to determine that penetration testing was performed during the period to identify vulnerabilities that could have been exploited to gain access to the production environment. | No exceptions noted. |
| | A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during the annual penetration test.<br>The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No critical or high vulnerabilities were discovered as a result of the penetration test. | Inquired of management and inspected penetration tests for vulnerabilities identified during the penetration test to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether a remediation plan was developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during the annual penetration test. | Not tested. No critical or high vulnerabilities were discovered as a result of the penetration test. |
| | Internal and external network vulnerability scans are performed quarterly to identify, quantify, and prioritize vulnerabilities. | Inspected internal and external network vulnerability scans for a sample of quarters to determine that internal and external network vulnerability scans were performed to identify, quantify, and prioritize vulnerabilities. | No exceptions noted. |

| System Operations | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | A remediation plan is developed and changes are implemented to remediate, at a minimum, all critical and high vulnerabilities identified during quarterly internal and external network vulnerability scans.<br>The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No critical or high vulnerabilities were discovered during the internal and external vulnerability scans. | Inquired of management and inspected vulnerability scans to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether a remediation plan was developed and changes were implemented to remediate all critical and high vulnerabilities identified during quarterly external network vulnerability scans. | Not tested. No critical or high vulnerabilities were discovered during the internal and external vulnerability scans. |
| **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. | | |
| | Security incident response policies and procedures are documented and provide guidance for detecting, responding to, and recovering from security events and incidents. The policies and procedures are communicated to authorized users. | Inspected the security incident response policies and procedures to determine that they were documented and provided guidance to Company personnel for detecting, responding to, and recovering from security events and incidents. | No exceptions noted. |
| | | Inspected the Company intranet to determine that the security incident response policies and procedures were communicated to authorized users. | No exceptions noted. |
| | All incidents related to security are logged, tracked, and communicated to affected parties by management until the Company has recovered from the incidents.<br>The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No security incidents occurred during the period. | Inquired of management and inspected security event documentation to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether all incidents related to security were logged, tracked, and communicated to affected parties by management until the Company had recovered from the incidents. | Not tested. No security incidents occurred during the period. |

| System Operations | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | Infrastructure supporting the service is 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 patching auto-deployment configurations in the production environment to determine that infrastructure supporting the service was patched as a part of routine maintenance and as a result of identified vulnerabilities. | No exceptions noted. |
| **CC7.5** | The entity identifies, develops, and implements activities to recover from identified security incidents. | | |
| | A documented business continuity/disaster recovery (BC/DR) plan is in place and tested annually. | Inspected the BC/DR plan to determine that a documented BC/DR plan was in place. | No exceptions noted. |
| | | Inspected results from the BC/DR plan testing to determine that testing was performed during the period. | No exceptions noted. |
| | Security incident response policies and procedures are documented and provide guidance for detecting, responding to, and recovering from security events and incidents. The policies and procedures are communicated to authorized users. | Inspected the security incident response policies and procedures to determine that they were documented and provided guidance to Company personnel for detecting, responding to, and recovering from security events and incidents. | No exceptions noted. |
| | | Inspected the Company intranet to determine that the security incident response policies and procedures were communicated to authorized users. | No exceptions noted. |

| System Operations | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | All incidents related to security are logged, tracked, and communicated to affected parties by management until the Company has recovered from the incidents.<br><br>The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No security incidents occurred during the period. | Inquired of management and inspected security event documentation to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether all incidents related to security were logged, tracked, and communicated to affected parties by management until the Company had recovered from the incidents. | Not tested. No security incidents occurred during the period. |
| | The incident response plan is tested at least annually to assess the effectiveness of the incident response program. | Inspected the incident response plan test to determine that the incident response plan was tested during the period to assess the effectiveness of the incident response program. | No exceptions noted. |

| Change Management | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| **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. | | |
| | Changes to software and infrastructure components of the service are authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment. | Inspected change request tickets for a sample of software and infrastructure changes to determine that software and infrastructure changes were authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment. | No exceptions noted. |
| | Access to migrate changes to production is restricted to authorized personnel. Developers are not granted access to the production environment and cannot deploy code. | Inspected system access listings to determine that access to migrate changes to production was restricted to authorized personnel and did not include personnel with development responsibilities. | No exceptions noted. |
| | Infrastructure supporting the service is 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 patching auto-deployment configurations in the production environment to determine that infrastructure supporting the service was patched as a part of routine maintenance and as a result of identified vulnerabilities. | No exceptions noted. |

| Risk Mitigation | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| **CC9.1** | The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. | | |
| | A documented risk management program is 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. The program considers the following:<br>- Compliance objectives<br>- External laws and regulations<br>- Tolerance for risk<br>- Establishment of sub-objectives to support primary objectives | Inspected the risk management policy to determine that a program had been established around the identification of potential threats, rating the significance of the risks associated with the identified threats, mitigation strategies for those risks, and that the program considered the following:<br>- Compliance objectives<br>- External laws and regulations<br>- Tolerance for risk<br>- Establishment of sub-objectives to support primary objectives | No exceptions noted. |
| | Security incident response policies and procedures are documented and provide guidance for detecting, responding to, and recovering from security events and incidents. The policies and procedures are communicated to authorized users. | Inspected the security incident response policies and procedures to determine that they were documented and provided guidance to Company personnel for detecting, responding to, and recovering from security events and incidents. | No exceptions noted. |
| | | Inspected the Company intranet to determine that the security incident response policies and procedures were communicated to authorized users. | No exceptions noted. |
| | The incident response plan is tested at least annually to assess the effectiveness of the incident response program. | Inspected the incident response plan test to determine that the incident response plan was tested during the period to assess the effectiveness of the incident response program. | No exceptions noted. |

| Risk Mitigation | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | A documented business continuity/disaster recovery (BC/DR) plan is in place and tested annually. | Inspected the BC/DR plan to determine that a documented BC/DR plan was in place. | No exceptions noted. |
| | | Inspected results from the BC/DR plan testing to determine that testing was performed during the period. | No exceptions noted. |
| | A multi-location strategy is employed for production environments to permit the resumption of operations at other data centers in the event of the loss of a facility. | Inspected evidence of redundant data centers to determine that the Company employed a multi-location strategy for its production environments to permit the resumption of operations at other data centers in the event of the loss of a facility. | No exceptions noted. |
| | Databases are replicated to a secondary data center in real time. Alerts are configured to notify administrators if replication fails. | Inspected database configurations to determine that databases were replicated to a secondary data center in real time and alerts were configured to notify administration if replication failed. | No exceptions noted. |
| **CC9.2** | The entity assesses and manages risks associated with vendors and business partners. | | |
| | Third-party providers are reviewed to ensure that they meet Stripe requirements based on their risk ranking. | Inspected third-party attestation report review or vendor risk assessment documentation for a sample of vendors to determine that third-party providers are reviewed to ensure that they meet Stripe requirements based on their risk ranking. | No exceptions noted. |
| | The Company reviews the attestation reports for all subservice organizations at least annually to evaluate the impact of noted exceptions on the service. | Inspected subservice organization attestation report review documentation to determine that the Company reviewed the attestation reports for all subservice organizations during the period to evaluate the impact of noted exceptions on the service. | No exceptions noted. |

| Risk Mitigation | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | Formal information sharing agreements are in place with critical vendors. These agreements include confidentiality commitments applicable to that entity. | Inspected contracts for a sample of critical vendors to determine that a formal information sharing agreement was in place and included applicable confidentiality agreements. | No exceptions noted. |

## Additional Criteria for Availability

| Availability | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| **A1.1** | The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives. | | |
| | System capacity is evaluated continuously, and system changes are implemented to help ensure that processing capacity can meet demand. | Inspected documentation of system capacity evaluations performed by management to determine that system capacity was evaluated continuously and system changes were implemented to help ensure that processing capacity could meet demand. | No exceptions noted. |
| | An infrastructure monitoring tool is utilized to monitor system or infrastructure availability and performance and generates alerts when specific, predefined thresholds are met. | Inspected the infrastructure monitoring tool configurations and an example notification to determine that an infrastructure monitoring tool was utilized to monitor system or infrastructure availability and performance and generated alerts when specific, predefined thresholds were met. | No exceptions noted. |
| **A1.2** | The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives. | | |
| | Snapshots of AWS Elastic Block Storage (EBS) volumes are taken hourly, and these backups are replicated nightly to another AWS region. | Inspected backup configurations to determine that AWS EBS snapshots were taken hourly and replicated nightly to another AWS region. | No exceptions noted. |
| | A documented business continuity/disaster recovery (BC/DR) plan is in place and tested annually. | Inspected the BC/DR plan to determine that a documented BC/DR plan was in place. | No exceptions noted. |
| | | Inspected results from the BC/DR plan testing to determine that testing was performed during the period. | No exceptions noted. |

| Availability | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | A multi-location strategy is employed for production environments to permit the resumption of operations at other data centers in the event of the loss of a facility. | Inspected evidence of redundant data centers to determine that the Company employed a multi-location strategy for its production environments to permit the resumption of operations at other data centers in the event of the loss of a facility. | No exceptions noted. |
| | Databases are replicated to a secondary data center in real time. Alerts are configured to notify administrators if replication fails. | Inspected database configurations to determine that databases were replicated to a secondary data center in real time and alerts were configured to notify administration if replication failed. | No exceptions noted. |
| | Formal procedures are documented that outline the process the Company's staff follows to back up and recover customer data. | Inspected formal backup and recovery procedures to determine that they were documented and outlined the process the Company's staff followed to back up and recover customer data. | No exceptions noted. |
| **A1.3** | The entity tests recovery plan procedures supporting system recovery to meet its objectives. | | |
| | Data backup restoration tests are performed at least monthly to verify data reliability and information integrity. | Inspected the results of data backup restoration testing to determine that data backup restoration tests were performed during the period to verify data reliability and information integrity. | No exceptions noted. |
| | A documented business continuity/disaster recovery (BC/DR) plan is in place and tested annually. | Inspected the BC/DR plan to determine that a documented BC/DR plan was in place. | No exceptions noted. |
| | | Inspected results from the BC/DR plan testing to determine that testing was performed during the period. | No exceptions noted. |

| Availability | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | Formal procedures are documented that outline the process the Company's staff follows to back up and recover customer data. | Inspected formal backup and recovery procedures to determine that they were documented and outlined the process the Company's staff followed to back up and recover customer data. | No exceptions noted. |

## Additional Criteria for Processing Integrity

| Processing Integrity | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| **PI1.1** | The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services. | | |
| | There is a process in place for customers to report suspected errors and issues with the management dashboard. Stripe provides customers a direct line of communication to the Support team, who responds to customer questions and concerns. | Inspected screenshots of Stripe Dashboard to determine that users have direct access to the Support team, who responds to questions and concerns regarding Account Information, Charges & Refunds, Transfer & Deposits, Connectivity, Subscriptions, International, Disputes & Fraud, and Accounting & Taxes. | No exceptions noted. |
| | At least quarterly, the Finance team reconciles internal data to the reports that Stripe receives from acquiring partners and from cash balances to identify any transaction processing errors that may have occurred. | Inspected financial reconciliations for a sample of quarters to determine that, at least quarterly, the Finance team reconciled internal data to the reports that Stripe received from acquiring partners and from cash balances to identify any transaction processing errors that may have occurred. | No exceptions noted. |
| **PI1.2** | The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives. | | |
| | Logic is coded into the system that generates on-screen alerts in the event that there are any issues processing transactions. | Inspected application code and observed an example on-screen alert to determine that logic was coded into the system that generated on-screen alerts in the event that there were any issues processing transactions. | No exceptions noted. |

| Processing Integrity | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | Automated internal financial reconciliation systems validate that completed credit and debit transactions align with scheduled payments for customers. | Inspected application code and system configurations to determine that an automated internal financial reconciliation system was used to validate that completed credit and debit transactions aligned with scheduled payments for customers. | No exceptions noted. |
| | New customers sign up for service on the Stripe website. Pricing agreements with customers are set forth in the Stripe Terms of Service and are coded into a data table in the API as part of the new customer registration process. | Inspected customer pricing agreements in the terms of service and the associated API data table for a sample of customers to determine that pricing agreements with customers were set forth in the Stripe Terms of Service and were coded into a data table in the API as part of the new customer registration process. | No exceptions noted. |
| **PI1.3** | The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives. | | |
| | Logging and monitoring tools are used to identify errors and issues with the Stripe management dashboard and also to monitor up-time. The tools are configured to send alerts when issues occur. | Inspected logging and monitoring tool configurations and an example alert to determine that these tools were used to identify errors and issues with the Stripe management dashboard, used to monitor up-time, and configured to send alerts when issues occurred. | No exceptions noted. |
| | Logic is coded into the system that generates on-screen alerts in the event that there are any issues processing transactions. | Inspected application code and observed an example on-screen alert to determine that logic was coded into the system that generated on-screen alerts in the event that there were any issues processing transactions. | No exceptions noted. |

| Processing Integrity | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | Automated internal financial reconciliation systems validate that completed credit and debit transactions align with scheduled payments for customers. | Inspected application code and system configurations to determine that an automated internal financial reconciliation system was used to validate that completed credit and debit transactions aligned with scheduled payments for customers. | No exceptions noted. |
| | Balance transactions are created for every financial event for a merchant and are reconciled with payouts. Stripe personnel are alerted to any inconsistencies or errors for payout transactions. | Inspected system configurations to determine that it was configured to create balance transactions for every merchant and were reconciled with payouts. | No exceptions noted. |
| | | Observed a financial event for a test merchant to determine that a balance transaction was created and reconciled with payouts. | No exceptions noted. |
| | | Inspected alert configurations and an example alert to determine that Stripe personnel were alerted to inconsistencies or errors for payout transactions. | No exceptions noted. |
| | Automated internal financial reconciliation systems validate that transaction fees are calculated and charged by Stripe in a manner consistent with customer agreements. Any errors that are detected are investigated and resolved. The internal admin dashboard displays the status of these automated financial reconciliations. | Observed an example transaction to determine that an automated internal financial reconciliation system validated its transaction fees in a manner consistent with the fee agreement. | No exceptions noted. |
| | | Observed the internal admin dashboard to determine that it displayed the status of automated financial reconciliations. | No exceptions noted. |
| | | Inspected alert configurations and an example alert to determine that any errors that were detected during the automated fee reconciliation were investigated and resolved. | No exceptions noted. |

| Processing Integrity | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | Systematically, Invoicing and Subscription transactions are processed via Recur completely and accurately based on merchants' configuration and the transaction status to complete the payment. | Inspected transaction configurations for invoicing and subscriptions to determine Recur completely and accurately processes the transactions based on the merchants' configuration and the transaction status to complete the payment. | No exceptions noted. |
| | Systematically, payment information and reconciliation for Invoicing and Subscription transactions are processed via Monster to ensure transactions are processed completely and appropriately based on the user's configuration. | Inspected transaction configurations for invoicing and subscriptions to determine Monster completely and accurately processes the transactions based on the user's configuration and the transaction status to complete the payment. | No exceptions noted. |
| | On a daily basis, an automated job runs to identify newly paid invoices for the current day to create Usage Events for Billing Invoice & Subscription Products. | Inspected invoicing configurations to determine an automated job runs daily for newly paid invoices for the current day to create Usage Events for Billing Invoice & Subscription Products | No exceptions noted. |
| **PI1.4** | The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives. | | |
| | Formal data retention and disposal procedures are documented to guide the secure retention and disposal of Company and customer data. | Inspected the data retention and disposal procedures to determine that data retention and disposal procedures were documented to guide the secure retention and disposal of Company and customer data. | No exceptions noted. |
| | Customers can access their transactional information and data via the Stripe management dashboard. The Stripe management dashboard is configured to capture and report customer transactions in real time as they occur. | Inspected the Stripe management dashboard and observed an example transaction to determine that the Stripe management dashboard was configured to capture and report transactions in real time. | No exceptions noted. |

| Processing Integrity | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | The Stripe management dashboard includes a module called Transfer Overview, which provides customers with a snapshot of all of their transactions and the status of funds transfers. | Observed the Stripe management dashboard's Transfer Overview module to determine that it provided customers with a snapshot of all of their transactions and the status of funds transfers. | No exceptions noted. |
| | Customers can access their transactional information and data via the Stripe management dashboard. The dashboard's reporting features include information about transaction fees and how such fees are calculated. | Observed the Stripe management dashboard to determine that customers could access their transactional information and data via the Stripe management dashboard. | No exceptions noted. |
| | Privileged access to the following in-scope production system components is restricted to authorized users with a business need:<br>- Network<br>- Applications<br>- OS<br>- Data stores<br>- AWS console<br>- Encryption keys<br>- Firewalls<br>- Log data | Inspected the access listings, inquired of management, and compared each user's level of access to their job role to determine that privileged access to the following in-scope production system components was restricted to authorized users with a business need:<br>- Network<br>- Applications<br>- OS<br>- Data stores<br>- AWS console<br>- Encryption keys<br>- Firewalls<br>- Log data | No exceptions noted. |

| Processing Integrity | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | On a daily basis, an automated check is performed to ensure the source data that impacts Billing Usage has associated Billing Usage Event for completeness. Discrepancies are investigated and resolved timely. | Inspected billing configurations to determine an automated check runs daily to ensure the source data that impacts Billing Usage has associated Billing Usage events for completeness and alerts for any discrepancies to investigate and resolve. | No exceptions noted. |
| | | Inspected tickets for a sample of billing discrepancies to determine they were investigated and resolved in a timely manner. | No exceptions noted. |
| | Systematically, integration tests run at the time of code change to validate transaction processed is written to the database completely and accurately with the code changes. | Inspected integration test configurations to determine integration tests run at the time of code changes to validate transactions were processed and written to the database completely and accurately with code changes. | No exceptions noted. |
| | Systematically, Subscription users are notified of invoice/transaction status via the user-configured communication channels. | Inspected invoice and transaction configurations to determine subscription users are notified of status via the user-configured communication channels. | No exceptions noted. |
| **PI1.5** | The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives. | | |
| | The application administration portal does not give system administrators the ability to modify transaction data. | Inspected the application administrator permissions to determine that the application administration portal did not give system administrators the ability to modify transaction data. | No exceptions noted. |

| Processing Integrity | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | Privileged access to the following in-scope production system components is restricted to authorized users with a business need:<br>- Network<br>- Applications<br>- OS<br>- Data stores<br>- AWS console<br>- Encryption keys<br>- Firewalls<br>- Log data | Inspected the access listings, inquired of management, and compared each user's level of access to their job role to determine that privileged access to the following in-scope production system components was restricted to authorized users with a business need:<br>- Network<br>- Applications<br>- OS<br>- Data stores<br>- AWS console<br>- Encryption keys<br>- Firewalls<br>- Log data | No exceptions noted. |
| | Customers can access their transactional information and data via the Stripe management dashboard. The Stripe management dashboard is configured to capture and report customer transactions in real time as they occur. | Inspected the Stripe management dashboard and observed an example transaction to determine that the Stripe management dashboard was configured to capture and report transactions in real time. | No exceptions noted. |
| | The Stripe management dashboard includes a module called Transfer Overview, which provides customers with a snapshot of all of their transactions and the status of funds transfers. | Observed the Stripe management dashboard's Transfer Overview module to determine that it provided customers with a snapshot of all of their transactions and the status of funds transfers. | No exceptions noted. |
| | Customers can access their transactional information and data via the Stripe management dashboard. The dashboard's reporting features include information about transaction fees and how such fees are calculated. | Observed the Stripe management dashboard to determine that customers could access their transactional information and data via the Stripe management dashboard. | No exceptions noted. |

| Processing Integrity | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | | Observed the reporting functionality of the Stripe management dashboard to determine that the dashboard's reporting features included information about transaction fees and how such fees were calculated. | No exceptions noted. |
| | Customers can opt to receive alert emails for transactions and bank account deposits to help ensure that transactions are processed correctly. | Observed the Stripe management dashboard to determine that customers could opt to receive alert emails for transactions and bank account deposits to help ensure that transactions were processed correctly. | No exceptions noted. |
| | Automated internal financial reconciliation systems validate that transaction fees are calculated and charged by Stripe in a manner consistent with customer agreements. Any errors that are detected are investigated and resolved. The internal admin dashboard displays the status of these automated financial reconciliations. | Observed an example transaction to determine that an automated internal financial reconciliation system validated its transaction fees in a manner consistent with the fee agreement. | No exceptions noted. |
| | | Observed the internal admin dashboard to determine that it displayed the status of automated financial reconciliations. | No exceptions noted. |
| | | Inspected alert configurations and an example alert to determine that any errors that were detected during the automated fee reconciliation were investigated and resolved. | No exceptions noted. |
| | An automatic job is configured to generate and send the daily settlements file to banks. Any errors that occur during the creation or transmission of files generate a pager alert to administrators. | Inspected the configuration settings and application code to determine that an automatic job was configured to generate and send the daily settlements file to banks. | No exceptions noted. |

| Processing Integrity | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | | Inspected alert configurations and an example alert to determine that any errors that occurred during the creation or transmission of files generated a pager alert to administrators. | No exceptions noted. |
| | The data table in the API that includes pricing can be updated via an internal admin portal. The ability to update pricing tables is restricted to authorized personnel who have a business need. | Inspected the admin portal settings to determine that the data table pricing could be updated by authorized personnel who have a business need. | No exceptions noted. |
| | An internal admin dashboard displays the status of automated financial reconciliations. Any errors that occur during the creation or transmission of files generate a pager alert to administrators. | Observed the internal admin dashboard to determine that it displayed the status of automated financial reconciliations. | No exceptions noted. |
| | | Inspected alert configurations and an example alert to determine that any errors that occurred during the creation or transmission of files generated a pager alert to administrators. | No exceptions noted. |
| | The system is configured to initiate automatic payments to merchants on an ongoing basis. | Inspected system configurations to determine that it was configured to initiate automatic payments to merchants. | No exceptions noted. |
| | An automatic job is configured to generate and send the daily settlements file to banks. Any errors that occur during the creation or transmission of files generate a pager alert to administrators. | Inspected the configuration settings and application code to determine that an automatic job was configured to generate and send the daily settlements file to banks. | No exceptions noted. |
| | | Inspected alert configurations and an example alert to determine that any errors that occurred during the creation or transmission of files generated a pager alert to administrators. | No exceptions noted. |

| Processing Integrity | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| | The Stripe management dashboard is built upon and configured to use data from the API for customer reporting. | Inspected the Stripe management dashboard API to determine that the Stripe management dashboard was built upon and configured to use data from the API for customer reporting. | No exceptions noted. |
| | The Stripe management dashboard is updated and enhanced periodically. When such updates occur, the change management process is initiated and testing is performed to ensure that the management dashboard continues to provide complete and accurate customer reporting. | Inspected a sample of changes to the Stripe management dashboard determine that changes were:<br>- Authorized<br>- Formally documented<br>- Tested prior to migration to production<br>- Peer reviewed and approved | No exceptions noted. |
| | The Stripe management dashboard includes notifications, which provide customers the ability to opt into various alerts from the system. | Inspected the Stripe management dashboard notifications module to determine that it provided customers the ability to opt into receiving various alerts from the system. | No exceptions noted. |
| | The Stripe management dashboard includes a module that allows customers to set payment rules based on Stripe standard or custom parameters. Rulesets require a payment to be reviewed or blocked depending on the type of rule. | Inspected the Stripe management dashboard Radar settings and an example of a payment that was blocked due to high fraud risk to determine it allowed customers to set payment blocking based on Stripe standard or custom parameters. | No exceptions noted. |
| | | Inspected the Stripe management dashboard Radar settings for payment review and an example payment to determine that they required a review prior to posting. | No exceptions noted. |
| | The Interchange (IC) Plus Report is produced monthly for each customer that is on IC Plus pricing. The IC Plus Report includes information about the calculation of transaction fees. | Inspected IC Plus Reports for a sample of customers to determine that the report included information about the calculation of transaction fees. | No exceptions noted. |

## Additional Criteria for Confidentiality

| Confidentiality | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| **C1.1** | The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality. | | |
| | A data classification policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel. | Inspected the data classification policy to determine that a policy was in place to help ensure that confidential data was properly secured and restricted to authorized personnel. | No exceptions noted. |
| | Confidential or sensitive customer data is prohibited by policy from being used or stored in non-production environments. | Inspected the Company change management policy to determine that the use and storage of confidential or sensitive data in non-production systems or environments was prohibited. | No exceptions noted. |
| | | Inspected the test environment to determine that only test data was used in non-production systems or environments. | No exceptions noted. |
| | Formal data retention and disposal procedures are documented to guide the secure retention and disposal of Company and customer data. | Inspected the data retention and disposal procedures to determine that data retention and disposal procedures were documented to guide the secure retention and disposal of Company and customer data. | No exceptions noted. |
| | Formal information sharing agreements are in place with critical vendors. These agreements include confidentiality commitments applicable to that entity. | Inspected contracts for a sample of critical vendors to determine that a formal information sharing agreement was in place and included applicable confidentiality agreements. | No exceptions noted. |

| Confidentiality | | | |
|---|---|---|---|
| | | | |
| **TSC Reference** | **Trust Services Criteria and Applicable Control Activities** | **Service Auditor's Tests** | **Results of Tests** |
| **C1.2** | The entity disposes of confidential information to meet the entity's objectives related to confidentiality. | | |
| | Electronic media containing confidential information is purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.<br><br>The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No electronic media was purged or destroyed. | Inquired of management and inspected media destruction evidence to determine that the circumstances that warrant the operation of the control did not occur during the period. As a result, no testing could be performed to determine whether electronic media containing confidential information was purged or destroyed in accordance with best practices or whether certificates of destruction were issued for each device destroyed. | Not tested. No electronic media was purged or destroyed. |
| | Customer data containing confidential information is purged or removed from the application environment in accordance with best practices when customers leave the service. | Inspected automated data deletion configurations to determine that customer data containing confidential information was purged or removed from the application environment in accordance with best practices when customers left the service. | No exceptions noted. |

# Section 5

# Other Information Provided by Stripe, Inc. That Is Not Covered by the Service Auditor's Report

## Management's Response to Testing Exceptions

| Service Organization's Controls | Results of Tests | Management's Response |
|---|---|---|
| Upon hire, employees must acknowledge an employee handbook that describes their responsibilities and expected behavior regarding data and information system usage. | Exceptions noted. 2 out of a sample of 44 employees did not acknowledge that they had read and agreed to the employee handbook upon hire. | Management views this as a process improvement as all handbooks were signed. Management has implemented additional processes to ensure employee handbooks are signed off timely. Additional processes include an audit to review any handbooks that have not been signed and daily notification reminders. |
| New personnel offered employment are subject to background checks upon hire. | Exceptions noted. 5 out of a sample of 44 new hires did not have their background checks initiated within 30 days of hire. | Management views this as a process improvement / best practice to improve on a go-forward basis as all background checks were completed. |
| Termination checklists are completed to track employee terminations, and access is revoked for employees within 24 business hours of termination as part of the termination process. | Exceptions noted. 3 out of a sample of 25 terminated employees retained their access beyond 24 business hours after termination. | Although access was not removed timely for the users identified, management inspected the user logs, and performed an impact analysis for any users that accessed internal systems post termination. Based on this analysis, management determined there were no inappropriate actions performed by these users before their access was revoked. Stripe also performs a quarterly access review to further mitigate the risk of unauthorized access. |