Report on Stripe, Inc.’s Stripe Payment Processing System Relevant to Security, Availability, and Confidentiality Throughout the Period October 1, 2022 to September 30, 2023

SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report

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 assertion titled "Assertion of Stripe, Inc. Management" (assertion) that the controls within the Stripe Payment Processing System (system) were effective throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that Stripe's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* (2017 TSC).

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

Service Organization's Responsibilities

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. Stripe has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Stripe is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is

fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

Our examination included:

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

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

Inherent Limitations

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

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

Opinion

In our opinion, management's assertion that the controls within the Stripe Payment Processing System were effective throughout the period October 1, 2022 to September 30, 2023, 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 is fairly stated, in all material respects.

Coalfire Controls LLC

Greenwood Village, Colorado
December 15, 2023

Section 2

Assertion of Stripe, Inc. Management

Assertion of Stripe, Inc. (“Stripe”) Management

We are responsible for designing, implementing, operating and maintaining effective controls within the Stripe Payment Processing System (system) throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that Stripe’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* (2017 TSC). Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

The description of the boundaries of the system 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.

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

We have performed an evaluation of the effectiveness of the controls within the system throughout the period October 1, 2022 to September 30, 2023, 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. Stripe’s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

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

We assert that the controls within the system were effective throughout the period October 1, 2022 to September 30, 2023 to provide reasonable assurance that Stripe’s service commitments and system requirements were achieved based on the applicable trust services criteria.

Stripe, Inc.

Attachment A

Stripe, Inc.’s Description of the Boundaries of Its Stripe Payment Processing System

Company Overview

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.

Stripe Payment

Stripe Payments is an online payment processing platform designed to handle financial transactions for businesses of any size. It provides a flexible suite of application programming interfaces (APIs) and hosted/embeddable payments UIs that enable users to support multiple payments use cases (recurring/subscriptions) and accept a wide array of payment methods that serve global buyers.

Integration Methods

Stripe’s Payments offers users a single integration for a localized payment experience, saving them the technical cost and ongoing operational burden of managing multiple integrations to payment gateways, payment methods and merchant banking services – each with bespoke settlement processes that are difficult to reconcile into a single business view.

Users can choose to integrate Stripe with their own custom-built consumer checkout form, or leverage Stripe’s hosted and embeddable payments acceptance UIs that are customizable to the user’s own style and workflow. These UI surfaces optimize buyer experiences based on the customer’s device and location, and ensure secure transmission of sensitive customer data from the browser directly to Stripe, so that users don’t need to collect and store payment method information directly.

Stripe Dashboard

Stripe Dashboard (“Dashboard”) is a tool that enables users to seamlessly operate their business day-to-day and deeply understand performance and growth opportunities for their business going forward. From within the Dashboard, users can view and manage incoming payments, create subscriptions for customers, submit evidence for disputes, and administer partial or full refunds. Users can also see detailed insights into their payments performance (total volume, refund rate), and customer cohorts (lifetime value, top customers), and can toggle on new features like payment methods directly from the Dashboard to further optimize their business performance. Users also have the flexibility to pull additional detailed transaction reports in CSV format for reconciliation purposes.

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.

Checkout

The legacy version of 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. The new version of Checkout (“Stripe Checkout”) is a prebuilt optimized payment form that can be embedded on a users’

site or served as a Stripe-hosted payment page. The branding of the form/page can be changed to match the rest of the users' site. It is built on top of Stripe.js v3.

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. Using Elements, customers can accept payments from 40+ payment methods using their customized payment form. Elements also makes collecting payment details more secure by generating a secure Inline Frame (IFrame) and isolating sensitive information from users' sites.

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.

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 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 and Mastercard as an issuer processor and is built on the same core payments acceptance platform.

Stripe Capital

Stripe Capital ("Capital") is Stripe's business financing program, and currently offers access to merchant cash advances and commercial term loans. Term loans are provided by banks, 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 make payments by having a percentage of the participant's payment processing proceeds withheld by Stripe.

Stripe Terminal

Stripe Terminal (“Terminal”) is an in-person payments solution that provides platforms and enterprises with developer tools, pre certified card readers, Tap to Pay on compatible iPhone and Android devices, and cloud-based device management.

The description of the boundaries of the system in this section of the report details the Stripe Payment Processing System. Any other Company services are not within the scope of this report. The accompanying description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at any subservice organizations (see below for further discussion of the 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.

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

The Company utilizes third parties to provide the resources to host the Stripe Payment Processing System. The Company leverages the experience and resources of the third parties 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 System architecture within the hosting provider’s environment 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**
Databases	Customer data storage
Firewalls	Network protection
Switches	Network traffic
Computers	Productivity

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, but are not limited to, the following applications, as shown in the table below:

Software	
Component	**Description**
OSs	OSs are used to support the covered services.
Data stores	Persistent customer data resides in non-relational document databases, cloud object storage instances, and relational databases.
Network infrastructure	The covered services network infrastructure utilizes security groups and Cloud Domain Name Systems web services.
Application and Infrastructure monitoring	The covered services are monitored using: • A real-time operational and business intelligence platform • An open-source application monitoring platform • An open-source system monitoring platform • An incident management platform • Real-time data processing • A managed distributed denial-of-service (DDoS) protection tool
Security	Security related to covered services are managed using: • Real-time data processing • Auditing, compliance monitoring, and a governance tool • Security information and event management • An automated configuration management tool • Antivirus • Endpoint security and management tool

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; the development, testing, and implementation of changes; incident response; and overall security at the Company.
Compliance and Legal	Responsible for facilitating compliance across various regulatory bodies and requirements (e.g., financial regulators, payment regulations, SOC, Anti-Money Laundering/Counter Financing Terrorism [AML/CFT]).

People	
Group/Role Name	**Function**
Design	Responsible for assisting with the design of product changes, enhancements, and upgrades.
IT	Responsible for supporting and monitoring internal Company systems, maintaining a physical inventory of hardware, and for identifying, addressing, and supporting technical issues.
Human Resources (HR)	Responsible for facilitating day-to-day activities relating to personnel, 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 list details procedures relevant to the operation of the Stripe Payment Processing System:

- Asset Management
- Backup Management
- Business Continuity and Disaster Recovery
- Change Management
- Configuration Management
- Data Management
- Identity and Access Management
- Incident Management
- Mobile Device Management
- Network Operations
- Risk Management
- System Monitoring
- Third-Party Management
- Training and Awareness
- Vulnerability Management

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. Through the 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 databases housing sensitive customer data.

Subservice Organizations

The Company uses subservice organizations for data center colocation services. The Company'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.

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. Controls are expected to be in place at the subservice organizations related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. The subservice organization's physical security controls should mitigate the risk of unauthorized access to the hosting facilities. The subservice organization's environmental protection controls should mitigate the risk of fires, power loss, climate, and temperature variabilities.

The Company management receives and reviews the subservice organization's SOC 2 reports annually. In addition, through its operational activities, Company management monitors the services performed by the subservice organizations to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organizations to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to management of the subservice organizations.

Complementary User Entity Controls

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.

Attachment B

Principal Service Commitments and System Requirements

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 via written service agreements.

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 • User access reviews • Logical access controls • Risk assessment standards • Change management controls
Availability	• Stripe will operate and maintain measures designed to maintain system availability. • Stripe will provide 99.9% system uptime/availability.	• Incident handling policies and procedures • Incident response plan • Business continuity and disaster recovery plan
Confidentiality	• Stripe will take reasonable precautions to protect customers' confidential information. • Stripe will only use customer data for the purposes of providing the services or as otherwise directed or authorized by customers.	• Encryption standards for data at rest and in transit • Data classification and data retention policies