Payment Card Industry
Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0

Revision 1

Publication Date: December 2022

PCI DSS v4.0 Attestation of Compliance for Report on Compliance – Service Providers

Entity Name: Stripe, Inc.

Assessment End Date: 02/02/2024

Date of Report as noted in the Report on Compliance: 03/01/2024

Section 1 Assessment Information

Instructions for Submission

This Attestation of Compliance (AOC) must be completed as a declaration of the results of the service provider's assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures* (“Assessment”). Complete all sections. The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which this AOC will be submitted for reporting and submission procedures.

This AOC reflects the results documented in an associated Report on Compliance (ROC). Associated ROC sections are noted in each AOC Part/Section below.

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Report on Compliance Template.

Part 1. Contact Information	
Part 1a. Assessed Entity **(ROC Section 1.1)**	
Company name:	Stripe, Inc.
DBA (doing business as):	Not Applicable
Company mailing address:	354 Oyster Point Blvd South San Francisco, CA 94080
Company main website:	https://www.stripe.com
Company contact name:	Aaron Spinks
Company contact title:	Head of Infrastructure
Contact phone number:	888-963-8955
Contact e-mail address:	support@stripe.com
Part 1b. Assessor **(ROC Section 1.1)**	
Provide the following information for all assessors involved in the Assessment. If there was no assessor for a given assessor type, enter Not Applicable.	
PCI SSC Internal Security Assessor(s)	
ISA name(s):	Akhila Chitiprolu
Qualified Security Assessor	
Company name:	Coalfire Systems, Inc.
Company mailing address:	8480 E. Orchard Rd., Suite 5800 Greenwood Village, CO 80111
Company website:	www.coalfire.com
Lead Assessor name:	Riona Mascarenhas
Assessor phone number:	303-554-6333

Assessor e-mail address:	CoalfireSubmission@coalfire.com
Assessor certificate number:	QSA – 205-285

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the Assessment (select all that apply):

Name of service(s) assessed:	Stripe Payments – (Checkout, Payment Links, Elements, Link, Stripe.js v3, Stripe.jsv2), Stripe Connect, Stripe Dashboard, Stripe Billing, Stripe Invoicing, Stripe Terminal, Stripe Mobile (iOS and Android Mobile SDKs), Stripe Issuing, Stripe API, Stripe Card Image Verification

Type of service(s) assessed:

Hosting Provider: ☐ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web-hosting services ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Multi-Tenant Service Provider ☐ Other Hosting (specify):	**Managed Services:** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☒ POI / card present ☒ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☐ Other processing (specify):
☐ Account Management	☒ Fraud and Chargeback	☒ Payment Gateway/Switch
☐ Back-Office Services	☒ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☒ Clearing and Settlement	☒ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☐ Others (specify): None		

Note: *These categories are provided for assistance only and are not intended to limit or predetermine an entity's service description. If these categories do not apply to the assessed service, complete "Others." If it is not clear whether a category could apply to the assessed service, consult with the entity(ies) to which this AOC will be submitted.*

Part 2a. Scope Verification *(continued)*		
Services that are provided by the service provider but were NOT INCLUDED in the scope of the Assessment (select all that apply):		
Name of service(s) not assessed:	Not Applicable	
Type of service(s) not assessed:		
Hosting Provider: □ Applications / software □ Hardware □ Infrastructure / Network □ Physical space (co-location) □ Storage □ Web-hosting services □ Security services □ 3-D Secure Hosting Provider □ Multi-Tenant Service Provider □ Other Hosting (specify):	**Managed Services:** □ Systems security services □ IT support □ Physical security □ Terminal Management System □ Other services (specify):	**Payment Processing:** □ POI / card present □ Internet / e-commerce □ MOTO / Call Center □ ATM □ Other processing (specify):
□ Account Management	□ Fraud and Chargeback	□ Payment Gateway/Switch
□ Back-Office Services	□ Issuer Processing	□ Prepaid Services
□ Billing Management	□ Loyalty Programs	□ Records Management
□ Clearing and Settlement	□ Merchant Services	□ Tax/Government Payments
□ Network Provider		
□ Others (specify): Not Applicable		
Provide a brief explanation why any checked services were not included in the Assessment:	Not Applicable	

Part 2b. Description of Role with Payment Cards (ROC Section 2.1)	
Describe how the business stores, processes, and/or transmits account data.	Stripe, Inc. is a fintech company that provides software solutions that allows businesses of all sizes to securely accept payments and expand globally. Stripe is an acquirer that processes card-not-present and card-present transactions via the api.stripe.com endpoint. Stripe is considered a Level 1 Service Provider and facilitates payment transactions for customers via Stripe payment applications and integration methods via JavaScript, Stripe API, mobile SDKs, and terminal hardware for transactions. Additionally, Stripe exports

	PANs for user migrations, law enforcement requests and for mandatory card reporting. Stripe's API service (api.stripe.com) enables payment transactions for merchants and allows Stripe to manage the collection, processing and storage of payments and CHD on their behalf. Merchants are provided with a tokenized API service to process credit card transactions. Merchants securely connect to Stripe by including a snippet of code in their back-end custom application. The API code allows the cardholder details such as name, address, primary account number (PAN), card expiration date, and card validation value (CVV2, CVC2, CID) that are collected to be transmitted securely via HTTPS using TLS to Stripe. Stripe vaults CHD within a token vault database using strong encryption. For payment processing, CHD details (such as primary account number (PAN), card expiration date, and card validation value (CVV2, CVC2, CID)) are sent outbound to Stripe's third-party payment processing partners via dedicated IPSec VPN tunnels or site-to-site VPN connections, which are contingent on the partner. Post authorization, only the status of the payment card transaction details and the token are stored in the databases for settlement processes. No Sensitive Authentication Data (SAD) is stored on any system components post authorization. In addition to payment processing, Stripe also enables Issuing services via the Stripe API.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	None – All functionality and services that could impact the security of cardholder data are described and listed above.
Describe system components that could impact the security of account data.	The following system components were assessed within the CDE: • Network firewalls, switches, and routers • Virtual firewalls (security groups) • Servers (bastions, application, logging, database) Support Systems o Multi-factor authentication o Server configuration management o Network Time Synchronization o Access authorization o Change Management o File Integrity Monitoring (FIM) o Intrusion Detection/Intrusion Prevention o Logging and Alerting

Part 2c. Description of Payment Card Environment	
Provide a high-level description of the environment covered by this Assessment. *For example:* • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.* • *System components that could impact the security of account data.*	Stripe's cardholder data environment (CDE) system components are hosted across AWS cloud hosting environments and Equinix datacenters. These environments are physically and logically separated from the company's corporate offices and development/testing environments. There is no direct physical or point to point Virtual Private Network (VPN) connections between the production CDE cloud environment and the Stripe corporate office network or the development/testing environments. The CDE is segmented from non CDE systems using virtual firewalls and Access Control Lists (ACLs). Inbound access from the Internet to the CDE is secured over HTTPS with TLS encryption supporting the most secure protocol and highest cipher that the customer's browser can negotiate to access the Stripe applications and to process payment transactions. Remote access to the CDE is restricted via bastion hosts enabled with multifactor authentications. Outbound connections are restricted to necessary ports and protocols to support forwarding transactions to payment partners for payment authorization.
Indicate whether the environment includes segmentation to reduce the scope of the Assessment. (Refer to the "Segmentation" section of PCI DSS for guidance on segmentation)	☒ Yes ☐ No

Part 2d. In-Scope Locations/Facilities **(ROC Section 4.6)**
List all types of physical locations/facilities (for example, corporate offices, data centers, call centers and mail rooms) in scope for this Assessment.

Facility Type	**Total Number of Locations** (How many locations of this type are in scope)	**Location(s) of Facility** (city, country)
Physical Data Centers	7	Equinix Colocation Data Centers • Tokyo, Japan • Osaka, Japan • San Jose, CA, USA • Washington DC USA • Seattle, WA, USA

© 2006 - 2022 PCI Security Standards Council, LLC. All rights reserved.

		• STET (Equinix datacenter regions of Saint-Denis, France and Paris, France)
Cloud hosted datacenters – AWS	9	AWS Cloud Hosting Data Centers • ap-northeast-1 / Asia Pacific (Tokyo) • ap-south-1 / Asia Pacific (Mumbai) • ap-southeast-1 / Asia Pacific (Singapore) • ap-southeast-2 / Asia Pacific (Sydney) • eu-west-1 / Europe (Ireland) • us-east-1 / US East (N. Virginia) • us-east-2 / US East (Ohio) • us-west-1 / US West (N. California) • us-west-2 / US West (Oregon)

Part 2e. PCI SSC Validated Products and Solutions
(ROC Section 3.3)

Does the entity use any item identified on any PCI SSC Lists of Validated Products and Solutions*?

☒ Yes ☐ No

Provide the following information regarding each item the entity uses from PCI SSC's Lists of Validated Products and Solutions:

Name of PCI SSC-validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which Product or Solution Was Validated	PCI SSC Listing Reference Number	Expiry Date of Listing
Stripe Terminal P2PE	Not Applicable	P2PE v3.1	2022-01212.001	05/26/2025

* For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components, appearing on the PCI SSC website (www.pcisecuritystandards.org) (for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Payment Applications (PA-DSS), Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, and Contactless Payments on COTS (CPoC) solutions).

Part 2f. Third-Party Service Providers (ROC Section 4.4)	
For the services being validated, does the entity have relationships with one or more third-party service providers that:	
- Store, process, or transmit account data on the entity's behalf (for example, payment gateways, payment processors, payment service providers (PSPs, and off-site storage))	☒ Yes ☐ No
- Manage system components included in the entity's Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting companies, and IaaS, PaaS, SaaS, and FaaS cloud providers)	☐ Yes ☒ No
- Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).	☐ Yes ☒ No

If Yes:

Name of Service Provider:	**Description of Services Provided:**
Amazon - Amazon Web Services (AWS)	Cloud Service Provider
Equinix, Inc.	Colocation Hosting Provider
Idemia UK	Facilitates Issuing of cards
Fastly	Content Delivery Network

Note: *Requirement 12.8 applies to all entities in this list.*

© 2006 - 2022 PCI Security Standards Council, LLC. All rights reserved.

Part 2g. Summary of Assessment
(ROC Section 1.8.1*)*

Indicate below all responses provided within each principal PCI DSS requirement.

PCI DSS Requirement	**Requirement Finding** More than one response may be selected for a given requirement. Indicate all responses that apply.				**Select If Below Method(s) Was Used**	
	In Place	**Not Applicable**	**Not Tested**	**Not in Place**	**Customized Approach**	**Compensating Controls**
Requirement 1:	☒	☒	☐	☐	☐	☐
Requirement 2:	☒	☒	☐	☐	☐	☐
Requirement 3:	☒	☒	☐	☐	☐	☐
Requirement 4:	☒	☒	☐	☐	☐	☐
Requirement 5:	☒	☒	☐	☐	☐	☐
Requirement 6:	☒	☒	☐	☐	☐	☐
Requirement 7:	☒	☐	☐	☐	☐	☐
Requirement 8:	☒	☒	☐	☐	☐	☐
Requirement 9:	☒	☒	☐	☐	☐	☐
Requirement 10:	☒	☒	☐	☐	☐	☐
Requirement 11:	☒	☒	☐	☐	☐	☐
Requirement 12:	☒	☒	☐	☐	☐	☐
Appendix A1:	☐	☒	☐	☐	☐	☐
Appendix A2:	☐	☒	☐	☐	☐	☐

© 2006 - 2022 PCI Security Standards Council, LLC. All rights reserved.

Section 2 Report on Compliance

(**ROC Sections 1.2 and 1.3.2**)

Date Assessment began: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*			07/19/2023
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*			02/02/2024
Were any requirements in the ROC unable to be met due to a legal constraint?			☐ Yes ☒ No
Were any testing activities performed remotely? If yes, for each testing activity below, indicate whether remote assessment activities were performed:			☒ Yes ☐ No
• Examine documentation	☒ Yes	☐ No	
• Interview personnel	☒ Yes	☐ No	
• Examine/observe live data	☒ Yes	☐ No	
• Observe process being performed	☒ Yes	☐ No	
• Observe physical environment	☐ Yes	☒ No	
• Interactive testing	☒ Yes	☐ No	
• Other: None	☐ Yes	☐ No	

© 2006 - 2022 PCI Security Standards Council, LLC. All rights reserved.

Section 3 Validation and Attestation Details

Part 3. PCI DSS Validation (ROC Section 1.7)

This AOC is based on results noted in the ROC dated *(Date of Report as noted in the ROC 03/01/2024)*.

Indicate below whether a full or partial PCI DSS assessment was completed:

☒ **Full Assessment** – All requirements have been assessed and therefore no requirements were marked as Not Tested in the ROC.

☐ **Partial Assessment** – One or more requirements have not been assessed and were therefore marked as Not Tested in the ROC. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the ROC noted above, each signatory identified in any of Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document *(select one):*

☒	**Compliant:** All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT** rating; thereby *Stripe, Inc.* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating; thereby Not Applicable has not demonstrated compliance with PCI DSS requirements. **Target Date** for Compliance: *Not Applicable* An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4.
☐	**Compliant but with Legal exception:** One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby Stripe has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction. This option requires additional review from the entity to which this AOC will be submitted. *If selected, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement from being met
Not Applicable	Not Applicable

Part 3a. Service Provider Acknowledgement	
Signatory(s) confirms: (Select all that apply)	
☒	The ROC was completed according to *PCI DSS*, Version 4.0 and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
☒	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Service Provider Attestation	
Aaron Spinks	
Signature of Service Provider Executive Officer ↑	Date: 03/01/2024
Service Provider Executive Officer Name: Aaron Spinks	Title: Head of Infrastructure

Part 3c. Qualified Security Assessor (QSA) Acknowledgement	
If a QSA was involved or assisted with this Assessment, indicate the role performed:	☒ QSA performed testing procedures.
	☐ QSA provided other assistance. If selected, describe all role(s) performed:
Riona Mascarenhas	
Signature of Lead QSA ↑	Date: 03/01/2024
Lead QSA Name: Riona Mascarenhas	
Signature of Duly Authorized Officer of QSA Company ↑	Date: 03/01/2024
Duly Authorized Officer Name: Nick Trenc	QSA Company: Coalfire Systems, Inc.

Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement	
If an ISA(s) was involved or assisted with this Assessment, indicate the role performed:	☐ ISA(s) performed testing procedures.
	☒ ISA(s) provided other assistance. If selected, describe all role(s) performed: Assisted in scheduling walkthroughs, and provided evidence for testing.

Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has Non-Compliant results noted in Section 3.

If asked to complete this section, select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement below. For any “No” responses, include the date the entity expects to be compliant with the requirement and provide a brief description of the actions being taken to meet the requirement.

PCI DSS Requirement	**Description of Requirement**	**Compliant to PCI DSS Requirements** (Select One)		**Remediation Date and Actions** (If “NO” selected for any Requirement)
		YES	**NO**	
1	Install and maintain network security controls	☒	□	
2	Apply secure configurations to all system components	☒	□	
3	Protect stored account data	☒	□	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	☒	□	
5	Protect all systems and networks from malicious software	☒	□	
6	Develop and maintain secure systems and software	☒	□	
7	Restrict access to system components and cardholder data by business need to know	☒	□	
8	Identify users and authenticate access to system components	☒	□	
9	Restrict physical access to cardholder data	☒	□	
10	Log and monitor all access to system components and cardholder data	☒	□	
11	Test security systems and networks regularly	☒	□	
12	Support information security with organizational policies and programs	☒	□	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	□	□	Not Applicable
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	□	□	Not Applicable