Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

June 2018

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS).* Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

Part 1. Service Provider and Qualified Security Assessor Information

Part 1a. Service Provider Organization Information

Company Name:	Stripe, Inc.	DBA (doing business as):	Stripe, Inc. (US) Stripe Payments Canada, Limited (Canada) Stripe Payments UK Limited Stripe Technology Europe Limited Stripe Payments Europe Limited Stripe Payments Singapore Pte Ltd. Stripe Payments Malaysia Sdn Bhd. PT Stripe Payments Indonesia Stripe Payments (Thailand) Ltd. Stripe India Private Limited Stripe Japan, Inc. Stripe Payments Australia Pty Ltd Stripe New Zealand Limited Stripe Brasil Soluções de Pagamento -Instituição de Pagamento Ltda. Stripe Payments Mexico, S. de R.L. de C.V.
Contact Name:	Aaron Spinks	Title:	Head of Infrastructure
Telephone:	(888) 963-8955	E-mail:	support@stripe.com
Business Address:	354 Oyster Point Blvd	City:	South San Francisco

State/Province:	California	Country:	USA	Zip:	94080
URL:	https://www.stripe.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:	Coalfire Systems, Inc.				
Lead QSA Contact Name:	Riona Mascarenhas		Title:	Senior Security Consultant	
Telephone:	303.554.6333		E-mail:	CoalfireSubmission@coalfire.com	
Business Address:	11000 Westmoor Circle, Suite 450		City:	Westminster	
State/Province:	CO	Country:	USA	Zip:	80021
URL:	https://www.coalfire.com				

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) assessed:	Stripe Payments – (Checkout, Payment Links and Elements, stripe. jsv3, 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, Link.	
Type of service(s) assessed:		
Hosting Provider: ☐ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☐ Other Hosting (specify):	**Managed Services (specify):** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☒ POS / 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 you feel these categories don't apply to your service, complete "Others." If you're unsure whether a category could apply to your service, consult with the applicable payment brand.*		

Part 2a. Scope Verification *(continued)*

Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment (check 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 ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☐ Other Hosting (specify):	**Managed Services (specify):** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☐ POS / 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 Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Stripe, Inc. is private fintech company that provides software solutions that allows businesses of all sizes to securely accept payments, expand globally and create new revenue streams. Stripe is a VisaNET processor, Level 1 Service Provider as well as an acquirer and an issuer that processes card-not-present (e-commerce) and card-present transactions (EMV, MSR) via the api.stripe.com endpoint. Stripe facilitates such transactions for customers via Stripe payment applications and integration methods via JavaScript, Stripe API, mobile SDKs, and terminal hardware for transactions. Stripe also exports PANs for user migrations, law enforcement requests and for mandatory card reporting. Stripe.js, is Stripe's foundational JavaScript library for building payment flows which allows the cardholder to input card data within an iFrame served from Stripe's domain. Stripe.js tokenizes sensitive payment details within this iFrame such that cardholder data does not touch merchant's servers. This enables payment transactions for merchants and allows Stripe to manage

	the collection, processing and storage of payments and CHD on their behalf. The API code allows the cardholder data 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 are sent outbound to Stripe's third-party payment processing partners. Post authorization, only the status of the payment card transaction details and the token is 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 and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Not Applicable - All business processes and system functionalities that have an impact to the security of cardholder data have been described above.

Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility:	Number of facilities of this type	Location(s) of facility (city, country):
Example: Retail outlets	*3*	*Boston, MA, USA*
Cloud hosting provider (Amazon Web Services)	9	• ap-northeast-1 • ap-south-1 • ap-southeast-1 • ap-southeast-2 • eu-west-1 • us-east-1 • us-east-2 • us-west-1 • us-west-2
Equinix Colocation Data Centers	7	• Tokyo, Japan • Osaka, Japan • San Jose, CA, USA • Washington DC USA • Seattle, WA, USA • STET (Saint-Denis, France and Paris, France)

Part 2d. Payment Applications

Does the organization use one or more Payment Applications? ☐ Yes ☒ No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
Not Applicable	Not Applicable	Not Applicable	☐ Yes ☐ No	Not Applicable

Part 2e. Description of 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 POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	Stripe's cardholder data environment (CDE) system components is 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 are 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. The following critical system components within the CDE were assessed: • Network firewalls, switches and routers • Virtual firewalls (security groups) • Servers (bastions, application, logging, database) Support Systems ○ Multi-factor authentication ○ Server configuration management ○ Network Time Synchronization ○ Access authorization ○ Change Management ○ File Integrity Monitoring (FIM) ○ Intrusion Detection/Intrusion Prevention ○ Logging and Alerting

	○ Vulnerability Scanning ○ Penetration testing

Does your business use network segmentation to affect the scope of your PCI DSS environment? *(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*	☒ Yes ☐ No

Part 2f. Third-Party Service Providers	
Does your company have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated?	☐ Yes ☒ No
If Yes:	
Name of QIR Company:	Not Applicable
QIR Individual Name:	Not Applicable
Description of services provided by QIR:	Not Applicable
Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?	☐ Yes ☐ No
If Yes:	

Name of service provider:	**Description of services provided:**
Amazon Web Services	Cloud hosting provider
Equinix	Datacenter hosting services
Cardinal Commerce	Service Provider
Idemia UK	Issuing service provider
Fastly	Content Delivery Network

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

Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as "Not Tested" or "Not Applicable" in the ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as "Not Tested" or "Not Applicable" in the ROC.
- **None** – All sub-requirements of that requirement were marked as "Not Tested" and/or "Not Applicable" in the ROC.

For all requirements identified as either "Partial" or "None," provide details in the "Justification for Approach" column, including:

- Details of specific sub-requirements that were marked as either "Not Tested" and/or "Not Applicable" in the ROC
- Reason why sub-requirement(s) were not tested or not applicable

***Note:** One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website*.

Name of Service Assessed:	Stripe Payments – (Checkout, Payment Links and Elements, stripe. jsv3, 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, Link

PCI DSS Requirement	**Details of Requirements Assessed**			
	Full	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Requirement 1:	☒	□	□	
Requirement 2:	□	☒	□	Requirement 2.1.1 – Not Applicable, Stripe does not possess wireless networks connected to the CDE. Requirement 2.2.3 – Not Applicable, Stripe does not possess insecure protocols within the CDE. Requirement 2.6 – Not Applicable, Stripe is not a shared hosting provider.
Requirement 3:	□	☒	□	Requirement 3.4.1 – Not Applicable, Stripe does not utilize any disk encryption technologies within its CDE. Requirement 3.6.a – Not Applicable, Stripe does not share keys with customers.
Requirement 4:	□	☒	□	Requirements 4.1.1 – Not Applicable, no wireless networks transmitting CHD are connected to the CDE.
Requirement 5:	☒	□	□	
Requirement 6:	□	☒	□	Requirements 6.4.6 – Not Applicable, Stripe did not have any significant changes made to the CDE in the past 12 months.
Requirement 7:	☒	□	□	

Requirement 8:	☐	☒	☐	Requirement 8.1.5 – Not Applicable, Stripe does not provide vendors with remote access to the CDE. Requirement 8.5.1 – Not Applicable, Stripe does not provide services that require remote access to customer premises or systems.
Requirement 9:	☐	☒	☐	Requirement(s) 9.5, 9.5.1, 9.6, 9.6.1, 9.6.2, 9.6.3, 9.7, 9.7.1, 9.8, 9.8.1, 9.8.2– Not Applicable, Stripe does not store PAN or sensitive authentication data in any form (digital or non-digital media) or backup media. Requirement (s) 9.9, 9.9.1, 9.9.2, and 9.9.3 – Not Applicable, protection and inspection of the POS devices used on customer premises is the responsibility of Stripe's customers who have such devices.
Requirement 10:	☒	☐	☐	
Requirement 11:	☐	☒	☐	Requirement 11.2.3 – Not Applicable, no significant changes were made to the CDE that required unscheduled scans. Requirement 11.3.3 – Not Applicable, no exploitable vulnerabilities observed during the penetration tests.
Requirement 12:	☐	☒	☐	Requirement 12.3.9 – Not Applicable, Stripe does not allow vendors with access to the CDE system components.
Appendix A1:	☐	☐	☒	A1.1, A1.2, A1.3, A1.4: Not Applicable – Stripe is not a shared hosting provider.
Appendix A2:	☐	☐	☒	A2.1, A2.2, A2.3: Not Applicable – Stripe does not utilize SSL or TLS 1.0 in the CDE environment.

Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	*03/01/2023*	
Have compensating controls been used to meet any requirement in the ROC?	☐ Yes	☒ No
Were any requirements in the ROC identified as being not applicable (N/A)?	☒ Yes	☐ No
Were any requirements not tested?	☐ Yes	☒ No
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes	☒ No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated *03/01/2023.*

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

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *Stripe,Inc.* as demonstrated full compliance with the PCI DSS.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby *Not Applicable* has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: Not Applicable An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with the payment brand(s) before completing Part 4.*
☐	**Compliant but with Legal exception:** One or more requirements are marked “Not in Place” due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand. *If checked, complete the following:*

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

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

☒	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version *3.2.1*, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
☐	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
☒	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
☒	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

Part 3a. Acknowledgement of Status (continued)	
☒	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☒	ASV scans are being completed by the PCI SSC Approved Scanning Vendor *Trustwave SecureTrust.*

Part 3b. Service Provider Attestation

Aaron Spinks

Signature of Service Provider Executive Officer ↑	*Date:* 3/1/2023 | 11:56 AM PST
Service Provider Executive Officer Name: Aaron Spinks	*Title:* Head of Infrastructure

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)	
If a QSA was involved or assisted with this assessment, describe the role performed:	Conducted PCI DSS 3.2.1 remote assessment and documented compliance results in a Report on Compliance and associated Attestation of Compliance (AOC).

Riona Mascarenhas

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* 3/1/2023 | 12:09 PM PST
Duly Authorized Officer Name: Riona Mascarenhas	*QSA Company:* Coalfire Systems, Inc.

Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)	
If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	Stripe ISA (Akhila Chitiprolu) supported on PCI DSS 3.2.1 remote assessment, provided policies and procedures, network diagrams, data flow diagrams, supported remote interviews, and document collection to support Stripe Report on Compliance and associated Attestation of Compliance (AOC).

[1] Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

[2] The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

[3] Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement. If you answer “No” to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with the applicable payment brand(s) before completing Part 4.

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 a firewall configuration to protect cardholder data	☒	☐	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	☐	
3	Protect stored cardholder data	☒	☐	
4	Encrypt transmission of cardholder data across open, public networks	☒	☐	
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	☐	
6	Develop and maintain secure systems and applications	☒	☐	
7	Restrict access to cardholder data by business need to know	☒	☐	
8	Identify and authenticate access to system components	☒	☐	
9	Restrict physical access to cardholder data	☒	☐	
10	Track and monitor all access to network resources and cardholder data	☒	☐	
11	Regularly test security systems and processes	☒	☐	
12	Maintain a policy that addresses information security for all personnel	☒	☐	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	☒	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☒	☐	