Security
Standards Council ®

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 France SARL Stripe Deutschland GmbH Stripe Netherlands B.V. Stripe Payments Mexico S de RL de CV Stripe Payments HK Limited Stripe Brasil Soluções de Pagamento Ltda Stripe Payments Canada Ltd. Stripe Canada Payment Services Ltd. Stripe Payments Europe Limited Stripe Payments UK, Ltd. Stripe Japan KK/Stripe Japan, Inc. Stripe Payments Australia, Ltd. Stripe New Zealand Limited Stripe Payments Singapore Pte, Ltd. Stripe India Private Limited Stripe Payments Malaysia Sdn. Bhd. PT Stripe Payments Indonesia Stripe Payments Company

Contact Name:	Mike Dahn		Title:	Security Policy Relations	
Telephone:	415-420-4331		E-mail:	md@stripe.com	
Business Address:	510 Townsend St		City:	San Francisco	
State/Province:	CA	Country:	USA	Zip:	94103
URL:	https://www.stripe.com				

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

Company Name:	Securisea, Inc.				
Lead QSA Contact Name:	Josh Daymont		Title:	Principal	
Telephone:	404-431-4042		E-mail:	joshd@securisea.com	
Business Address:	Suite 1100 – 201 Spear St		City:	San Francisco	
State/Province:	CA	Country:	USA	Zip:	94105
URL:	https://www.securisea.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 - including Stripe Elements, Stripe.js, Stripe Checkout, Stripe mobile libraries, Stripe Terminal SDK, the Stripe API and Stripe issuing

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):		

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:	N/A

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):		

Provide a brief explanation why any checked services were not included in the assessment:	

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Stripe provides e-commerce and card-present payment processing services to merchants. Stripe received cardholder data from its merchants via the following Stripe integration methods: Javascript libraries, mobile libraries, hosted payment fields, or direct posts to the API. Card numbers are stored, encrypted, in Stripe's Card Data Vault, and merchants are issued tokens that represent those cards for later use.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Stripe handles cardholder data for the transactions and cardholders it processes data for, and can impact the security of this data. Stripe also provisions various Stripe integration code for merchants to accept cardholder data (e.g., hosted payment fields, Javascript and mobile libraries). Stripe does not perform other services that might impact the security of cardholder data.

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*
Corporate offices	2	San Francisco, CA Seattle, WA
IaaS	1	Covered by Stripes TPSP AoC for Amazon Web Services
Datacenters	5	Tokyo, Japan Osaka, Japan San Jose, CA, USA Asburn, VA, USA Seattle, WA, USA

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)
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	

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*	Stripe's PCI environment, consisting of certain dataenter transmission locations and its Stripe Card Data Vault (CDV), is segmented from the rest of the Stripe infrastructure. The CDV receives requests containing cardholder data, tokenizes the CHD, and forwards the requests to Stripe's

necessary payment components, as applicable.	payment processing environment. Outbound traffic to payment processors passes through the CDV environment in which tokens are substituted for the orignial cardholder data. The CDV environment contains only the services required to receive data from third parties, transmit data to third parties, and perform the tokenization and vaulting processes, with some supporting management infrastructure. Management of the CDE is performed remotely using Stripe laptops, accessing the CDE via SSH with two-factor authentication. Some networking equipment is co-located in datacenters where physical routers provided by payment brands are required. These environments are managed in the same fashion and do not contain cardholder data.

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:	
QIR Individual Name:	
Description of services provided by QIR:	
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 (AWS)	IaaS
Equinix	Colocation datacenters for North America
Objective Ventures	Colocation datacenters for Japan

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 - including Stripe Elements, Stripe.js, Stripe Checkout, Stripe mobile libraries, and the Stripe API and Stripe Issiung

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:	□	☒	□	1.2.3 is not applicable as there are no wireless in scope
Requirement 2:	□	☒	□	2.1.1 is not applicable as there are no wireless in scope
Requirement 3:	□	☒	□	3.4.1 is not applicable as disk encryption is not used to achieve PCI compliance
Requirement 4:	□	☒	□	4.1.1 is not applicable as there are no wireless networks in scope
Requirement 5:	□	□	☒	Except for documentation requirements, Requirement 5 is not applicable as Stripe does not have any in-scope systems that are commonly affected by malware. All in scope systems are Linux or vendor proprietary
Requirement 6:	☒	□	□	
Requirement 7:	☒	□	□	
Requirement 8:	□	☒	□	8.1.5 is not applicable as Stripe does not permit any 3rd party access to its CDE 8.5.1 is not applicable as Stripe does not access

				customer environments
Requirement 9:	☐	☒	☐	Requirement 9.9 is not applicable as Stripe does not use any POS systems
Requirement 10:	☐	☒	☐	10.2.7 is not applicable as ASAPP's AWS Lambda CDE implementation does not support changes to system level objects
Requirement 11:	☒	☐	☐	
Requirement 12:	☒	☐	☐	
Appendix A1:	☐	☐	☒	Stripe is not a shared service provider
Appendix A2:	☐	☐	☒	A2.1 is not applicable as Stripe does not use any POS systems

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:	March 1st 2019	
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 March 1st 2019**.**

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. has 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 *(Service Provider Company Name)* has not demonstrated full compliance with the PCI DSS.

Target Date for Compliance:

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

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

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	*Date:* March 1, 2019
Service Provider Executive Officer Name:	*Title:* Security Policy Relations

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	Full PCI-DSS Assessment and preparation of Report on Compliance

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* March 1st 2019
Duly Authorized Officer Name: Josh Daymont	*QSA Company:* Securisea, 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:	

[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	☒	☐	

AMERICAN EXPRESS DISCOVER JCB mastercard VISA