



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 Brasil Emissora Ltda. Stripe Payments Mexico, S. de R.L. de C.V.
Contact Name:	Mike Dahn	Title:	Head of Compliance Management
Telephone:	(888) 963-8955	E-mail:	pci-contact@stripe.com
Business Address:	OP 354 Oyster Point Blvd,	City:	San Francisco

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

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

Company Name:	Coalfire Systems, Inc.				
Lead QSA Contact Name:	Gerald Drake III	Title:	Senior Manager		
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, PaymentLinks 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
------------------------------	---

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):

- | | | |
|---|--|--|
| <input type="checkbox"/> Account Management | <input checked="" type="checkbox"/> Fraud and Chargeback | <input checked="" type="checkbox"/> Payment Gateway/Switch |
| <input type="checkbox"/> Back-Office Services | <input checked="" type="checkbox"/> Issuer Processing | <input type="checkbox"/> Prepaid Services |
| <input type="checkbox"/> Billing Management | <input type="checkbox"/> Loyalty Programs | <input type="checkbox"/> Records Management |
| <input checked="" type="checkbox"/> Clearing and Settlement | <input checked="" type="checkbox"/> Merchant Services | <input type="checkbox"/> Tax/Government Payments |
| <input type="checkbox"/> Network Provider | | |
| <input type="checkbox"/> 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: 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 is a 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 offers several tools that enable business customers to integrate and connect to the Stripe application programming interface (API) to perform payment transactions for card-present and card-not-present. Stripe facilitates transactions for their customers via Stripe payment solutions and integration methods via JavaScript, Stripe API, mobile SDKs, and terminal hardware for card-present transactions.

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. Stripe provides merchants with a tokenized API service to process credit card transactions. Stripe's web API makes an underlying function of a web site or application available to third-party services. In addition to payment processing, Stripe also enables Issuing services via the Stripe API.

Merchants securely connect to Stripe by including a snippet of code in their public web-based shopping cart or back-end custom application. The API code allows the cardholder data (full PAN, expiry) collected on the HTML form fields to be transmitted securely back to Stripe. Stripe vaults CHD within a token vault database using AES256SIV encryption.

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 card-present and card-not-present transactions and the cardholders it processes data for, which can impact the security of this data. Stripe provides various Stripe integration code for merchants to accept cardholder data using the in-scope Stripe Products.

Stripe does not perform any 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):
-------------------	-----------------------------------	--

Cloud Hosting Provider (PaaS)	9	Amazon Web Services (AWS): ap-northeast-1 / Asia Pacific ap-south-1 / Asia Pacific ap-southeast-1 / Asia Pacific ap-southeast-2 / Asia Pacific eu-west-1 / Europe us-east-1 / US East us-east-2 / US East us-west-1 / US West us-west-2 / US West
Data Centers	7	Seattle, WA Washington DC, USA San Jose, CA Osaka, Japan Tokyo, Japan Saint-Denis, France Bailly-Romainvillers, France
Corporate Offices	2	San Francisco, CA Seattle, WA

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.	Not applicable.	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 is a 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 receives PANs via e-commerce, mobile, terminal devices and batch upload from other payment processors/users. Stripe also exports PANs for user migrations, law enforcement requests and for mandatory card reporting.

Stripe facilitates transactions for their customers via Stripe payment applications and integration methods via JavaScript, Stripe API, mobile SDKs, and terminal hardware for transactions.

Stripe offers customers the ability to perform payment transactions via a number of Stripe services, including: payment processing API endpoints (i.e. api.stripe.com), code to integrate Stripe payments (i.e. Stripe.jsv3 and Mobile

	<p>SDKs), and third-party terminal hardware for card-present customers.</p> <p>The Stripe 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. Stripe provides card present and card-not-present merchants with a tokenized API service to process credit card transactions. Stripe's web API makes an underlying function of a web site or application available to third-party services.</p> <p>Merchants connect to Stripe by including a snippet of code in their public web-based shopping cart or back-end custom application. The API code allows the cardholder data (full PAN, expiry) collected on the HTML form fields to be transmitted securely back to Stripe.</p> <p>Stripe vaults CHD within a token vault database using AES 256-bit minimum encryption. Stripe processes CHD on behalf of their merchants.</p> <p>In addition to payment processing, Stripe also enables Issuing services via the Stripe API.</p>
--	--

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.

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 services / Platform as a Service
Equinix	Physical security and colocation services
Cardinal Commerce	Service Provider
Idemia UK	Issuing Service Provider
Fastly	Content Delivery Network

CloudFlare	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, PaymentLinks 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		
PCI DSS Requirement	Details of Requirements Assessed			Justification for Approach (Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)
	Full	Partial	None	
Requirement 1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1.2.2 - Not applicable. Coalfire observed that routers are not in use within Stripe's in-scope environment
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2.1.1 - Not applicable. Stripe does not permit wireless networks or wireless access to the CDE. 2.2.3 – Not applicable. Stripe does not permit insecure services, protocols, or daemons within the CDE. 2.6 – Not applicable. Stripe is not a shared hosting provider.
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	3.4.1 – Not applicable. Stripe does not utilize disk encryption for storage of CHD.
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	4.1.1 - Not applicable. Stripe does not permit wireless networks or wireless access to the CDE.
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 6:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	6.4.6 – Not applicable. No significant changes.
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Requirement 8:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	8.1.5 - Not applicable. Stripe does not permit any 3rd parties access to their CDE, which includes vendor remote access.
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	9.6-9.8.2 - Not applicable. Stripe does not distribute media externally to 3rd parties or individual entities. 9.9-9.9.3 – Not applicable. Stripe does not maintain any physical card reader devices or point of sale devices.
Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 11:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	11.2.3 – Not applicable. No significant changes occurred where Stripe would need to perform out of band vulnerability management activities.
Requirement 12:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

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 1 st , 2022
Have compensating controls been used to meet any requirement in the ROC?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any requirements in the ROC identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Were any requirements not tested?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> 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, 2022.

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**):

<input checked="" type="checkbox"/>	<p>Compliant: All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby Stripe has demonstrated full compliance with the PCI DSS.</p>				
<input type="checkbox"/>	<p>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 (<i>Service Provider Company Name</i>) has not demonstrated full compliance with the PCI DSS.</p> <p>Target Date for Compliance:</p> <p>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. <i>Check with the payment brand(s) before completing Part 4.</i></p>				
<input type="checkbox"/>	<p>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.</p> <p><i>If checked, complete the following:</i></p> <table border="1" style="width: 100%;"> <thead> <tr> <th style="width: 50%;">Affected Requirement</th> <th style="width: 50%;">Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td style="height: 20px;"> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met		
Affected Requirement	Details of how legal constraint prevents requirement being met				

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(**Check all that apply**)

<input checked="" type="checkbox"/>	The ROC was completed according to the <i>PCI DSS Requirements and Security Assessment Procedures</i> , Version 3.2.1, and was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
<input type="checkbox"/>	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
<input checked="" type="checkbox"/>	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
<input checked="" type="checkbox"/>	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)

<input checked="" type="checkbox"/>	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.
<input checked="" type="checkbox"/>	ASV scans are being completed by the PCI SSC Approved Scanning Vendor Trustwave SecureTrust

Part 3b. Service Provider Attestation

 <small>DocuSigned by: 430873F2F1F042C...</small>	
Signature of Service Provider Executive Officer ↑	Date: 03/01/2022
Service Provider Executive Officer Name:	Title:

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).
 <small>DocuSigned by: 61CAC99DA6244BC...</small>	
Signature of Duly Authorized Officer of QSA Company ↑	Date: 03/01/2022
Duly Authorized Officer Name: Gerald Drake III	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 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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems against malware and regularly update anti-virus software or programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify and authenticate access to system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10	Track and monitor all access to network resources and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

