



# **Payment Card Industry Data Security Standard**

---

## **Attestation of Compliance for Report on Compliance – Service Providers**

**Version 4.0.1**

Publication Date: August 2024

# **PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance – Service Providers**

**Entity Name: Stripe, Inc.**

**Date of Report as noted in the Report on Compliance: 03/01/2025**

**Date Assessment Ended: 02/05/2025**

## 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):	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.
Company mailing address:	354 Oyster Point Blvd South San Francisco, CA 94080
Company main website:	<a href="https://www.stripe.com">https://www.stripe.com</a>
Company contact name:	Aaron Spinks
Company contact title:	Head of Infrastructure
Contact phone number:	888-963-8955
Contact e-mail address:	<a href="mailto:support@stripe.com">support@stripe.com</a>

#### 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): Not Applicable

## Qualified Security Assessor

Company name: Coalfire Systems, Inc.

Company mailing address: 8480 E Orchard Rd, Suite 5800, Greenwood Village, CO 80111

Company website: <https://www.coalfire.com>

Lead Assessor name: Riona Mascarenhas

Assessor phone number: +1 877-224-8077

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 Multiprocessor

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 2. Executive Summary *(continued)*

### 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):

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 Sections 2.1 and 3.1)

Describe how the business stores, processes, and/or transmits account data.

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

	<p>exports PANs for user migrations, law enforcement requests and for mandatory card reporting.</p> <p>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.</p> <p>In addition to payment processing, Stripe also enables Issuing services via the Stripe API.</p>
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 above.
Describe system components that could impact the security of account data.	The system components assessed impacting the security of the CDE are in scope databases, servers, firewalls/network security groups.

## Part 2. Executive Summary *(continued)*

### 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. The following critical system components within

the CDE were assessed:

- AWS applicable services (Virtual firewalls (security groups), load balancers, audit trails, time synchronization)
- Servers (bastions, application, logging, database)
- AWS Management console

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 <ul style="list-style-type: none"> <li>• Tokyo, Japan</li> <li>• Osaka, Japan</li> <li>• San Jose, CA, USA</li> <li>• Washington DC USA</li> <li>• Seattle, WA, USA</li> <li>• STET (Equinix datacenter regions of Saint-Denis, France and Paris, France)</li> </ul>
Cloud hosted datacenters – AWS	9	AWS Cloud Hosting Data Centers <ul style="list-style-type: none"> <li>• ap-northeast-1 / Asia Pacific (Tokyo)</li> <li>• ap-south-1 / Asia Pacific (Mumbai)</li> <li>• ap-southeast-1 / Asia Pacific (Singapore)</li> <li>• ap-southeast-2 / Asia Pacific (Sydney)</li> <li>• eu-west-1 / Europe (Ireland)</li> <li>• us-east-1 / US East (N. Virginia)</li> <li>• us-east-2 / US East (Ohio)</li> <li>• us-west-1 / US West (N. California)</li> <li>• us-west-2 / US West (Oregon)</li> </ul>

## Part 2. Executive Summary *(continued)*

### 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](http://www.pcisecuritystandards.org)) (for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions), and Mobile Payments on COTS (MPoC) products.

## Part 2. Executive Summary *(continued)*

### 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))	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> 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)	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
• Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> 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 Generation and issuing of cards
Thales	Facilitates Generation and issuing of cards
Fastly	Content Delivery Network
Kodex, Inc.	Provides secure platform for legal subpoena and litigation responses
Euronet Services India Pvt. Ltd	Provides financial and payment processing services, supporting colocation hosting
STET (Cartes Bancaires)	Provides financial and payment processing services, supporting colocation hosting

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

## Part 2. Executive Summary *(continued)*

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

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

For all requirements identified as either “Not Applicable” or “Not Tested,” complete the “Justification for Approach” table below.

**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, 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 Multiprocessor

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If a Compensating Control(s) Was Used
	In Place	Not Applicable	Not Tested	Not in Place	
Requirement 1:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 2:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 3:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 4:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 5:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 6:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 8:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 9:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 11:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 12:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Justification for Approach

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.

Requirement 1.2.6 – Not Applicable, there are no insecure protocols or services in Stripe CDE.

Requirement 1.3.3 – Not Applicable, there are no wireless networks connected to Stripe CDE.

Requirement 2.2.5 - Not Applicable, there are no insecure services, daemons or protocols enabled in Stripe CDE.

Requirement (s) 2.3.1. 2.3.2 - Not Applicable, Stripe does not maintain any in-scope wireless networks connecting to the cardholder data environment.

Requirement 3.5.1.1 - Not Applicable, hashes are not utilized in the CDE.

Requirement (s) 3.5.1.2, 3.5.1.3 - Not Applicable, Stripe does not utilize disk encryption in the CDE

Requirement 3.6.1.3 - Not Applicable, There is no cleartext access to the cryptographic key materials.

Requirement 3.7.6 – Not Applicable, Stripe does not maintain manual clear text cryptographic key operations in the CDE.

Requirement 3.7.2, 3.7.9 – Not Applicable, Stripe does not share or distribute keys in the CDE

Requirement 4.2.1.2 – Not Applicable, Stripe does not have wireless networks connected to the CDE

Requirement 5.2.3.1 – Not Applicable, Stripe has anti-malware enabled for all assets in the CDE.

Requirement 8.2.2 – Not Applicable, Stripe does not have any shared, generic user accounts in the CDE.

Requirement 8.2.3 – Not Applicable, Stripe does not maintain access to remotely connect to customer premises.

Requirement 8.2.7 - Not Applicable, Stripe does not have remote access to customer premises.

Requirement 8.3.9 – Not Applicable, Stripe has MFA solutions deployed along with passwords.

Requirement (s) 8.3.10. 8.3.10.1 - Not Applicable, Stripe does not provide non-consumer customer access to the CDE.

Requirement (s) 8.6.1, 8.6.2, 8.6.3 – Not Applicable, that there are no accounts used for interactive logins for systems or applications.

Requirement (s) 9.4.1, 9.4.1.1, 9.4.1.2, 9.4.2, 9.4.3, 9.4.4, 9.4.5, 9.4.5.1, 9.4.6, 9.4.7 – Not Applicable, Stripe does not store PAN or sensitive authentication data in any form (digital and non-digital media) or backup media.

Requirement (s) 9.5.1, 9.5.1.1, 9.5.1.2, 9.5.1.2.1, 9.5.1.3 – Not Applicable, Stripe does not maintain POS/POI devices in the CDE.

Requirement (s) 11.3.1.3, 11.3.2.1 - Not Applicable, Stripe did not have any significant changes to the CDE.

Requirement 11.4.4 - Not Applicable, no exploitable vulnerabilities found during the penetration test.

Requirement 11.4.7 - Not Applicable, Stripe does not conduct and maintain penetration testing support for customers.

	<p>Requirement 12.3.2 – Not Applicable, Stripe does not utilize customized approach in the CDE.</p> <p>Requirement 12.5.3 – Not Applicable, there were no significant changes to the organizational structure.</p> <p>Requirement (s) A1.1.1, A1.1.2, A1.1.3, A1.1.4, A1.2.1, A1.2.2, A1.2.3 - Not Applicable, Stripe customers do not have access to the CDE and hence customer specific controls are not applicable.</p> <p>Requirement (s) A2.1.1, A2.1.2, A2.1.3 – Not Applicable, Stripe does not maintain POS/POI devices that use SSL/early TLS.</p>
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	Not Applicable

## Section 2 Report on Compliance

### (ROC Sections 1.2 and 1.3)

Date Assessment began: <b>Note:</b> <i>This is the first date that evidence was gathered, or observations were made.</i>	08/29/2024
Date Assessment ended: <b>Note:</b> <i>This is the last date that evidence was gathered, or observations were made.</i>	02/05/2025
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any testing activities performed remotely?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

## 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 03/01/2025)*.

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*):

<input checked="" type="checkbox"/>	<p><b>Compliant:</b> 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 <b>COMPLIANT</b> rating; thereby Stripe, Inc. has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.</p>				
<input type="checkbox"/>	<p><b>Non-Compliant:</b> 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 <b>NON-COMPLIANT</b> rating; thereby <i>Not Applicable</i> has not demonstrated compliance with PCI DSS requirements.</p> <p><b>Target Date</b> for Compliance: <i>Not Applicable</i></p> <p>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.</p>				
<input type="checkbox"/>	<p><b>Compliant but with Legal exception:</b> 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 <b>COMPLIANT BUT WITH LEGAL EXCEPTION</b> rating; thereby <i>Not Applicable</i> 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.</p> <p>This option requires additional review from the entity to which this AOC will be submitted.</p> <p><i>If selected, complete the following:</i></p> <table border="1"> <thead> <tr> <th>Affected Requirement</th> <th>Details of how legal constraint prevents requirement from being met</th> </tr> </thead> <tbody> <tr> <td>Not Applicable</td> <td>Not Applicable</td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement from being met	Not Applicable	Not Applicable
Affected Requirement	Details of how legal constraint prevents requirement from being met				
Not Applicable	Not Applicable				



### Part 3. PCI DSS Validation *(continued)*

#### Part 3a. Service Provider Acknowledgement

**Signatory(s) confirms:**

(Select all that apply)

<input checked="" type="checkbox"/>	The ROC was completed according to <i>PCI DSS</i> , Version 4.0.1 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 the Assessment in all material respects.
<input checked="" type="checkbox"/>	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

#### Part 3b. Service Provider Attestation

	
  Signature of Service Provider Executive Officer ↑	Date: 03/03/2025
Service Provider Executive Officer Name: Aaron Spinks	Title: Head of Infrastructure



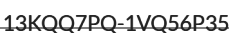
#### Part 3c. Qualified Security Assessor (QSA) Acknowledgement

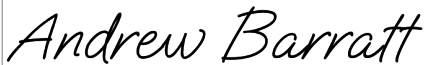

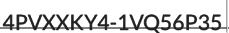
If a QSA was involved or assisted with this Assessment, indicate the role performed:

☒ QSA performed testing procedures.

☐ QSA provided other assistance.

If selected, describe all role(s) performed: Not Applicable

	
  Signature of Lead QSA ↑	Date: 03/03/2025
Lead QSA Name: Riona Mascarenhas	

	
  Signature of Duly Authorized Officer of QSA Company ↑	Date: 03/03/2025
Duly Authorized Officer Name: Andrew Barratt	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:

## 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	<input type="checkbox"/>	<input type="checkbox"/>	
2	Apply secure configurations to all system components	<input type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored account data	<input type="checkbox"/>	<input type="checkbox"/>	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	<input type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems and networks from malicious software	<input type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and software	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to system components and cardholder data by business need to know	<input type="checkbox"/>	<input type="checkbox"/>	
8	Identify users and authenticate access to system components	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
10	Log and monitor all access to system components and cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
11	Test security systems and networks regularly	<input type="checkbox"/>	<input type="checkbox"/>	
12	Support information security with organizational policies and programs	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	<input 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 type="checkbox"/>	<input type="checkbox"/>	

*Note: The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance accepting organization to ensure that this form is acceptable in their program. For more information about PCI SSC and our stakeholder community please visit: [https://www.pcisecuritystandards.org/about\\_us/](https://www.pcisecuritystandards.org/about_us/)*