



# **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: Evo Merchant Services, LLC.**

**Date of Report as noted in the Report on Compliance: 29-Oct-2024**

**Date Assessment Ended: 29-Oct-2024**



## Section 1: Assessment Information

### Instructions for Submission

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

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

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

| Part 1. Contact Information   |  |
|---|--|
| Part 1a. Assessed Entity<br>(ROC Section 1.1)   |  |
| Company name:   | EVO Merchant Services, LLC                                 |
| DBA (doing business as):  | PayFabric  |
| Company mailing address:  | 5995 Windward Parkway, Alpharetta, GA 30005                |
| Company main website:   | https://www.globalpayments.com                             |
| Company contact name:   | Walid Barakat  |
| Company contact title:  | Senior Vice President, Technology and Cyber Risk           |
| Contact phone number:   | 404-731-1375   |
| Contact e-mail address:   | walid.barakat@globalpay.com                                |
| Part 1b. Assessor<br>(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:   | Elizabeth Thomas   |
| Assessor phone number:  | 303-554-6333   |
| Assessor e-mail address:  | CoalfireSubmission@coalfire.com                            |
| Assessor certificate number:  | Coalfire Systems, Inc.                                     |



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: PayFabric  |  |   |
| Type of service(s) assessed:  |  |   |
| <b>Hosting Provider:</b><br><input type="checkbox"/> Applications / software<br><input type="checkbox"/> Hardware<br><input type="checkbox"/> Infrastructure / Network<br><input type="checkbox"/> Physical space (co-location)<br><input type="checkbox"/> Storage<br><input type="checkbox"/> Web-hosting services<br><input type="checkbox"/> Security services<br><input type="checkbox"/> 3-D Secure Hosting Provider<br><input type="checkbox"/> Multi-Tenant Service Provider<br><input type="checkbox"/> Other Hosting (specify):<br>Not Applicable | <b>Managed Services:</b><br><input type="checkbox"/> Systems security services<br><input type="checkbox"/> IT support<br><input type="checkbox"/> Physical security<br><input type="checkbox"/> Terminal Management System<br><input type="checkbox"/> Other services (specify):<br>Not Applicable | <b>Payment Processing:</b><br><input checked="" type="checkbox"/> POI / card present<br><input checked="" type="checkbox"/> Internet / e-commerce<br><input checked="" type="checkbox"/> MOTO / Call Center<br><input type="checkbox"/> ATM<br><input type="checkbox"/> Other processing (specify):<br>Not Applicable |
| <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 type="checkbox"/> Issuer Processing   | <input type="checkbox"/> Prepaid Services   |
| <input checked="" 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 checked="" type="checkbox"/> Others (specify): Tokenization  |  |   |

**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):  
 Not Applicable

#### Managed Services:

- ☐ Systems security services  
☐ IT support  
☐ Physical security  
☐ Terminal Management System  
☐ Other services (specify):  
 Not Applicable

#### Payment Processing:

- ☐ POI / card present  
☐ Internet / e-commerce  
☐ MOTO / Call Center  
☐ ATM  
☐ Other processing (specify):  
 Not Applicable

☐ Account Management

☐ Fraud and Chargeback

☐ Payment Gateway/Switch

☐ Back-Office Services

☐ Issuer Processing

☐ Prepaid Services

☐ Billing Management

☐ Loyalty Programs

☐ Records Management

☐ Clearing and Settlement

☐ Merchant Services

☐ Tax/Government Payments

☐ Network Provider

☐ Others (specify): Not Applicable

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

Not Applicable

### Part 2b. Description of Role with Payment Cards (ROC Sections 2.1 and 3.1)

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

Evo Merchant Services receives and sends CHD (Cardholder data) as noted below for various customers:

- Accepts transactions from merchants via an Internet connection using TLS 1.2 with AES 256-bit and RSA 2048-bit encryption
- Acceptance of transactions from merchants utilizing PayFabric's portal, for payment processing



|  |   |
|--|---|
|  | <ul style="list-style-type: none"><li>• Direct connection from the following card brands (encrypted dedicated circuits, with the bit length varying from AES 128 to AES 256)<ul style="list-style-type: none"><li>◦ Visa</li><li>◦ Mastercard</li><li>◦ Discover</li><li>◦ American Express</li></ul></li><li>• Connection from external merchants POS devices, leveraging TLS V1.2 connections, with AES 128 to AES 256-bit length.</li><li>• HTTPS connections with external clients, leveraging TLS V1.2 connections, with AES 128 to AES 256-bit length.</li></ul> <p>The data received by Evo Merchant Services is processed for a variety of provided services, such as transaction processing, dispute management, backend settlement and clearing.</p> <p>The received data is stored encrypted using AES 256-bit encryption in Microsoft SQL Databases, including:</p> <ul style="list-style-type: none"><li>• PAN</li><li>• Expiry Date</li></ul> <p>SAD (Sensitive Authentication data) is not stored, and is only handled in memory.</p> <p>Evo Merchant Services receives, handles, or provides an interface for interacting with cardholder data via the applications detailed below:</p> <ul style="list-style-type: none"><li>• <b>Spoon:</b> Boarding and residual system for Sterling merchants to SNAP</li><li>• <b>SNAP:</b> Payment gateway switch that routes payment transactions to the various EVO Front-Ends around the globe.</li><li>• <b>Payfabric:</b> PayFabric is an EVO payment processing platform and storage hub that can be integrated easily with any application, system, and/or back-office environment.</li><li>• <b>NGTrans:</b> NGTrans is an acquirer system processing credit, debit, EBT, gift and loyalty transactions.</li><li>• <b>NGTIPS:</b> An add on for NGTRANS that handles receives transactions from US merchants.</li><li>• <b>Esafe:</b> EVO Transaction Risk Monitoring Tool</li><li>• <b>A360:</b> A360 processes transactions and pays merchant via ACH</li></ul> |
|--|---|



|  |  |
|--|--|
|  | <ul style="list-style-type: none"> <li>• <b>Onboard:</b> Onboarding system to A360 and NGTrans</li> <li>• <b>Multipay:</b> Multipay is the payment gateway for EVO Mexico and Chile</li> <li>• <b>Sterling Gateway:</b> Processes transactions for Sterling Merchants via SNAP</li> </ul> <p>The PayFabric application is hosted, developed, and managed by EVO Merchant Services, LLC. It is included among the suite of applications which comprise EVO Merchant Services, LLC's assessment.</p>   |
| Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data. | Not applicable – TSYS stores, processes, and transmits CHD, as described above.  |
| Describe system components that could impact the security of account data.   | <p>The technologies that constitute the Evo Merchant Services CDE include:</p> <ul style="list-style-type: none"> <li>• Firewalls - Filter traffic between the Internet and the CDE, provide segmentation and network address translation.</li> <li>• Load Balancers - Application traffic load balancing and real-time traffic redirection.</li> <li>• Routers and Switches - Provide network connections and manage network traffic</li> <li>• Intrusion Detection/Prevention Systems – To help detect and prevent network intrusions.</li> <li>• Anti-virus - These applications protect the hosts against malware threats and manage the configurations for protecting the hosts.</li> <li>• File Integrity Monitoring - These applications help monitor, detect, and alert on any unauthorised changes to systems and applications in the CDE.</li> <li>• Encryption/Decryption - Applications and appliances that provide encryption, decryption, and key management services for CHD encryption in Evo Merchant Services CDE.</li> <li>• Multi-factor Authentication – Cisco AnyConnect VPN client used in conjunction with Safenet Plus tokens to allow ability to remotely manage systems within the CDE.</li> <li>• Virtualization Management - Administration and management of virtual hosts.</li> <li>• Operating Systems - OS platforms on the servers in the CDE including application, web, database, and jump servers.</li> </ul> |



|  |  |
|--|--|
|  | <ul style="list-style-type: none"><li>• Database Repository - Data repositories storing encrypted CHD in the CDE.</li><li>• Encrypted Storage - Arrays Storage arrays containing CHD in the CDE.</li><li>• Log Monitoring - Splunk is the centralized log management system for log management, retention, and monitoring solution</li></ul> |
|--|--|





Part 2. Executive Summary (continued)

Part 2c. Description of Payment Card Environment

|  |  |
|--|--|
| <p>Provide a high-level description of the environment covered by this Assessment.</p> <p><i>For example:</i></p> <ul style="list-style-type: none"><li>• <i>Connections into and out of the cardholder data environment (CDE).</i></li><li>• <i>Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.</i></li><li>• <i>System components that could impact the security of account data.</i></li></ul> | <p>Supporting processes:</p> <ul style="list-style-type: none"><li>▪ Change Control - Change management processes used for making modifications to systems or applications in the CDE.</li><li>▪ Incident Response - Incident response processes for security related alerts.</li><li>▪ Physical Security - Physical security processes for the control of access for the in-scope sampled physical locations.</li><li>▪ Vulnerability Management - Vulnerability management processes which follows several vendor and industry feeds to identify possible vulnerabilities to systems and platforms.</li><li>▪ Penetration Testing – Evo Merchant Services provision at least annual external, internal, and application penetration testing for its CDE. All Critical findings are addressed to minimize the risk to the Evo Merchant Services CDE.</li><li>▪ Access Provisioning - Logical access control mechanisms for support staff to support services, applications, and infrastructure in the Evo Merchant Services CDE.</li><li>▪ Log Management - Activities on the systems, databases, and applications are logged and monitored to detect any anomalous activity.</li></ul> <p>Software Development - Evo Merchant Services has a software development life cycle that emphasizes code reviews and secure-coding practices for all in-house applications developed to manage or support the processes in the Evo Merchant Services CDE.</p> <p>The technologies that constitute the Evo Merchant Services CDE include:</p> <ul style="list-style-type: none"><li>• Firewalls - Filter traffic between the Internet and the CDE, provide segmentation and network address translation.</li></ul> |
|--|--|



|  |  |
|--|--|
|  | <ul style="list-style-type: none"><li>• Load Balancers - Application traffic load balancing and real-time traffic redirection.</li><li>• Routers and Switches - Provide network connections and manage network traffic</li><li>• Intrusion Detection/Prevention Systems – To help detect and prevent network intrusions.</li><li>• Anti-virus - These applications protect the hosts against malware threats and manage the configurations for protecting the hosts.</li><li>• File Integrity Monitoring - These applications help monitor, detect, and alert on any unauthorised changes to systems and applications in the CDE.</li><li>• Encryption/Decryption - Applications and appliances that provide encryption, decryption, and key management services for CHD encryption in Evo Merchant Services CDE.</li><li>• Multi-factor Authentication – Cisco AnyConnect VPN client used in conjunction with Safenet Plus tokens to allow ability to remotely manage systems within the CDE.</li><li>• Virtualization Management - Administration and management of virtual hosts.</li><li>• Operating Systems - OS platforms on the servers in the CDE including application, web, database, and jump servers.</li><li>• Database Repository - Data repositories storing encrypted CHD in the CDE.</li><li>• Encrypted Storage - Arrays Storage arrays containing CHD in the CDE.</li><li>• Log Monitoring - Splunk is the centralized log management system for log management, retention, and monitoring solution</li></ul> |
|--|--|

|   |   |
|---|---|
| Indicate whether the environment includes segmentation to reduce the scope of the Assessment. | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
|---|---|



|   |  |
|---|--|
| (Refer to the “Segmentation” section of PCI DSS for guidance on segmentation) |  |
|---|--|

**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<br>(How many locations of this type are in scope) | Location(s) of Facility<br>(city, country) |
|-----------------------|---|--|
| Example: Data centers | 3   | Boston, MA, USA                            |
| Data Center           | 2   | Portland, ME<br>Moorestown, NJ             |



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 |
|---|--------------------------------|---|----------------------------------|------------------------|
| Not Applicable                                | Not Applicable                 | Not Applicable  | Not Applicable                   | Not Applicable         |

\* 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: |
|--|-----------------------------------|
| Global Payments                          | Transaction processing            |
| Chase Paymentech                         | Transaction processing            |
| Total Systems (TSYS Acquiring Solutions) | Transaction processing            |
| Shred-IT                                 | Secure shredding                  |
| FIS                                      | Debit Payment Processing          |
| PayTrace                                 | Transaction processing            |
| eGlobal                                  | Transaction processing            |
| Fiserv                                   | Debit Payment Processing          |
| NMI                                      | Transaction processing            |

**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: Evo Merchant Services

| PCI DSS Requirement | Requirement Finding<br>More than one response may be selected for a given requirement.<br>Indicate all responses that apply. |                                     |                          |                          | Select If a<br>Compensating<br>Control(s) Was<br>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 checked="" 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 checked="" 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.

1.2.6 - No insecure ports, protocols or services are utilized in the in-scope environment

2.2.5 - No insecure ports, protocols or services are utilized in the in-scope environment

2.3.1, 2.3.2 - Wireless networks are out of scope for this assessment

3.3.1, 3.3.1.1, 3.3.1.2, 3.3.1.3, 3.3.2, 3.3.3 - Evo Merchant Services does not store any sensitive authentication data

3.4.2 - This requirement is a best practice until March 31, 2025

3.5.1.1 - Evo Merchant Services does not use hashing to render PAN unreadable

3.5.1.2 - This requirement is a best practice until March 31, 2025

4.2.1.1 - This requirement is a best practice until March 31, 2025

4.2.1.2 - Wireless networks are out of scope for this assessment

5.3.3 - There is no removable electronic media in-scope for this assessment

6.3.2, 6.4.3 - This requirement is a best practice until March 31, 2025

6.5.2 - There have been no significant changes to the Evo Merchant Services environment within the assessment period

8.2.3 - Evo Merchant Services does not have remote access to customer premises

8.2.7 - Evo Merchant Services does not provision vendor accounts to manage or support CDE

8.3.10, 8.3.10.1, 8.5.1, 8.6.1, 8.6.2, 8.6.3 - This requirement is a best practice until March 31, 2025

9.4.1.1, 9.4.1.2, 9.4.2, 9.4.3, 9.4.4, 9.4.5, 9.4.5.1 - There is no removable electronic media in-scope for this assessment

9.4.6 - There are no hard copy materials in-scope for this assessment

9.5.1, 9.5.1.1, 9.5.1.2, 9.5.1.2.1, 9.5.1.3 - Evo Merchant Services does not have any point-of-sale (POS) devices or perform any card-present transactions that are in scope for this assessment

10.4.1.1, 10.4.2.1 - This requirement is a best practice until March 31, 2025

11.3.1.2 - This requirement is a best practice until March 31, 2025

11.3.1.3, 11.3.2.1 - There have been no significant changes to the Evo Merchant Services environment within the assessment period

11.4.7 - Evo Merchant Services is not a multi-tenant service provider

11.5.1.1, 11.6.1 - This requirement is a best practice until March 31, 2025

12.3.3 - This requirement is a best practice until March 31, 2025



|   |  |
|---|--|
|   | A1.1.1, A1.1.2, A1.1.3, A1.1.4, A1.2.1, A1.2.2, A1.2.3 - Evo Merchant Services is not a multi-tenant service provider<br>A2.1.1, A2.1.2, A2.1.3 - Evo Merchant Services does not have any point-of-sale (POS) devices or perform any card-present transactions that are in scope for this assessment |
| 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:<br><i><b>Note:</b> This is the first date that evidence was gathered, or observations were made.</i> | 7-Aug-2024  |
| Date Assessment ended:<br><i><b>Note:</b> This is the last date that evidence was gathered, or observations were made.</i>  | 29-Oct-2024   |
| 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 (29-Oct-2024).

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

- ☒ **Full Assessment** – All requirements have been assessed and therefore no requirements were marked as Not Tested in the ROC.
- ☐ **Partial Assessment** – One or more requirements have not been assessed and were therefore marked as Not Tested in the ROC. Any requirement not assessed is noted as Not Tested in Part 2g above.

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

☒ **Compliant:** All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT** rating; thereby *Evo Merchant Services* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.

☐ **Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating; thereby *Not Applicable* has not demonstrated compliance with PCI DSS requirements.  
**Target Date** for Compliance: *Not Applicable*  
An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4.

☐ **Compliant but with Legal exception:** One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *Not Applicable* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction.  
This option requires additional review from the entity to which this AOC will be submitted.  
If selected, complete the following:

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



Part 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

|   |                  |
|---|------------------|
| DocuSigned by:<br><i>David L. Green</i>   |                  |
| Signature of Service Provider Executive Officer  | Date:10/30/2024  |
| Service Provider Executive Officer Name: David Green  | Title: Secretary |

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

|   |   |
|---|---|
| If a QSA was involved or assisted with this Assessment, indicate the role performed:                      | <input checked="" type="checkbox"/> QSA performed testing procedures.   |
|   | <input type="checkbox"/> QSA provided other assistance.<br>If selected, describe all role(s) performed: <i>Not Applicable</i> |
| Signature of Lead QSA  |   |
| Date:   |   |
| Lead QSA Name: Elizabeth Thomas   |   |

|   |                                   |
|---|-----------------------------------|
| Signature of Duly Authorized Officer of QSA Company  | Date:                             |
| Duly Authorized Officer Name:   | QSA Company: Coalfire Systems Ltd |

Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

|  |  |
|--|--|
| If an ISA(s) was involved or assisted with this Assessment, indicate the role performed: | <input type="checkbox"/> ISA(s) performed testing procedures.  |
|  | <input type="checkbox"/> ISA(s) provided other assistance.<br>If selected, describe all role(s) performed: <i>Not Applicable</i> |



## 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<br>(Select One) |                          | Remediation Date and Actions<br>(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/)*