

# **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: Payrix Holdings, LLC**

**Date of Report as noted in the Report on Compliance: 17 March 2025**

**Date Assessment Ended: 17 March 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:	Payrix Holdings, LLC
DBA (doing business as):	Payrix, LLC Payrix Solutions, LLC Benchmark Merchant Solutions, LLC Payrix Canada Corp.
Company mailing address:	5605 Glenridge Drive, Suite 375, Atlanta, Georgia 30342 USA
Company main website:	<a href="https://www.payrix.com">https://www.payrix.com</a>
Company contact name:	Jack Tsigankov
Company contact title:	Director IT & Information Security
Contact phone number:	+1 (215) 500-4263
Contact e-mail address:	<a href="mailto:jack.tsigankov@payrix.com">jack.tsigankov@payrix.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:	A-LIGN Compliance and Security, Inc. dba A-LIGN
Company mailing address:	400 N Ashley Drive, Suite 1325, Tampa, Florida 33602 USA
Company website:	<a href="https://www.A-LIGN.com">https://www.A-LIGN.com</a>
Lead Assessor name:	Svilen Mirchev
Assessor phone number:	+1 (888) 702-5446

Assessor e-mail address:	Svilen.Mirchev@A-LIGN.com
Assessor certificate number:	QSA, 206-536

## 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:	Payment Facilitator Platform (PayFac Platform)	
Type of service(s) assessed:		
<b>Hosting Provider:</b> <input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web-hosting services <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Multi-Tenant Service Provider <input type="checkbox"/> Other Hosting (specify):	<b>Managed Services:</b> <input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify):	<b>Payment Processing:</b> <input type="checkbox"/> POI / card present <input checked="" type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):
<input type="checkbox"/> Account Management	<input checked="" type="checkbox"/> Fraud and Chargeback	<input type="checkbox"/> Payment Gateway/Switch
<input type="checkbox"/> Back-Office Services	<input 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 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 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:		
<b>Hosting Provider:</b> <input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web-hosting services <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Multi-Tenant Service Provider <input type="checkbox"/> Other Hosting (specify):	<b>Managed Services:</b> <input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify):	<b>Payment Processing:</b> <input type="checkbox"/> POI / card present <input type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input type="checkbox"/> Payment Gateway/Switch
<input type="checkbox"/> Back-Office Services	<input 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 type="checkbox"/> Clearing and Settlement	<input type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> Network Provider		
<input type="checkbox"/> Others (specify):		
Provide a brief explanation why any checked services were not included in the Assessment:		Not Applicable. All services provided by Payrix were included within the scope of this assessment.

### 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.	<p>Payrix provides a payment platform, providing authorization and settlement services, as well as transaction analysis services including risk identification and fraud detection. Payrix maintains a database for storing encrypted cardholder data on behalf of their customers to enable scheduled recurring payments to be processed.</p> <p>All credit card information is received by the Payrix API via encrypted connections and stored encrypted within a cloud service provider. A token is generated by Payrix and returned to the client. Cardholder data is inaccessible after this point by the client but may be</p>
---	--

	<p>sent to the processor in future transactions that use the corresponding token. Sensitive Authentication Data, if supplied, is stored temporarily, for a maximum of 24 hours or until the first use of the token for a subscription payment to be made and authorization performed. SAD is only used internally when the token is processed, and then securely deleted from the database when the authorization is made.</p> <p>When processing transactions, Payrix uses encrypted connections to transfer cardholder data to the Worldpay processor.</p>
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Not Applicable. Payrix is not involved in nor has the ability to impact the security of cardholder data, other than their primary business functions related to the payment platform included within the scope of this assessment.
Describe system components that could impact the security of account data.	Payrix utilizes a web server and an API fleet to forward account data to a payment processor. Security impacting systems include a cloud management console, security SaaS solutions (SIEM, Antivirus) and various cloud services used to perform security functions, which are managed by FIS parent entity.

## 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>The assessed environment consists of multiple networks hosted within a PCI compliant cloud service provider as well as web application, and database servers used to receive, process, and store cardholder data in the Payrix environment. Each network contains connections into and out of the CDE to support payment gateway connections.</p> <p>Critical system components included load balancers, firewalls, web servers, databases.</p>
<p>Indicate whether the environment includes segmentation to reduce the scope of the Assessment.</p> <p>(Refer to the "Segmentation" section of PCI DSS for guidance on segmentation)</p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p>

### 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)
<i>Example: Data centers</i>	3	<i>Boston, MA, USA</i>
Datacenter	1	AWS Data Center US East (N. Virginia)
Corporate HQ	1	Atlanta, Georgia, USA
Office	1	Toronto, Ontario, Canada

## 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:
Amazon Web Services	On-demand cloud computing platform that hosts the entity application/services
Fidelity National Information Services, Inc (FIS)	Parent entity responsible for administrative processes, security controls, infrastructure and support
FIS Worldpay US Core Vantiv	Payment Facilitator Third-party Servicer
Cloudflare	Web Application Firewall through which traffic traverses prior to hitting the Payrix platform
Millennium Digital Technologies	VPN provider for access to FIS Worldpay Vantiv and hosting for transaction authorization

**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: Payment Facilitator Platform (PayFac Platform)

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 checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 7:	<input checked="" type="checkbox"/>	<input checked="" 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: Not Applicable. No insecure services, daemons, or protocols were identified.  
 2.3.1 - 2.3.2: Not Applicable. No wireless networks connecting to the CDE or transmitting CHD are present.  
 3.3.3: Not Applicable. The entity is not an issuer.  
 3.4.2: Not Applicable. This requirement is a best practice until 31 March 2025.  
 3.5.1.1: Not Applicable. No hashes of PAN present within the environment.  
 3.5.1.2 - 3.5.1.3: Not Applicable. Disk encryption is not used for encrypting CHD.  
 4.2.1.1: Not Applicable. This requirement is a best practice until 31 March 2025.  
 5.2.3.1: Not Applicable. This requirement is a best practice until 31 March 2025.  
 5.3.2.1 - 5.3.3: Not Applicable. This requirement is a best practice until 31 March 2025.  
 5.4.1: Not Applicable. This requirement is a best practice until 31 March 2025.  
 6.3.2: Not Applicable. This requirement is a best practice until 31 March 2025.  
 6.4.2 - 6.4.3: Not Applicable. This requirement is a best practice until 31 March 2025.  
 6.5.2: Not Applicable. No significant changes have occurred in the past 12 months.  
 7.2.4 - 7.2.5.1: Not Applicable. This requirement is a best practice until 31 March 2025.  
 8.3.6: Not Applicable. This requirement is a best practice until 31 March 2025.  
 8.3.9: Not Applicable. All authentication into in-scope systems required MFA.  
 8.3.10.1: Not Applicable. This requirement is a best practice until 31 March 2025.  
 8.4.2: Not Applicable. This requirement is a best practice until 31 March 2025.  
 8.5.1 - 8.6.3: Not Applicable. This requirement is a best practice until 31 March 2025.  
 9.5.1 - 9.5.1.3: Not Applicable. The entity does not utilize POS/POI within the environment.  
 10.4.1.1: Not Applicable. This requirement is a best practice until 31 March 2025.  
 10.4.2.1: Not Applicable. This requirement is a best practice until 31 March 2025.  
 10.7.2: Not Applicable. This requirement is a best practice until 31 March 2025.  
 11.3.1.1 - 11.3.1.2: Not Applicable. This requirement is a best practice until 31 March 2025.  
 11.3.1.3: Not Applicable. No significant changes have occurred in the past 12 months.  
 11.3.2.1: Not Applicable. No significant changes have occurred in the past 12 months.  
 11.4.7, A1.1.1 - A1.2.3: Not Applicable. The entity is not a multi-tenant service provider.

	<p>11.5.1.1: Not Applicable. This requirement is a best practice until 31 March 2025.</p> <p>11.6.1: Not Applicable. This requirement is a best practice until 31 March 2025.</p> <p>12.3.1: Not Applicable. This requirement is a best practice until 31 March 2025.</p> <p>12.3.2: Not Applicable. No requirements have been met with the customized approach.</p> <p>12.3.3 - 12.3.4: Not Applicable. This requirement is a best practice until 31 March 2025.</p> <p>12.5.2.1 - 12.5.3: Not Applicable. This requirement is a best practice until 31 March 2025.</p> <p>12.6.2: Not Applicable. This requirement is a best practice until 31 March 2025.</p> <p>12.6.3.1 - 12.6.3.2: Not Applicable. This requirement is a best practice until 31 March 2025.</p> <p>12.10.4.1: Not Applicable. This requirement is a best practice until 31 March 2025.</p> <p>12.10.7: Not Applicable. This requirement is a best practice until 31 March 2025.</p> <p>A2.1.1 - A2.1.3: Not Applicable. The entity does not utilize POS/POI within the environment.</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>	26 November 2024
Date Assessment ended: <b>Note:</b> <i>This is the last date that evidence was gathered, or observations were made.</i>	17 March 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 17 March 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 <b>Payrix Holdings, LLC</b> 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 (Service Provider Company Name) has not demonstrated compliance with PCI DSS requirements.</p> <p><b>Target Date</b> for Compliance:</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 (Service Provider Company Name) 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> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement from being met						
Affected Requirement	Details of how legal constraint prevents requirement from being met								

### 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

*Jack Tsigankov*

Signature of Service Provider Executive Officer ↑	Date: 17 March 2025
Service Provider Executive Officer Name: Evgeniy (Jack) Tsigankov	Title: Director IT and Information Security

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

*Svilen Mirchev*

Signature of Lead QSA ↑	Date: 17 March 2025
Lead QSA Name: Svilen Mirchev	

*Petar Besalev*

Signature of Duly Authorized Officer of QSA Company ↑	Date: 17 March 2025
Duly Authorized Officer Name: Petar Besalev, EVP Cybersecurity and Compliance Services	QSA Company: A-LIGN

**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/)*