



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: Paragon Payment Solutions

Date of Report as noted in the Report on Compliance: December 15, 2024

Date Assessment Ended: December 9, 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 (ROC Section 1.1)

Company name:	Blue Parasol Group, LLC (Paragon Payment Solutions), a wholly owned subsidiary of Paya Holdings Inc.
DBA (doing business as):	Paragon Payment Solutions
Company mailing address:	303 Perimeter Center North, Suite 600, Atlanta, GA 30346
Company main website:	https://paya.com
Company contact name:	Alex Tan
Company contact title:	Chief Security Officer
Contact phone number:	404-933-6140
Contact e-mail address:	alex.t@nuvei.com

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:	AARC-360
Company mailing address:	8000 Avalon Boulevard Suite 100, Alpharetta GA 30009
Company website:	https://www.aarc-360.com
Lead Assessor name:	James Spence
Assessor phone number:	(866) 576-4414 ex 108
Assessor e-mail address:	James.Spence@AARC-360.com

Assessor certificate number: 025-041

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: Paragon Payment Solutions

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):

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:	All services were included in the assessment.	
Type of service(s) not assessed:		
Hosting Provider: <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):	Managed Services: <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):	Payment Processing: <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:		

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.

Paragon Solutions engages in financial transaction processing services that involve multiple cardholder data flows. These flows are how cardholder data is stored, processed, and transmitted in each, as follows:

Updating Credit Card Information in Card Safe

1. Paragon Solutions initiates a transaction on CDE Server over port 443 through the Azure Network Security Groups to send PGP Key to third-party gateway provider.

	<p>2. Third-party gateway provider transmits encrypted credit card information via SFTP to provide access to the data center.</p> <p>3. Paragon Solutions decrypts the data on CDE Server and uploads it to Paragon Solutions gateway over port 443 and stores the cardholder data (CHD) encrypted in an SQL database on the database server.</p> <p>4. <i>platform.paragonsolutions.com</i> responds with tokens over TLS.</p> <p>5. Paragon Solutions sends tokens to Integrated Service Vendor (ISV) from the CDE server via HTTPS.</p> <p>Payment Gateway</p> <p>1. Merchant initiates a transaction on <i>platform.paragonsolutions.com</i> over port 443 TLS HTTPS via API, Hosted Payment Page, or Virtual Terminal through the Phoenix Managed Networks (PMN) load balancer and Azure Virtual Application Firewall Cluster.</p> <p>2. <i>platform.paragonsolutions.com</i> queries the Azure SQL database over port 1433 through the Azure Private Network.</p> <p>3. Database responds to <i>platform.paragonsolutions.com</i> over the established connection.</p> <p>4. <i>platform.paragonsolutions.com</i> initiates a transaction with the Processor over TLS.</p> <p>5. Processor responds with the transaction approval over TLS.</p> <p>6. <i>platform.paragonsolutions.com</i> stores responses in the Azure SQL database over port 1433 through the Azure Private Network and stores the CHD encrypted in the SQL database.</p> <p>7. Database responds with completion.</p> <p>8. Merchant is notified of the approval status.</p>
<p>Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.</p>	<p>Paragon Solutions stores, processes and transmits cardholder data received from its customers to facilitate payment processing.</p>
<p>Describe system components that could impact the security of account data.</p>	<p>Web application servers, load balancers Database.</p>

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.

Paragon Solutions receives CHD via gateway servers in Azure (managed by PMN). Customers connect to gateway application and transmit CHD over TLS, which may then be stored in Azure SQL encrypted. Paragon then sends CHD to processors via TLS.

Authorization data flows are related to Paragon Solutions Gateway activities as follows:

1. Merchant initiates a transaction on *platform.paragonsolutions.com* over port 443 TLS https via API, Hosted Payment Page or Virtual Terminal through the Rackspace load balancer, and Azure Virtual Application Firewall Cluster.
2. *platform.paragonsolutions.com* queries the Azure SQL database over port 1433 through the Azure Private Network.
3. Database responds to *platform.paragonsolutions.com* over the established connection.
4. *platform.paragonsolutions.com* initiates transaction with Processor over TLS or Private connection.
5. Processor responds with the transaction approval over TLS or Private connection.
6. *platform.paragonsolutions.com* stores response in the Azure SQL database over port 1433 through the Azure Private Network.
7. Database responds with completion.
8. Merchant is notified of approval status.

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)
Example: Data centers	3	Boston, MA, USA

Azure Cloud	1	USA
QTS data center	1	Atlanta, GA

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
None				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD

* 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) (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:

<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> 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:
Phoenix Managed Networks (PMN)	Network management (including management of Azure environment)
TSYS Acquiring Solutions	Payment processing services, VISANET
First Data (Fiserv Solutions)	Payment processing services
AWS	Hosting provider (DR site)
Azure	Azure N/A Hosting provider

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: Paragon Payment Solutions

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.

1.3.3 - Not applicable – the assessor examined the scope, dataflow diagrams, the configuration settings and confirmed that no wireless networks are included in the PMNs environment.

2.3.2 - Not applicable - The assessor examined the scope, diagrams and network settings and confirmed that there were no wireless systems in scope.

3.3.1.3 - Not applicable - The assessor verified that Paragon Payment Solutions (PMS) does not store personal identification numbers (PIN) or encrypted PIN block after authorization.

3.3.2 - Not applicable -Best practice until March 31, 2025

3.3.3 - Not applicable - Paragon Payment Solutions (PMS) is not a card issuer.

3.5.1.1 - Not applicable. Hashing was not used.

3.5.1.2 through 3.5.1.3 - Not applicable – Paragon Payment Solutions does not use disk-level encryption.

3.7.7 - all cardholder data is in the Azure environment is the responsibility of and managed by PCI DSS compliant services provider Phoenix Managed Networks

3.7.9 - Not applicable – Paragon Solutions is a service provider, but they do not share keys with their customers.

4.2.1.2 - Not applicable – Wireless networks are not part of the Azure cloud.

4.2.2 - Not applicable – End-user messaging technologies are not used to send card holder data.

5.2.2 - these systems are the responsibility of and managed by PCI DSS compliant services provider Phoenix Managed Networks

5.4.1 - Best practice until March 31, 2025.

6.3.2 - Best practice until March 31, 2025.

6.4.3 - Not applicable - The assessor interviewed Int-01 and verified there are no payment scripts loaded or executed in a consumer's browser.

7.2.4 through 7.2.5.1 - Not applicable - Best practice until March 31, 2025

8.2.3 - Not applicable – the assessor reviewed account settings, user IDs access controls in networks and confirmed that service providers do not have remote access to customer premises.

8.2.7 - Not applicable – third parties are not granted access to system components. Review of accounts and interviews confirmed this.

8.3.6 - Not applicable - Best practice until March 31, 2025

8.3.10 through 8.3.10.1 - Not applicable – customers are not granted access.

8.3.11 - Not applicable – underlying systems are cloud based or managed by QTS and PMN in Azure.

8.4.2 - Not applicable - Best practice until March 31, 2025

	<p>8.5.1 through 8.6.3 - Not applicable - Best practice until March 31, 2025</p> <p>9.4.1 through 9.4.7 - Not applicable – No media exists in the cloud-based CHD. 9.5.1 through 9.5.1.3 - Not applicable - Paragon Solutions does not maintain POI devices in its CDE.</p> <p>11.2.1 through 11.2.2 - No wireless components are available in the cloud-based environment. 11.3.1.1 through 11.3.1.2 - Not applicable - Best practice until March 31, 2025. 11.4.7 - Not applicable – not a multi-tenant service provider. 11.6.1 - Not applicable - Best practice until March 31, 2025.</p> <p>12.3.2 - Not applicable – Paragon Payment Solutions did not use a customized approach. 12.3.3 through 12.3.4 - Not applicable - Best practices until March 31, 2025. 12.6.3.1 - Not applicable - Best practices until March 31, 2025.</p> <p>A1 - Paragon is not a Multi-Tenant Service Provider. A2 - Paragon does not have Card-Present transactions.</p>
<p>For any Not Tested responses, identify which sub-requirements were not tested and the reason.</p>	<p>Not applicable</p>

Section 2 Report on Compliance

(ROC Sections 1.2 and 1.3)

Date Assessment began: <i>Note: This is the first date that evidence was gathered, or observations were made.</i>	August 29, 2024
Date Assessment ended: <i>Note: This is the last date that evidence was gathered, or observations were made.</i>	December 9, 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 type="checkbox"/> Yes <input checked="" 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 December 15, 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*):

<input checked="" type="checkbox"/>	<p>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 Paragon Payment Solutions has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.</p>								
<input type="checkbox"/>	<p>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 (<i>Service Provider Company Name</i>) has not demonstrated compliance with PCI DSS requirements.</p> <p>Target Date for Compliance: YYYY-MM-DD</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>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 (<i>Service Provider Company Name</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" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <thead> <tr> <th style="width: 35%;">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

Alex Tan

Alex Tan (Dec 16, 2024 07:23 EST)

Signature of Service Provider Executive Officer ↑	Date: 16/12/24
Service Provider Executive Officer Name: Alex Tan	Title: Chief Security Officer

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:

James Spence

Signature of Lead QSA ↑	Date: 16/12/24
Lead QSA Name: James Spence	

Neil Gonsalves

Signature of Duly Authorized Officer of QSA Company ↑	Date: December 15, 2024
Duly Authorized Officer Name: Neil Gonsalves	QSA Company: AARC-360

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/









PCI DSS AOC - Paragon

Final Audit Report

2024-12-16

Created:	2024-12-16
By:	Neil Gonsalves (neil.gonsalves@aarc-360.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAEJZXAR3RjNhioqyRvHokJQAtgshp0wV-

"PCI DSS AOC - Paragon" History

-  Document created by Neil Gonsalves (neil.gonsalves@aarc-360.com)
2024-12-16 - 3:22:50 AM GMT- IP address: 103.171.43.219
-  Document emailed to James Spence (james.spence@aarc-360.com) for signature
2024-12-16 - 3:22:55 AM GMT
-  Email viewed by James Spence (james.spence@aarc-360.com)
2024-12-16 - 3:23:02 AM GMT- IP address: 52.202.236.132
-  Document e-signed by James Spence (james.spence@aarc-360.com)
Signature Date: 2024-12-16 - 6:33:11 AM GMT - Time Source: server- IP address: 143.44.165.110
-  Document emailed to Alex Tan (alex.t@nuvei.com) for signature
2024-12-16 - 6:33:13 AM GMT
-  Email viewed by Alex Tan (alex.t@nuvei.com)
2024-12-16 - 12:15:48 PM GMT- IP address: 104.47.17.126
-  Document e-signed by Alex Tan (alex.t@nuvei.com)
Signature Date: 2024-12-16 - 12:23:22 PM GMT - Time Source: server- IP address: 163.116.252.33
-  Agreement completed.
2024-12-16 - 12:23:22 PM GMT