



# **Payment Card Industry (PCI) Data Security Standard**

---

## **Attestation of Compliance for Onsite Assessments – Service Providers**

**Version 3.2.1**

June 2018

## Section 1: Assessment Information

### Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

#### Part 1. Service Provider and Qualified Security Assessor Information

##### Part 1a. Service Provider Organization Information

Company Name:	Blue Parasol Group, LLC, a wholly owned subsidiary of Paya Holdings Inc.	DBA (doing business as):	Paragon Payment Solutions		
Contact Name:	Alex Tan	Title:	Chief Security Officer		
Telephone:	(404) 933-6140	E-mail:	Alex.Tan@paya.com		
Business Address:	303 Perimeter Center North, Suite 600, Atlanta, GA 30346	City:	Atlanta		
State/Province:	GA	Country:	USA	Zip:	30346
URL:	https://paya.com				

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

Company Name:	AARC-360				
Lead QSA Contact Name:	James Spence	Title:	Senior Manager		
Telephone:	+1 866 576 4414 Ext. 108	E-mail:	James.Spence@AARC-360.com		
Business Address:	8000 Avalon Boulevard, Suite 100	City:	Alpharetta		
State/Province:	GA	Country:	USA	Zip:	30009
URL:	https://www.aarc-360.com				

## Part 2. Executive Summary

### Part 2a. Scope Verification

**Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):**

Name of service(s) assessed:	Paragon Payment Solutions	
Type of service(s) assessed:		
<b>Hosting Provider:</b> <input checked="" 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 <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Shared Hosting Provider <input type="checkbox"/> Other Hosting (specify):	<b>Managed Services (specify):</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"/> POS / 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 checked="" 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 you feel these categories don't apply to your service, complete "Others." If you're unsure whether a category could apply to your service, consult with the applicable payment brand.

**Part 2a. Scope Verification** *(continued)*

**Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment** (check all that apply):

Name of service(s) not assessed:	Not Applicable	
Type of service(s) not assessed:		
<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 <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Shared Hosting Provider <input type="checkbox"/> Other Hosting (specify):	<b>Managed Services (specify):</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"/> POS / 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 Payment Card Business**

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	<p>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:</p> <p><b>Updating Credit Card Information in Card Safe</b></p> <ol style="list-style-type: none"> <li>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.</li> <li>2. Third-party gateway provider transmits encrypted credit card information via SFTP to provide access to the data center.</li> <li>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.</li> <li>4. <i>platform.paragonsolutions.com</i> responds with tokens over TLS.</li> <li>5. Paragon Solutions sends tokens to Integrated</li> </ol>
--	--

	<p>Service Vendor (ISV) from the CDE server via HTTPS.</p> <p><b>Payment Gateway</b></p> <ol style="list-style-type: none"> <li>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.</li> <li>2. <i>platform.paragonsolutions.com</i> queries the Azure SQL database over port 1433 through the Azure Private Network.</li> <li>3. Database responds to <i>platform.paragonsolutions.com</i> over the established connection.</li> <li>4. <i>platform.paragonsolutions.com</i> initiates a transaction with the Processor over TLS.</li> <li>5. Processor responds with the transaction approval over TLS.</li> <li>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.</li> <li>7. Database responds with completion.</li> <li>8. Merchant is notified of the approval status.</li> </ol>
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Paragon Solutions stores, processes and transmits cardholder data received from its customers to facilitate payment processing.

**Part 2c. Locations**

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility:	Number of facilities of this type	Location(s) of facility (city, country):
<i>Example: Retail outlets</i>	3	<i>Boston, MA, USA</i>
Not applicable		

**Part 2d. Payment Applications**

Does the organization use one or more Payment Applications?  Yes  No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
Not applicable			<input type="checkbox"/> Yes <input type="checkbox"/> No	

			<input type="checkbox"/> Yes <input type="checkbox"/> No
			<input type="checkbox"/> Yes <input type="checkbox"/> No
			<input type="checkbox"/> Yes <input type="checkbox"/> No
			<input type="checkbox"/> Yes <input type="checkbox"/> No
			<input type="checkbox"/> Yes <input type="checkbox"/> No
			<input type="checkbox"/> Yes <input type="checkbox"/> No
			<input type="checkbox"/> Yes <input type="checkbox"/> No

**Part 2e. Description of Environment**

Provide a **high-level** description of the environment covered by this assessment.

*For example:*

- *Connections into and out of the cardholder data environment (CDE).*
- *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*

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.

Does your business use network segmentation to affect the scope of your PCI DSS environment?  
*(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*

Yes  No

**Part 2f. Third-Party Service Providers**

Does your company have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated?  Yes  No

**If Yes:**

Name of QIR Company: Not applicable

QIR Individual Name:

Description of services provided by QIR:

Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?  Yes  No

**If Yes:**

Name of service provider:	Description of services provided:
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 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as “Not Tested” or “Not Applicable” in the ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as “Not Tested” or “Not Applicable” in the ROC.
- **None** – All sub-requirements of that requirement were marked as “Not Tested” and/or “Not Applicable” in the ROC.

For all requirements identified as either “Partial” or “None,” provide details in the “Justification for Approach” column, including:

- Details of specific sub-requirements that were marked as either “Not Tested” and/or “Not Applicable” in the ROC
- Reason why sub-requirement(s) were not tested or not applicable

**Note:** One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.

Name of Service Assessed:		Paragon Payment Solutions		
PCI DSS Requirement	Details of Requirements Assessed			Justification for Approach (Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)
	Full	Partial	None	
Requirement 1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1.2.2 - N/A - Reviewed network diagrams and interviewed administrators to verify that there are no routers present in the Paragon Solution CDE. 1.2.3 - N/A - Reviewed network diagrams and interviewed administrators to verify that there are no wireless environments present in the Paragon Solution CDE.
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2.1.1, 2.2.3 - N/A - Azure is responsible for this control for the Azure tload server environment (security impacting and importing/exporting card flow systems) as documented in the AOC and Responsibility Matrix dated 3/4/2022 2.6 - N/A - Paragon Solutions is not a shared hosting provider.
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	3.4.1 - N/A Disk Encryption not used. 3.6 - N/A - Paragon Solutions is a service provider, but they do not share keys with their customers. 3.6.6 - N/A - No clear-text cryptographic key management operations are used
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	4.1.1 - N/A - Wireless networks are not part of the Paragon Solutions CDE.
Requirement 5:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	5.1.2 - N/A – Paragon Solutions implements anti-virus protection on all CDE systems.
Requirement 6:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	



Requirement 8:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	8.5.1 - N/A - Paragon Solutions is a service provider but does not have remote access to customer environments.
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	9.5, 9.5.1, 9.6, 9.6.1, 9.6.2, 9.6.3, 9.7, 9.7.1, 9.8, 9.8.1, 9.8.2 - N/A – No media exists that contains CHD. 9.9, 9.9.1, 9.9.2, 9.9.3 - N/A - Paragon Solutions does not maintain POI devices in its CDE.
Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 11:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 12:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	N/A - Paragon Solutions is not a shared hosting provider.
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	N/A - Paragon Solutions has no POS POI terminals in its CDE.

## Section 2: Report on Compliance

---

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	December 15, 2023
Have compensating controls been used to meet any requirement in the ROC?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any requirements in the ROC identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Were any requirements not tested?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

## Section 3: Validation and Attestation Details

### Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated *December 15, 2023*.

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

<input checked="" type="checkbox"/>	<p><b>Compliant:</b> All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall <b>COMPLIANT</b> rating; thereby <i>Paragon Payment Solutions</i> has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p><b>Non-Compliant:</b> Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall <b>NON-COMPLIANT</b> rating, thereby (<i>Service Provider Company Name</i>) has not demonstrated full compliance with the PCI DSS.</p> <p><b>Target Date</b> for Compliance:</p> <p>An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. <i>Check with the payment brand(s) before completing Part 4.</i></p>						
<input type="checkbox"/>	<p><b>Compliant but with Legal exception:</b> One or more requirements are marked “Not in Place” due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.</p> <p><i>If checked, complete the following:</i></p> <table border="1" style="width: 100%;"> <thead> <tr> <th style="width: 35%;">Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met				
Affected Requirement	Details of how legal constraint prevents requirement being met						

### Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(**Check all that apply**)

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

**Part 3a. Acknowledgement of Status (continued)**

<input checked="" type="checkbox"/>	No evidence of full track data <sup>1</sup> , CAV2, CVC2, CID, or CVV2 data <sup>2</sup> , or PIN data <sup>3</sup> storage after transaction authorization was found on ANY system reviewed during this assessment.
<input checked="" type="checkbox"/>	ASV scans are being completed by the PCI SSC Approved Scanning Vendor <i>Tenable</i>

**Part 3b. Service Provider Attestation**



Alex Tan (Dec 16, 2023 17:44 EST)

Signature of Service Provider Executive Officer ↑	Date: 16/12/2023
Service Provider Executive Officer Name: Alex Tan	Title: Chief Security Officer

**Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)**

If a QSA was involved or assisted with this assessment, describe the role performed:

AARC-360 verified scope of the environment, reviewed business processes and policy and procedure documents, examined network and data flow diagrams, and reviewed systems and applications inventory.

AARC-360 interviewed subject matter experts to discuss business processes, requested and reviewed evidence such as screenshots and system generated reports of sampled systems, discussed onboarding and off-boarding process with HR, and reviewed processes and procedures to validate PCI DSS v3.2.1 compliance activities.

Additionally, AARC-360 performed research on service providers and other critical technologies used within the Paya in-scope environment, conducted follow up meetings, and wrote the PCI DSS v3.2.1 Report on Compliance.



Signature of Duly Authorized Officer of QSA Company ↑	Date: December 15, 2023
Duly Authorized Officer Name: Neil Gonsalves	QSA Company: Neil Gonsalves & Associates LLC, dba AARC-360

**Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)**

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:

Not Applicable.

<sup>1</sup> Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

<sup>2</sup> The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

<sup>3</sup> Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

## Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement. If you answer “No” to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

*Check with the applicable payment brand(s) before completing Part 4.*

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If “NO” selected for any Requirement)
		YES	NO	
1	Install and maintain a firewall configuration to protect cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems against malware and regularly update anti-virus software or programs	<input type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input type="checkbox"/>	<input type="checkbox"/>	
8	Identify 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	Track and monitor all access to network resources and cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting 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"/>	








# PCI DSS AOC - Service Providers

Final Audit Report

2023-12-16

Created:	2023-12-15
By:	Neil Gonsalves (neil.gonsalves@aarc-360.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAMNvBjC3Re6WceXFQfbg5w9d4NJKvCNmv

## "PCI DSS AOC - Service Providers" History

-  Document created by Neil Gonsalves (neil.gonsalves@aarc-360.com)  
2023-12-15 - 10:10:44 PM GMT- IP address: 71.59.9.4
-  Document emailed to Alex Tan (alex.tan@paya.com) for signature  
2023-12-15 - 10:10:49 PM GMT
-  Email viewed by Alex Tan (alex.tan@paya.com)  
2023-12-16 - 10:44:20 PM GMT- IP address: 162.206.225.33
-  Document e-signed by Alex Tan (alex.tan@paya.com)  
Signature Date: 2023-12-16 - 10:44:47 PM GMT - Time Source: server- IP address: 162.206.225.33
-  Agreement completed.  
2023-12-16 - 10:44:47 PM GMT