



# Payment Card Industry (PCI) Data Security Standard

---

## Attestation of Compliance for Onsite Assessments – Service Providers

**Version 3.2.1**

Revision 2

September 2022

## Document Changes

Date	Version	Description
September 2022	3.2.1 Revision 2	Updated to reflect the inclusion of UnionPay as a Participating Payment Brand.

## 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:	Amber Innovations	DBA (doing business as):	AmberPay		
Contact Name:	Ekaterina Savadia	Title:	Director		
Telephone:	1-876-818-60-70	E-mail:	ekaterina@myambergroup.com		
Business Address:	Suite B11, Pinnacle Pointe, 53 Lady Musgrave Rd	City:	Kingston		
State/Province:		Country:	Jamaica.	Zip:	
URL:	<a href="https://www.myamberinnovations.com/">https://www.myamberinnovations.com/</a>				

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

Company Name:	Panacea Infosec (P) Ltd.				
Lead QSA Contact Name:	Raghendra Shukla	Title:	QSA		
Telephone:	+91 8929627083	E-mail:	raghvendra@panaceainfosec.com		
Business Address:	Plot no-226, 3rd Floor, A-2, Sector - 17 Dwarka	City:	New Delhi		
State/Province:	Delhi	Country:	India	Zip:	110075
URL:	<a href="https://www.panaceainfosec.com">https://www.panaceainfosec.com</a>				

## 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: Payment Aggregator

Type of service(s) assessed:

#### Hosting Provider:

- Applications / software
- Hardware
- Infrastructure / Network
- Physical space (co-location)
- Storage
- Web
- Security services
- 3-D Secure Hosting Provider
- Shared Hosting Provider
- Other Hosting (specify):

#### Managed Services (specify):

- Systems security services
- IT support
- Physical security
- Terminal Management System
- Other services (specify):

#### Payment Processing:

- POS / 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): Not Applicable

**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:

**Hosting Provider:**

- Applications / software
- Hardware
- Infrastructure / Network
- Physical space (co-location)
- Storage
- Web
- Security services
- 3-D Secure Hosting Provider
- Shared Hosting Provider
- Other Hosting (specify):

**Managed Services (specify):**

- Systems security services
- IT support
- Physical security
- Terminal Management System
- Other services (specify):

**Payment Processing:**

- POS / card present
- Internet / e-commerce
- MOTO / Call Center
- ATM
- 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

**Part 2b. Description of Payment Card Business**

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.

Amber Innovations is a payment aggregator facilitating payment related services to merchants across Caribbean islands. Entity has hosted the entire infrastructure using AWS cloud services which is a PCI DSS compliant entity.

CHD Transmission and Processing:

AmberPay as per their business process provides APIs to its merchant which will be integrated to their payment page and transmits card values. Paygoal receives the cardholder data comprising of PAN, Expiry date, cardholder name and CVV as a part of payment transactions from the merchants over TLS 1.2 through e-link, QR code and submit button embedded on merchants which re-directs the customer to e-link page. The message received from merchants is also encrypted using AES 128-bit encryption through their API application (<https://elink-payment.myamberpay.com/gateway/v1/standard-checkout>) and forwards it to third party payment service provider for further processing.

AmberPay is not directly involved in card data processing as it receives the card data and directly forward it to third party service providers for any further processing.

AmberPay is also having e-Stores application which is provided to merchants for account management where customer can perform the payment for the services opted using card details. Customer is re-directed to e-link application for payment.

CHD Storage:

AmberPay do not store any cardholder data in its PCI in-scope environment. Entity only stores First six and last 4 digits of PAN and token received from third payment processor for chargeback, reconciliation related activities and recurring transactions in internal database and transaction logs. The token cannot be decrypted to get the full card number.

AmberPay acts as payment aggregator required to facilitate the merchant while providing API integration and seamless connectivity with payment processors. This process requires AmberPay to transmit the card data and for respective back-office services last 4 digits are getting stored. AmberPay facilitates the back-office services like settlement and chargeback to the payment processor by providing relevant information of the transaction with the help of last 4 digits of PAN. This is the only reason AmberPay

	<p>needs to store the First six and last 4 digits of card holder data. AmberPay also stores token of the card number received from third party payment processor. The token cannot be decrypted to get the full card number.</p> <p>AmberPay is not directly involved in card data processing as it receives the card data and directly forwards it to a third-party payment service provider for any further processing.</p>
<p>Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.</p>	<p>will be integrated to their payment page and transmits card values. Paygoal receives the cardholder data comprising of PAN, Expiry date, cardholder name and CVV as a part of payment transactions from the merchants over TLS 1.2 through e-link, QR code and submit button embedded on merchants which re-directs the customer to e-link page. The message received from merchants is also encrypted using AES 128-bit encryption through their API application (<a href="https://elink-payment.myamberpay.com/gateway/v1/standard-checkout">https://elink-payment.myamberpay.com/gateway/v1/standard-checkout</a>) and forwards it to third party payment service provider for further processing.</p> <p>AmberPay is not directly involved in card data processing as it receives the card data and directly forward it to third party service providers for any further processing and does not perform the storage of cardholder data.</p> <p>Hence, AmberPay is having minimal capacity to impact the security of cardholder data.</p>

**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>
Corporate Office	1	Suite B11, Pinnacle Pointe, 53 Lady Musgrave Rd, Kingston 10, Jamaica.
AWS data center	1	North Virginia, USA



### 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)
E-store Application	v1.0	Not Applicable	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	Not Applicable
E-link Application	v1.0	Not Applicable	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	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	

### 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.*

The assessment covered the following technologies :-

- Application
- Database
- AWS IAM Console
- Network Security Groups
- Server
- Wazuh (SIEM and FIM)
- Antivirus Application (ClamAV)

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:

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:
Amazon Web Services	Cloud Hosting Services
First Atlantic Commerce	Payment Processing

**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:		Payment Aggregator		
PCI DSS Requirement	Details of Requirements Assessed			Justification for Approach <small>(Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)</small>
	Full	Partial	None	
Requirement 1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p><b>Req 1.2.3 is not applicable as there are no wireless networks in the scoped environment.</b></p> <p><b>Req 1.3.6 is not applicable as cardholder data is not stored in the scoped environment.</b></p>
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p><b>Req 2.1.1 is not applicable as there are no wireless networks in the scoped environment.</b></p> <p><b>Req 2.2.3 is not applicable as there are no insecure services present in the scoped environment.</b></p> <p><b>Req 2.6 is not applicable as entity is not a shared hosting provider.</b></p>
Requirement 3:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p><b>Req 3.1, 3.4, 3.5, 3.5.1, 3.5.3, 3.5.4, 3.6, 3.6.1, 3.6.2, 3.6.3, 3.6.4, 3.6.5, 3.6.6, 3.6.7 and 3.6.8 are not applicable as cardholder data is not stored in the scoped environment.</b></p>
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p><b>Req 4.1.1 is not applicable as cardholder data is not transmitted over wireless channel.</b></p>
Requirement 5:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p><b>Req 5.1.2 is not applicable as there are no systems which are not considered to be commonly affected by malicious software.</b></p>
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"/>	<p>Req 8.1.5 is not applicable as there are no service providers accessing scoped environment.</p> <p>Req 8.5.1 is not applicable as there are entity does not take remote access to customer premises.</p> <p>Req 8.7 is not applicable as there are no databases storing cardholder data.</p>
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>Req 9.5, 9.5.1 are not applicable as AmberPay scoped environment does not use any removable media for backing up any cardholder data. Hence the control is not applicable.</p> <p>Req 9.6, 9.7 (including all sub requirement) are not applicable as AmberPay scoped environment does not use any removable media for backing up any cardholder data. Hence the control is not applicable.</p> <p>Req 9.8 (including all sub requirement) are not applicable as AmberPay scoped environment does not use any removable media including CDs, DVDs, Tapes, USB, paper receipt, paper reports, and faxes for storing any data from cardholder data environment. Hence this requirement is not applicable</p> <p>Req 9.9, 9.9.1, 9.9.1. a, 9.9.1.b, 9.9.1.c, 9.9.2, 9.9.2.a, 9.9.2.b, 9.9.3, 9.9.3.a, 9.9.3.b are not applicable as there is no POS in AmberPay scoped environment PCI DSS environment, hence this requirement is not applicable.</p>
Requirement 10:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Req 10.2.1 is not applicable as cardholder data is not stored in the scoped environment.
Requirement 11:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 12:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Req 12.3.9 is not applicable as there are no service providers taking remote access to scoped environment.
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Appendix A1 is not applicable as entity is not a shared hosting provider.
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<p>A2.1 is not applicable as entity does not have POS terminals in its environment. Hence this requirement is not applicable.</p> <p>A2.2 is not applicable as entity does not use any SSL or early TLS protocol in the environment. Hence, this requirement is not applicable.</p> <p>A2.3 is not applicable as entity does not have any POS/POI offering service and also does not provide any insecure IT services hence the requirement is not applicable.</p>

## 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:	<i>3<sup>rd</sup> December 2022</i>	
Have compensating controls been used to meet any requirement in the ROC?	<input checked="" type="checkbox"/> Yes	<input 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 (3<sup>rd</sup> December 2022).

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>Amber Innovations</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%; border-collapse: collapse;"> <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</i> , Version (3.2.1), 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 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, CVN2, CVV2, or CID 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>Panacea InfoSec Pvt. Ltd.</i> )

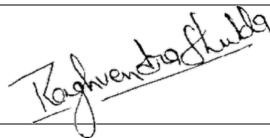
**Part 3b. Service Provider Attestation**



Signature of Service Provider Executive Officer ↑	Date: 3 <sup>rd</sup> December 2022
Service Provider Executive Officer Name: Ekaterina Savadia	Title: Director

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

If a QSA was involved or assisted with this assessment, describe the role performed:	QSA performed the assessment against the PCI DSS 3.2.1 standard at the assessed entity and documented the findings in the report on compliance.
--	---



Signature of Duly Authorized Officer of QSA Company ↑	Date: 3 <sup>rd</sup> December 2022
Duly Authorized Officer Name: Raghvendra Shukla	QSA Company: Panacea Infosec Pvt. Ltd.

**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 checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems against malware and regularly update anti-virus software or programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify and authenticate access to system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10	Track and monitor all access to network resources and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	<input checked="" 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 checked="" type="checkbox"/>	<input type="checkbox"/>	

