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: Amber Innovations

Date of Report as noted in the Report on Compliance: 5th December 2025

Date Assessment Ended: 4th December 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:	Amber Innovations
DBA (doing business as):	AmberPay
Company mailing address:	Amber Innovations, 5th Floor, 13 Haining Road, Kingston 5,Jamaica
Company main website:	https://www.myamberinnovations.com/
Company contact name:	Sellva Manoj D S
Company contact title:	Chief Information Security Officer
Contact phone number:	+919940983622
Contact e-mail address:	sellva@myambergroup.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:	Panacea InfoSec Pvt. Ltd.
Company mailing address:	3rd Floor, Plot No. 226, A-2, Sector 17, Dwarka, New Delhi-110075, India
Company website:	www.panaceainfosec.com
Lead Assessor name:	Raghvendra Shukla
Assessor phone number:	+91-8929627083
Assessor e-mail address:	raghvendra@panaceainfosec.com
Assessor certificate number:	QSA (206-005), S-SLC Assessor (1600-137), Secure Software Assessor (1500-131)

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were <u>INCLUDED</u> in the scope of the Assessment (select all that apply):

Name of service(s) assessed:	Payment Aggregator and Managed White Label Solution Provider

Type of service(s) assessed:

Hosting Provider:	Managed Services:	Payment Processing:
☒ Applications / software	☐ Systems security services	☐ POI / card present
☐ Hardware	☐ IT support	☒ Internet / e-commerce
☒ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web-hosting services		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Multi-Tenant Service Provider		
☐ Other Hosting (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 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 <u>NOT INCLUDED</u> in the scope of the Assessment (select all that apply):

Name of service(s) not assessed:	Not Applicable

Type of service(s) not assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POI / card present
☐ Hardware	☐ IT support	☐ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web-hosting services		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Multi-Tenant Service Provider		
☐ Other Hosting (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):

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

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

Describe how the business stores, processes, and/or transmits account data.	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 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 by decrypted to get the full card number.
	Amberpay as a part of white label solution offering to payment partners receives cardholder data and CVV from their merchants and transmit the same to third party service providers opted by customers for further payment processing.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Amber Innovations is a payment aggregator facilitating payment related services to merchants across Carribean 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. Entity 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 hosts a white label solution which is offered to various business partners as complete package for their payment processing needs. Entity develops and manages the white label entirely and perform changes to the application as per client need. Clients cannot perform code level as well as any functionality level changes. However, they do have access to perform administrative changes on the portal provided to them for performing their day-to-day activities. Clients opting for white label solution are responsible for onboarding their third-party service providers for payment processing and apply appropriate configuration on Amber provided portal for performing live transactions. Entity receives transaction authorization request from merchants onboarded by over secure encrypted web channel i.e utilization of TLS 1.3 CA certificate along with AES 128-bit encryption algorithm and transmits the payment data consisting of PAN, expiry date, cardholder name and CVV to third party service providers for further processing as opted by customers.
	Amber 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.

	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 by decrypted to get the full card number.
Describe system components that could impact the security of account data.	System components within the CDE that could impact the security of account data: ● Network Security Controls (NSCs) ● EC2 instances ● RDS databases ● AWS Services AWS Services ● Amazon CloudWatch ● Amazon EC2 (AL2) ● Amazon Elastic Container Service (ECS) ● Amazon RDS ● DNS Firewall ● Amazon Simple Storage Service (S3) ● Amazon Virtual Private Cloud (VPC) ● AWS WAF ● AWS Shield ● AWS CloudTrail ● IAM Support Systems ● Multi-factor authentication ● Access Authorization ● Change Management ● File Integrity Monitoring ● Intrusion Detection Systems ● Logging and Alerting ● External ASV Scanning ● Penetration Testing ● Software/Code Deployment Pipeline

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.*	The assessment covered the following technologies :- • Application • Database • AWS IAM Console • Network Security Groups • DNS Firewall • Server • Wazuh (SIEM and FIM) • Antivirus Application (ClamAV)

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*
Corporate Office	1	Amber Innovations, 5th Floor, 13 Haining Road, Kingston 5,Jamaica
AWS Data Center	1	North Virginia, USA

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
				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:

• 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))	☒ Yes ☐ 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)	☒ Yes ☐ No
• Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).	☐ Yes ☒ No

If Yes:

Name of Service Provider:	Description of Services Provided:
Amazon Web Services, Inc.	Cloud hosting services
Powertranz LTD	Payment Processing

Note: Requirement 12.8 applies to all entities in this list.

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment (ROC Section 1.8.1)

Indicate below all responses provided within each principal PCI DSS requirement.

For all requirements identified as either "Not Applicable" or "Not Tested," complete the "Justification for Approach" table below.

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

Name of Service Assessed: Payment Aggregator and Managed White Label Solution Provider

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:	☒	☒	☐	☐	☐
Requirement 2:	☒	☒	☐	☐	☐
Requirement 3:	☒	☒	☐	☐	☐
Requirement 4:	☒	☒	☐	☐	☐
Requirement 5:	☒	☒	☐	☐	☐
Requirement 6:	☒	☒	☐	☐	☐
Requirement 7:	☒	☐	☐	☐	☐
Requirement 8:	☒	☒	☐	☐	☒
Requirement 9:	☒	☒	☐	☐	☐
Requirement 10:	☒	☐	☐	☐	☐
Requirement 11:	☒	☒	☐	☐	☐
Requirement 12:	☒	☒	☐	☐	☐
Appendix A1:	☐	☒	☐	☐	☐
Appendix A2:	☐	☒	☐	☐	☐

Justification for Approach

	Requirement 1:
	1.2.6- Not Applicable as there is no services protocols and ports are in use which is considered to be insecure.
	1.3.3 - Not Applicable as wireless network is not present in scoped environment.
	Requirement 2:
	2.2.5- Not Applicable as "Amber Innovations" doesn't utilize any insecure services across the scoped environment.
	2.3.1- Not Applicable as wireless network is not present in scoped environment.
	2.3.2- Not Applicable as wireless network is not present in scoped environment.
	Requirement 3:
	3.2.1- Not applicable as cardholder data is not stored in the scoped environment.
	3.3.1- Not Applicable as SAD is not retained after authorization
	3.3.2- Not Applicable as SAD is not stored post authorization.
For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	3.3.3- Not Applicable as Amber Innovations does not support the Issuing services.
	3.4.1- Not applicable as cardholder data is not stored in the scoped environment.
	3.4.2- Not applicable, as Amber Innovations does not support the copying and/or relocation of PAN for all personnel when using remote-access technologies.
	3.5.1- Not applicable as cardholder data is not stored in the scoped environment.
	3.5.1.1- Not applicable as there is no Hashes used to render PAN unreadable in scoped environment.
	3.5.1.2- Not applicable as there is no removable media in scoped environment.
	3.5.1.3-Not Applicable as disk encryption is not used in the "Amber Innovations" scoped environment.
	3.6.1, 3.6.1.1, 3.6.1.2, 3.7.1, 3.7.2, 3.7.3, 3.7.4, 3.7.5, 3.7.7, 3.7.8 - Not applicable as cardholder data is not stored in the scoped environment.
	3.6.1.3- Not Applicable as there is no cleartext key in the scoped environment.
	3.6.1.4- Not applicable as cardholder data is not stored in the scoped environment.

3.7.6- Not applicable as manual clear text cryptography is not utilized.

3.7.9- Not Applicable as Amber Innovations does not share any cryptographic keys with customer.

Requirement 4:

4.2.1.2- Not Applicable as wireless network is not present in scoped environment.

4.2.2- Not Applicable as PAN is not transmitted over end-user messaging technologies.

Requirement 5:

5.2.3- Not applicable as there are no systems considered to be not commonly affected by malicious software.

5.2.3.1- Not applicable as there are no systems components that considered to be not commonly affected by malicious software.

5.3.3- Not Applicable as removal media is not acceptable in "Amber Innovations" environment.

Requirement 6:

6.5.2- Not applicable as there are no significant changes.

Requirement 8:

8.2.3- Not applicable as entity is not having access to customer's environment.

8.2.7- Not applicable as there are no third parties having access to scoped environment.

8.4.3- Not applicable as there are no users accessing entity's environment from outside the entity's network.

8.6.1, 8.6.2- Not Applicable as interactive login to the systems is not scoped in entity's network.

Requirement 9:

9.2.3- Not Applicable as wireless network is not present in scoped environment.

9.4.1, 9.4.1.1, 9.4.1.2, 9.4.2, 9.4.3, 9.4.4, 9.4.5, 9.4.5.1, 9.4.6, 9.4.7- Not Applicable as there is no media in the scoped environment.

9.5.1, 9.5.1.1, 9.5.1.2, 9.5.1.2.1, 9.5.1.3: Not Applicable as there are no POI devices in the scoped environment.

Requirement 11:

	11.2.2: Not applicable as there is no wireless network in the scoped environment.
	11.3.1.3: Not applicable as there has been no significant change in the scoped environment.
	11.3.2.1: Not applicable as there has been no significant change.
	11.4.7: Not applicable as entity is not a multi-tenant service provider.
	Requirement 12:
	12.3.2: Not Applicable as customized approach is not used for any of the requirements.
	Appendix A1: Not applicable as entity is not a multi-tenant service provider.
	Appendix A2: Not applicable as entity is not a multi-tenant service provider.
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: **Note:** *This is the first date that evidence was gathered, or observations were made.*	2025-11-17
Date Assessment ended: **Note:** *This is the last date that evidence was gathered, or observations were made.*	2025-12-04
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes ☒ No
Were any testing activities performed remotely?	☒ Yes ☐ 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 *(Date of Report as noted in the ROC 2025-12-05)*.

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

☒ **Full Assessment** – All requirements have been assessed and therefore no requirements were marked as Not Tested in the ROC.

☐ **Partial Assessment** – One or more requirements have not been assessed and were therefore marked as Not Tested in the ROC. Any requirement not assessed is noted as Not Tested in Part 2g above.

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

☒	**Compliant:** All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT** rating; thereby *(Amber Innovations)* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating; thereby *(Service Provider Company Name)* has not demonstrated compliance with PCI DSS requirements. **Target Date** for Compliance: *YYYY-MM-DD* An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4.
☐	**Compliant but with Legal exception:** One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *(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. This option requires additional review from the entity to which this AOC will be submitted. *If selected, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement from being met

Part 3. PCI DSS Validation *(continued)*

Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:

(Select all that apply)

☒	The ROC was completed according to *PCI DSS*, Version 4.0.1 and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
☒	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑ | Date: 2025-12-05
Service Provider Executive Officer Name: Sellva Manoj D S | Title: Chief Information 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: PCI DSS v4.0.1 Compliance Assessment and Attestation along with evidence collection and validation, ROC and AOC writing.

Signature of Lead QSA ↑ | Date: 2025-12-05
Lead QSA Name: Raghvendra Shukla |

Signature of Duly Authorized Officer of QSA Company ↑ | Date: 2025-12-05
Duly Authorized Officer Name: Himanshu Mishra | QSA Company: Panacea Infosec Pvt Ltd.

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

If an ISA(s) was involved or assisted with this Assessment, indicate the role performed:	☐ 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	☐	☐	
2	Apply secure configurations to all system components	☐	☐	
3	Protect stored account data	☐	☐	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	☐	☐	
5	Protect all systems and networks from malicious software	☐	☐	
6	Develop and maintain secure systems and software	☐	☐	
7	Restrict access to system components and cardholder data by business need to know	☐	☐	
8	Identify users and authenticate access to system components	☐	☐	
9	Restrict physical access to cardholder data	☐	☐	
10	Log and monitor all access to system components and cardholder data	☐	☐	
11	Test security systems and networks regularly	☐	☐	
12	Support information security with organizational policies and programs	☐	☐	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	☐	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☐	☐	

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/