PCI Security Standards Council®

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:	Innovins Technologies Pvt Ltd		DBA (doing business as):	Innovins	
Contact Name:	Mr. Suhas Jadhav		Title:	CEO	
Telephone:	+91-9930034418		E-mail:	suhas@chargemonk.com	
Business Address:	503, 5th Floor, Advent Atria, Chincholi Bunder Road, Off S.V Road , Malad (West)		City:	Mumbai	
State/Province:	Maharashtra	Country:	India	Zip:	400064
URL:	https://www.chargemonk.com/				

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

Company Name:	SISA				
Lead QSA Contact Name:	Ms. Sonali Samantaray		Title:	Associate Consultant	
Telephone:	+91-7625072467		E-mail:	sonali.samantaray@sisainfosec.com	
Business Address:	SISA House, No.3029B, Sri Sai Darshan Marg,13th Main Road, HAL II Stage, Indiranagar.		City:	Bangalore	
State/Province:	Karnataka	Country:	India	Zip:	560008
URL:	https://sisainfosec.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:	ChargeMonk Application Module	
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): N/A	**Managed Services (specify):** □ Systems security services □ IT support □ Physical security □ Terminal Management System □ Other services (specify): N/A	**Payment Processing:** □ POS / card present ☒ Internet / e-commerce □ MOTO / Call Center □ ATM □ Other processing (specify): N/A
□ 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): N/A		

***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:	N/A

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):

N/A

Managed Services (specify):

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

N/A

Payment Processing:

□ POS / card present
□ Internet / e-commerce
□ MOTO / Call Center
□ ATM
□ Other processing (specify):

N/A

□ 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): N/A		

Provide a brief explanation why any checked services were not included in the assessment:	N/A

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Chargemonk acquires cardholder data (Cardholder's Name, PAN, Expiry and CVV) and PII data through its custom API or payment page. It is integrated with Spreedly- a third party receiver to transmit cardholder data through HTTPS over TLS v1.2 for processing and then sends back the result of the transaction to the end user. End Customers create a subscription on Chargemonk website for subscription services from different merchants. Spreedly is responsible to add merchant's payment gateway and it provides gateway token to Chargemonk for future card processing. Further, Chargemonk adds customer's card to Spreedly for making payments and for future processing of cards for subscription payments which in return provides payment token back to Chargemonk. Using this token, Chargemonk applies a charge on the customer's card whenever the subscription due is pending. Chargemonk does not store any card details of the end customers. The third party receiver - Spreedly sends request to payment gateway to deduct any charge from customer's card. Innovins does not store or process CHD in their environment.They only collect CHD from the end customer over their application Chargemonk and transmit the CHD (PAN, Expiry and CVV) to the third party receivers for further processing.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	N/A

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):
Example: Retail outlets	*3*	*Boston, MA, USA*
Corporate Office	1	Mumbai, Maharashtra, india
AWS Data Center	1	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)
Chargemonk	v1.0	In-house	☐ Yes ☒ No	Not Applicable
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ 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.*	Innovins Technologies Pvt. Ltd. (henceforth referred to as Innovins) provides recurring subscription management system services to customers seeking to accept electronic forms of payment for the exchange of services through ChargeMonk application that emphasizes on optimizing subscription of customers along with enhancing their recurring revenue. Details like PII and cardholder is collected and passed through to the third party receivers i.e. Spreedly which in turn passes it to the payment gateway for authorization and acceptance. The resilient plan management options of ChargeMonk intends to fulfill a variety of business requirements and support several payment and billing plans within a single dashboard. Hence, facilitates you to achieve the wide spectrum of potential customers. In other words, it manages subscriptions at scale, automates recurring billing, and access metrics that matter. Chargemonk is a recurring subscription management system. It is designed in such a way that merchant can make informed decisions by protecting the interest of customers. Charge monk's subscription model allows merchants to modify their product or

	services and pricing plans from a single dashboard. In the recurring revenue businesses, this will implement and manage the pricing changes of merchant smoothly. The critical technologies are as follows: - IPsec VPN: VPN Tunnel created from the corporate VLAN to AWS. - AWS Instances : All the technical infrastructure was hosted on AWS - Security Group: Acts as a virtual firewall - Clam AV – Antivirus Solution - Cloud Watch - Log Monitoring solution - Google Authenticator- Multi factor Authentication - Surikata-IDS solution

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:	N/A
QIR Individual Name:	N/A
Description of services provided by QIR:	N/A

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 Service	Infrastructure Service Provider (Data Center)
Spreedly	Third Party Service 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:	ChargeMonk Application Module			
PCI DSS Requirement	**Details of Requirements Assessed**			
	Full	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Requirement 1:	□	☒	□	Req 1.2.2 is not applicable as routers were not a part of the current PCI-DSS scope of the assessed entity. Req 1.2.3 is not applicable as no wireless network was present in the assessed entity's environment Requirement 1.3.6 is not applicable as the entity does not store any CHD.
Requirement 2:	□	☒	□	Req 2.1.1 is not applicable as wireless environment is not present in the assessed entity's PCI-DSS scope environment. Req 2.2.3 is not applicable as insecure services, protocols or daemons were not configured in the PCI-DSS scope. Req 2.3 is not applicable as there is no non console access into the PCI Scoped environment Req 2.6 is not applicable as the assessed entity is not a shared hosting provider.
Requirement 3:	□	☒	□	Req 3.1 is not applicable as CHD is not being stored by the assessed entity. Req 3.2 is not applicable as Sensitive Authentication Data is not received by the assessed entity.

				Requirement 3.3 is not applicable as the entity is not involved in masking of the PAN Req 3.4 is not applicable as the assessed entity does not store CHD Req 3.4.1 are not applicable as no disk encryption has been used in the entity's environment. Req 3.5, 3.5.1, 3.5.2, 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, 3.6.8 are not applicable as no CHD is stored in the scope
Requirement 4:	☐	☒	☐	Req 4.1.1 is not applicable as there are no wireless networks transmitting cardholder data or connected to the cardholder data environment.
Requirement 5:	☐	☒	☐	Req 5.1.2 is not applicable as all systems have Clam AV is installed and running
Requirement 6:	☐	☒	☐	Req 6.4.6 is not applicable as there is no significant change from the last 12 months.
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	Req 8.1.3 is not applicable as none of the users got terminated in the last 6 months Req 8.1.5 is not applicable as there are no vendor accounts in place. Re 8.3.1 is not applicable as there is no non console access into the PCI Scoped environment Req 8.5.1 is not applicable as personnel from Innovins doesn't access customer environment. Req 8.7 is not applicable as Card numbers (PAN) are not stored in the assessed entity's environment.
Requirement 9:	☐	☐	☒	All the requirements were marked as not applicable as all the system components are being hosted in AWS and it's the responsibility of AWS to maintain the security which was confirmed by reviewing AWS AOC dated 27-Mar-2019
Requirement 10:	☒	☐	☐	
Requirement 11:	☐	☒	☐	Req 11.1.1 and 11.1.2 are not applicable as the whole infrastructure is hosted over AWS so no CHD is being processed or transmitted over Wireless network connections. Req 11.2.3 is not applicable as verified by observation of state that no significant infrastructure or application upgrade or modification occurred during the past 12 months.

				Req 11.3.3 is not applicable as verified by review of External PT Report and Internal PT Report that exploitable vulnerabilities were not found during penetration test. Req 11.3.4 and 11.3.4.1 are not applicable as the entire network of Innovins is assessed as a part of PCI-DSS scope and no segmentation has been done.
Requirement 12:	☐	☒	☐	Req 12.3.9 is not applicable as remote access is not provided to any vendor or business partner. Req 12.3.10 is not applicable as Innovins personnel cannot access cardholder data via remote access technologies.
Appendix A1:	☐	☐	☒	Appendix A1 was not applicable as the assessed entity is not a shared hosting provider.
Appendix A2:	☐	☐	☒	Appendix A2 was not applicable as the assessed entity is not using SSL/early TLS.

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:	29th January 2020	
Have compensating controls been used to meet any requirement in the ROC?	☐ Yes	☒ No
Were any requirements in the ROC identified as being not applicable (N/A)?	☒ Yes	☐ No
Were any requirements not tested?	☐ Yes	☒ No
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes	☒ No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated 29th January 2020***.***

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):***

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby Innovins Technologies Pvt Ltd. has demonstrated full compliance with the PCI DSS.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby N/A has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: N/A 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. *Check with the payment brand(s) before completing Part 4.*
☐	**Compliant but with Legal exception:** 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. *If checked, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement being met
N/A	N/A

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

☒	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version 3.2.1, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
☐	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
☒	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
☒	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)

☒	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☒	ASV scans are being completed by the PCI SSC Approved Scanning Vendor SISA

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	*Date:* 17/2/2020
Service Provider Executive Officer Name: **Mr. Suhas Jadhav**	*Title:* **CEO**

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

If a QSA was involved or assisted with this assessment, describe the role performed:	PCI-DSS v3.2.1 Gap Assessment and Consulting

Sonali Samantaray

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* 17/2/2020
Duly Authorized Officer Name: Ms. Sonali Samantaray	*QSA Company:* SISA

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:	N/A

[1] 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.

[2] 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.

[3] 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	☒	☐	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	☐	
3	Protect stored cardholder data	☒	☐	
4	Encrypt transmission of cardholder data across open, public networks	☒	☐	
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	☐	
6	Develop and maintain secure systems and applications	☒	☐	
7	Restrict access to cardholder data by business need to know	☒	☐	
8	Identify and authenticate access to system components	☒	☐	
9	Restrict physical access to cardholder data	☒	☐	
10	Track and monitor all access to network resources and cardholder data	☒	☐	
11	Regularly test security systems and processes	☒	☐	
12	Maintain a policy that addresses information security for all personnel	☒	☐	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	☐	☐	N/A
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☐	☐	N/A