



# **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:	Magpie.IM Inc.	DBA (doing business as):	Magpie.IM		
Contact Name:	Dominick Nowell A. Danao	Title:	Chief Executive Officer		
Telephone:	+639178180020	E-mail:	dom@magpie.im		
Business Address:	3F Valero Plaza Condominium, Valero Street	City:	Makati City		
State/Province:	Metro Manila	Country:	Philippines	Zip:	1200
URL:	https://magpie.im				

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

Company Name:	GlobalTech & Infosec Pvt Ltd				
Lead QSA Contact Name:	Nishikant Singh	Title:	Director Information Security		
Telephone:	+91 9818398494	E-mail:	nishikant@gtisec.com		
Business Address:	1136, Pocket 3 Sector 19	City:	Dwarka		
State/Province:	New Delhi	Country:	India	Zip:	110075
URL:	www.gtisec.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: api.magpie.im & checkout.magpie.im

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):

**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: NONE

Type of service(s) not assessed:

<b>Hosting Provider:</b>	<b>Managed Services (specify):</b>	<b>Payment Processing:</b>
<input type="checkbox"/> Applications / software	<input type="checkbox"/> Systems security services	<input type="checkbox"/> POS / card present
<input type="checkbox"/> Hardware	<input type="checkbox"/> IT support	<input type="checkbox"/> Internet / e-commerce
<input type="checkbox"/> Infrastructure / Network	<input type="checkbox"/> Physical security	<input type="checkbox"/> MOTO / Call Center
<input type="checkbox"/> Physical space (co-location)	<input type="checkbox"/> Terminal Management System	<input type="checkbox"/> ATM
<input type="checkbox"/> Storage	<input type="checkbox"/> Other services (specify):	<input type="checkbox"/> Other processing (specify):
<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):		
<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**

<p>Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.</p>	<p>Magpie.IM Inc. allows its customer merchants to collect card payments by presenting and serving a payment form (checkout) to merchants' clients and tokenizing card information so that merchants can safely make charges. Magpie uses Spreedly tokenization solution for all Credit Card storage. Spreedly is a PCI Level 1 Service Provider, the highest level of PCI DSS certification.</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>Magpie.IM takes PAN and CVV information in behalf of the merchants, which are immediately sent to its tokenization and payment account vault service. No PAN or CVV information is logged or retained in Magpie.IM's systems. Magpie uses Spreedly tokenization solution for all Credit Card storage. Spreedly is a PCI Level 1 Service</p>

Provider, the highest level of PCI DSS certification.

### 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	Makati City, Philippines

### 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)
			<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.*

This assessment covered the Magpie core gateway, which accepts cardholder data on behalf of merchant customers via two methods: the checkout service (a drop-in payment acceptance form), and via API.

Magpie.IM accepts PAN data from merchant customers via API or via web form at checkout.magpie.im, after which data is sent directly to its tokenization and vault service (Spredly). A token is returned to Magpie, and Magpie returns its version of the token to the merchant. The merchant

may make charges against the payment token via API calls.

When payment charges are made, Magpie accepts the calls (tokenized and free from PAN and CVV information), and send it off to Spreedly, which in turn makes outbound connections to payment processors to facilitate authorization and settlement.

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 Service	Hosting services
Spredly Inc.	Payment card tokenization and vaulting

**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:		Details of Requirements Assessed		
PCI DSS Requirement	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:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>Magpie is using AWS Cloud Service provider for hosting services, ITS PCIDSS Certified hosting service provider.</p> <p>1.2.2 – Magpie does not implement and manage any router. Hence, this requirement is not applicable.</p> <p>1.2.3 – No wireless network exists in the Magpie. Hence, this requirement is not applicable.</p> <p>1.3.6 – Magpie network does not store any cardholder data, they process all credit card information to PCIDSS Certified tokenization solution provider (Spreadley). Hence, this requirement is not applicable.</p> <p>1.4 – There are no portable devices in the Magpie environment which are used to access to CDE segment from outside. Hence, this requirement is not applicable.</p>
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>Magpie is using AWS Cloud service provider Platform as a services for entire application environment.</p> <p>2.1.1 – No wireless network exists in Magpie environment. Hence, this requirement is not applicable.</p>



				<p>2.2.1.b – No virtualization technologies are used. Hence, this requirement is not applicable.</p> <p>2.6 – Magpie is not a shared hosting provider. Hence, this requirement is not applicable.</p>
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>Magpie is not storing Credit Card information.</p> <p>3.1, 3.4, 3.5, 3.6, 3.7-- Magpie does not store cardholder data. Hence, this requirement is not applicable.</p> <p>3.2—Magpie neither receives nor store sensitive authentication data. Hence, this requirement is not applicable.</p> <p>3.3-- Magpie does not display full PAN or masked PAN on any application in their environment.</p>
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>4.1.1 –Magpie does not transmit cardholder data over the wireless network. Hence, this requirement is not applicable.</p> <p>4.2 – Magpie has no cardholder data which is transmitted over email, chat or messaging systems.</p>
Requirement 5:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>5.1.2 – There are no systems, which are considered commonly affected by malicious softwares. Hence, this requirement is not applicable.</p>
Requirement 6:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>6.3, 6.3.1, 6.3.2, 6.4, 6.4.1, 6.4.2, 6.4.3, 6.4.4 - Magpie environment does not involve any in house software development for any cardholder applications. Hence, these requirements are not applicable.</p> <p>6.4.6 – There is no significant change in the Magpie environment since last year. Hence, the requirement is not applicable.</p> <p>6.5, 6.5.1, 6.5.2, 6.5.3, 6.5.4, 6.5.5, 6.5.6, 6.5.7, 6.5.8, 6.5.9, 6.5.10 - Magpie environment does not involve any in house software development for any cardholder applications. Hence, these requirements are not applicable.</p> <p>6.6-There is no public facing card holder Applications in Magpie PCI DSS Scoped Environment. Hence, this requirement is not applicable.</p>
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>8.1.5 – Magpie does not allows remote access. Hence, this requirement is not applicable.</p>

				<p>8.3.1—Magpie there is no involvement of CHD in the assessed environment, hence this control is not applicable.</p> <p>8.3.2-- Remote access from outside the Magpie is not allowed to accessed AWS cloud. Hence, this requirement is not applicable.</p> <p>8.5.1-- Magpie does not connect to their customer environment for remote management. Hence, this requirement is not applicable.</p> <p>8.6 -- There was no other authentication mechanism used apart from password. Hence, this requirement is not applicable.</p> <p>8.7 -- There is no database containing cardholder data at Magpie. Hence, this requirement is not applicable.</p>
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>9.5, 9.5.1, 9.6, 9.6.1, 9.6.2, 9.6.3, 9.7, 9.7.1- No cardholder data is stored in backup media. Hence, these requirements are not applicable.</p> <p>9.8, 9.8.1, 9.8.2 --There is no media including computers, removable electronic media, paper receipts, paper reports, and faxes containing card data in the Magpie. Hence, these requirements are not applicable.</p> <p>9.9, 9.9.1-9.9.3 - No POS devices are in Magpie environment. Hence, these requirements are not applicable.</p>
Requirement 10:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>10.2.1-- Magpie does not store, process or transmit any cardholder data. Hence, this requirement is not applicable.</p>
Requirement 11:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>11.1.1 - No wireless network is present in Magpie environment. Hence, this requirement is not applicable</p>
Requirement 12:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>12.3.8-12.3.10 - No remote access in Magpie and from outside environment. Hence, these requirements are not applicable.</p> <p>12.8,12.8.1-12.8.5 - Magpie does not engage service providers with whom cardholder data is shared. Hence, these requirements are not applicable.</p>
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<p>Clavax Technologies is not a shared hosting provider</p>
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<p>Clavax Technologies does not support Early TLS/SSL versions.</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:	23rd October 2019
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 (23rd October 2019).

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>Service Provider Company Name</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</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 checked="" 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 (Qualys)

**Part 3b. Service Provider Attestation**



<i>Signature of Service Provider Executive Officer</i> ↑	<i>Date:</i> 7 November 2019
<i>Service Provider Executive Officer Name:</i> Dominick Danao	<i>Title:</i> CEO

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

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

<i>Signature of Duly Authorized Officer of QSA Company</i> ↑	<i>Date:</i> 23rd October 2019
<i>Duly Authorized Officer Name:</i> Nishikant Singh	<i>QSA Company:</i> GlobalTech & 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:	
---	--

<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 type="checkbox"/>	<input checked="" 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 checked="" type="checkbox"/>	

