



# **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:	MageMojo LLC	DBA (doing business as):	N/A		
Contact Name:	Martin Pachol	Title:	Chief Technology Officer		
Telephone:	800.217.8142 x502	E-mail:	martin@magemojo.com		
Business Address:	428 Forbes Ave	City:	Pittsburgh		
State/Province:	PA	Country:	USA	Zip:	15219
URL:	<a href="https://magemojo.com/">https://magemojo.com/</a>				

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

Company Name:	Schellman & Company, LLC				
Lead QSA Contact Name:	Phil Dorczuk	Title:	Manager		
Telephone:	866.254.0000 ext. 161	E-mail:	pciocs@schellman.com		
Business Address:	4010 W Boy Scout Boulevard, Suite 600	City:	Tampa		
State/Province:	FL	Country:	USA	Zip:	33607
URL:	<a href="https://www.schellman.com/pci-dss-validation">https://www.schellman.com/pci-dss-validation</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: STRATUS Magento as a Service

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: 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):

 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 Payment Card Business**

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

Not applicable. MageMojo does not process cardholder data in the scope of this assessment.

Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.

Cardholder data may be stored or transmitted on MageMojo-owned systems depending on how their customers have configured their web applications. MageMojo does not directly process cardholder data. Customers may choose to implement a connection from their Magento storefront, hosted with MageMojo, to a third-party payment gateway that stores, processes, or transmits cardholder data. Customers were solely responsible for the transmission, and storage of cardholder data for their storefronts hosted on the STRATUS MaaS offering.



## 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>
Amazon Web Services regions	Four (4)	ap-southeast-2, eu-central-1, eu-west-1, us-east-1

## Part 2d. Payment Applications

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

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

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
Not applicable.	Not applicable.	Not applicable.	<input type="checkbox"/> Yes <input 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.*

MageMojo is a Software as a Service (SaaS) provider founded in 2009. The service assessed is STRATUS Magento as a Service (MaaS) which provides Magento storefronts to customers. Magento is an open-source e-commerce application written in hypertext preprocessor (PHP) and distributed under Open Software License (OSL) v3.0. Magento is not the responsibility of MageMojo.

MageMojo is responsible for the architecture underlying its customer's Magento storefronts that run as Kubernetes deployments including the Kubernetes clusters, core underlying operating system, web, and database



	<p>containers on which customer Magento applications reside.</p> <p>All systems are hosted in AWS. AWS is responsible for the network (e.g., routing, switching), physical, and environmental security for the underlying virtualization management layer.</p>
<p>Does your business use network segmentation to affect the scope of your PCI DSS environment?</p> <p><i>(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)</i></p>	<p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p>



**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?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
---	---

**If Yes:**

Name of QIR Company:	Not applicable.
QIR Individual Name:	Not applicable.
Description of services provided by QIR:	Not applicable.

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?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
---	---

**If Yes:**

Name of service provider:	Description of services provided:
AWS	Cloud hosting services.

**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:** STRATUS Magento as a Service

PCI DSS Requirement	Details of Requirements Assessed			Justification for Approach (Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)
	Full	Partial	None	
Requirement 1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1.2.2: Not applicable. MageMojo did not utilize any routers connected to the cardholder data environment.
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2.1: Not applicable. Observed the hardware and software inventory and noted that there were no systems type or applications in the CDE that had default credentials from the vendor. 2.1.1: Not applicable. Observed VPC, network ACL, and security groups and network diagrams and noted that there were no wireless networks within or connected to the CDE.
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	3.1 - 3.2, 3.3 - 3.7: Not applicable. MageMojo did not store or access cardholder data. MageMojo’s customers were responsible for meeting this requirement.
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	4.1.1: Not applicable. Observed VPC, network ACL, and security groups and network diagrams and noted that there were no wireless networks within or connected to the CDE. 4.2: Not applicable. MageMojo did not directly receive or transmit cardholder data but rather provided the Magento application instances and underlying for their customer’s applications.
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	





Requirement 6:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>6.3 - 6.3.2: Not applicable. MageMojo did not develop applications in relation to the in-scope environment.</p> <p>6.4.1 - 6.4.4: Not applicable. MageMojo did not develop applications in relation to the in-scope environment.</p> <p>6.4.6 - 6.6: Not applicable. MageMojo did not develop applications in relation to the in-scope environment.</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: Not applicable. Observed user access lists for the in-scope systems and interviewed system administrators and noted that there were no vendor accounts present on systems.</p> <p>8.5.1: Not applicable. MageMojo did not have remote access to customer premises.</p> <p>8.7: Not applicable. MageMojo did not maintain any databases that stored cardholder data. MageMojo customers were responsible for meeting this requirement.</p>
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>9.5 - 9.8.2: Not applicable. Observed the listing of system components and network and data flow diagrams and interviewed the CTO and noted that all in-scope system components were cloud-hosted at AWS data centers and as such, MageMojo did not maintain any media containing cardholder data.</p> <p>9.9 - 9.9.3: Not applicable. Observed the listing of system components and network and data flow diagrams and interviewed the CTO and noted that all in-scope system components were cloud-hosted at AWS data centers and as such, MageMojo did not maintain any card-interaction devices.</p>
Requirement 10:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>10.2.1: Not applicable. MageMojo did not store cardholder data in relation to the in-scope environment.</p>
Requirement 11:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>11.2.3: Not applicable. Interviewed the CTO and observed a listing of changes made to in-scope systems and noted that no significant changes had occurred during the previous 12 months.</p> <p>11.3.4 - 11.3.4.1: Not applicable. Segmentation was not used.</p>
Requirement 12:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>12.3.9: Not applicable. Observed user access lists for the in-scope systems and interviewed system administrators and noted that there were no vendor accounts present on systems.</p> <p>12.3.10: Not applicable. MageMojo did not store or access cardholder data. MageMojo's customers were responsible for meeting this requirement.</p>
Appendix A1:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	



---

Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	There were no instances of early TLS observed in the environment.
--------------	--------------------------	--------------------------	-------------------------------------	---

---



## 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>June 9, 2021</i>
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 *June 9, 2021*.

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 MageMojo LLC 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 MageMojo LLC has not demonstrated full compliance with the PCI DSS.  
**Target Date** for Compliance: Not applicable.  
 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 |
|----------------------|--|
| Not applicable.      | Not applicable.  |
|                      |  |

### Part 3a. Acknowledgement of Status

Signatory(s) confirms:

*(Check all that apply)*

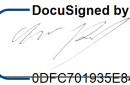

- The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures, Version 3.2.1*, and was completed according to the instructions therein.
- All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material 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)

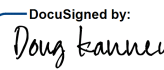

- |                                     |  |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | No evidence of full track data <sup>1</sup> , CAV2, CVC2, CID, or CVV2 data <sup>2</sup> , or PIN data <sup>3</sup> storage after transaction authorization was found on ANY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

### Part 3b. Service Provider Attestation

DocuSigned by: 	
0DFC701935E8421...	
Signature of Service Provider Executive Officer 	Date: 6/21/2021
Service Provider Executive Officer Name: <b>Martin Pachol</b>	Title: <b>Chief Technology Officer</b>

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

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

DocuSigned by: 	
E2B3593E0A364CA...	
Signature of Duly Authorized Officer of QSA Company 	Date: 6/21/2021
Duly Authorized Officer Name: Doug Kanney	QSA Company: Schellman & Company, LLC

### 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:	<i>Not applicable.</i>
--	------------------------

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

