



**Attestation of Compliance – Service Providers
Payment Card Industry (PCI)
Data Security Standard**

**Attestation of Compliance for
Onsite Assessments – Service Providers**

Version 2.0

October 2010

Instructions for Submission

The Qualified Security Assessor (QSA) and Service Provider must complete this document as a declaration of the Service Provider's compliance status with the Payment Card Industry Data Security Standard (PCI DSS). Complete all applicable sections and submit to the requesting payment brand.

Part 1. Service Provider and Qualified Security Assessor Information

Service Provider Organization Information

Company Name:	Magento	DBA(s):	None
Contact Name:	Kseniya Bulavko	Title:	Information Security Delivery Manager
Telephone:	408 967 7220	E-mail:	kseniya@x.com
Business Address:	10441 W. Jefferson Blvd. Suite 200	City:	Culver City
State/Province:	CA	Country:	US
		Zip:	90232
URL:	http://www.magento.com		

Qualified Security Assessor Company Information

Company Name:	Trustwave		
Lead QSA Contact Name:	James Jemison	Title:	Security Consultant
Telephone:	(214) 325-1917	E-mail:	jjemison@trustwave.com
Business Address:	70 West Madison Street, Suite 1050	City:	Chicago
State/Province:	IL	Country:	US
		Zip:	60602
URL:	http://www.trustwave.com		

Part 2 PCI DSS Assessment Information

Part 2a. Services Provided that WERE INCLUDED in the Scope of the PCI DSS Assessment (check all that apply)

<input checked="" type="checkbox"/> Payment Processing-POS	<input type="checkbox"/> Tax/Government Payments	<input type="checkbox"/> Fraud and Chargeback Services
<input type="checkbox"/> Payment Processing-Internet	<input type="checkbox"/> Payment Processing – ATM	<input type="checkbox"/> Payment Processing – MOTO
<input type="checkbox"/> Issuer Processing	<input checked="" type="checkbox"/> Payment Gateway/Switch	<input type="checkbox"/> Clearing and Settlement
<input type="checkbox"/> Account Management	<input type="checkbox"/> 3-D Secure Hosting Provider	<input type="checkbox"/> Loyalty Programs
<input type="checkbox"/> Back Office Services	<input type="checkbox"/> Prepaid Services	<input type="checkbox"/> Merchant Services
<input type="checkbox"/> Hosting Provider – Web	<input type="checkbox"/> Managed Services	<input type="checkbox"/> Billing Management
<input type="checkbox"/> Network Provider/Transmitter	<input type="checkbox"/> Hosting Provider – Hardware	<input type="checkbox"/>
<input type="checkbox"/> Records Management	<input type="checkbox"/> Data Preparation	<input type="checkbox"/>

Others (please specify):

List facilities and locations included in PCI DSS review: Rackspace datacenters Elk Grove, IL and Xerox Datacenter in Las Vegas, NV.

Part 2b. Relationships

Does your company have a relationship with one or more third-party service providers (for example, gateways, web-hosting companies, airline booking agents, loyalty program agents, etc.)? Yes No

Part 2c. Transaction Processing

How and in what capacity does your business store, process and/or transmit cardholder data? Magento provides a SaaS platform for customers to set up virtual store fronts. Customers may leverage many payment options within their shopping carts via an iFrame connection (i.e., PayPal and Authorize.net or the Magento Payment Bridge). If the customer opts to use the Magento Payment Bridge, the bridge acts as a front-end to PayPal, Payflow, PAYONE, Authorize.net, First Data, DIBS, CyberSource, PSiGate, WorldPay, Orgone, Sage Pay, eWay or Braintree payment gateways for transaction processing via an SSL connection. The information (PAN/CVV2) is temporarily written to a MySQL database in an AES 128-bit encrypted format. The deployed version of the hosted Magento Payment Bridge is also offered as an application sold to customers and has been PA-DSS certified by Trustwave.

Please provide the following information regarding the Payment Applications your organization uses:

Payment Application in Use	Version Number	Last Validated according to PABP/PA-DSS
Magento Payment Bridge	1.11.18.0	23 Jul 2013

Part 3. PCI DSS Validation

Based on the results noted in the Report on Compliance (“ROC”) dated *March 11, 2013*, *James Jemison* asserts the following compliance status for the entity identified in Part 2 of this document as of *March 11, 2013* (check one):

Compliant: All requirements in the ROC are marked “in place¹,” and a passing scan has been completed by the PCI SSC Approved Scanning Vendor *Trustwave* thereby *Magento* has demonstrated full compliance with the PCI DSS 2.0.

Non-Compliant: Some requirements in the ROC are marked “not in place,” resulting in an overall **NON-COMPLIANT** rating, or a passing scan has not been completed by a PCI SSC Approved Scanning Vendor, thereby *Magento* has not demonstrated full compliance with the PCI DSS.

Target Date for Compliance:

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, since not all payment brands require this section.*

Part 3a. Confirmation of Compliant Status

QSA and Service Provider confirm:

- | | |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | The ROC was completed according to the <i>PCI DSS Requirements and Security Assessment Procedures</i> , Version 2.0, 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 the assessment in all material respects. |
| <input checked="" type="checkbox"/> | The Service Provider has read the PCI DSS and recognizes that they must maintain full PCI DSS compliance at all times. |
| <input checked="" type="checkbox"/> | No evidence of magnetic stripe (that is, track) data ² , CAV2, CVC2, CID, or CVV2 data ³ , or PIN data ⁴ storage after transaction authorization was found on ANY systems reviewed during this assessment. |



¹ “In place” results should include compensating controls reviewed by the QSA. If compensating controls are determined to sufficiently mitigate the risk associated with the requirement, the QSA should mark the requirement as “in place.”

² 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 magnetic stripe data after transaction authorization. The only elements of track data that may be retained are account number, expiration date, and name.

³ The three- or four-digit value printed on the signature panel or face of a payment card used to verify card-not-present transactions.

⁴ Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

Part 3b. QSA and Service Provider Acknowledgments

	
Signature of Service Provider Executive Officer ↑	Date: 3/13
Service Provider Executive Officer Name: A. Toshoff	Title: CISO
	
Signature of Lead QSA ↑	Date: March 11, 2013
Lead QSA Name: James Jemison	Title: Security Consultant

Part 4. Action Plan for Non-Compliant Status

Please select the appropriate “Compliance Status” for each requirement. If you answer “No” to any of the requirements, you are required to provide the date Company will be compliant with the requirement and a brief description of the actions being taken to meet the requirement. *Check with the payment brand(s) before completing Part 4 since not all payment brands require this section.*

PCI Requirement	Description	Compliance Status (Select One)	Remediation Date and Actions (if Compliance Status is “No”)
1	Install and maintain a firewall configuration to protect cardholder data.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
2	Do not use vendor-supplied defaults for system passwords and other security parameters.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
3	Protect stored cardholder data.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
4	Encrypt transmission of cardholder data across open, public networks.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
5	Use and regularly update anti-virus software.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
6	Develop and maintain secure systems and applications.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
7	Restrict access to cardholder data by business need to know.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
8	Assign a unique ID to each person with computer access.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
9	Restrict physical access to cardholder data.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
10	Track and monitor all access to network resources and cardholder data.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
11	Regularly test security systems and processes.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
12	Maintain a policy that addresses information security.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	

