Security Standards Council™

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:	Sage Payment Solutions, Inc.	DBA(s):			
Contact Name:	Rob Chenault	Title:	Sr. Director, Network Services & Security		
Telephone:	703-269-9134	E-mail:	Robert.Chenault@sage.com		
Business Address:	1750 Old Meadow Rd., Suite 300	City:	McLean		
State/Province:	VA	Country:	USA	Zip:	22102
URL:	http://www.NA.sage.com				

Qualified Security Assessor Company Information

Company Name:	Verizon Business				
Lead QSA Contact Name:	Matthew Arntsen	Title:	QSA		
Telephone:	336-467-0605	E-mail:	Matthew.Arntsen@Verizon.com		
Business Address:	22001 Loudon County Parkway	City:	Ashburn		
State/Province:	VA	Country:	USA	Zip:	20147
URL:	http://www.verizonbusiness.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)

☒ Payment Processing-POS
☒ Payment Processing-Internet
☐ Issuer Processing
☐ Account Management
☐ Back Office Services
☐ Hosting Provider – Web
☐ Network Provider/Transmitter
☐ Records Management

☐ Tax/Government Payments
☐ Payment Processing – ATM
☒ Payment Gateway/Switch
☐ 3-D Secure Hosting Provider
☐ Prepaid Services
☐ Managed Services
☐ Hosting Provider – Hardware
☐ Data Preparation

☐ Fraud and Chargeback Services
☒ Payment Processing – MOTO
☐ Clearing and Settlement
☐ Loyalty Programs
☐ Merchant Services
☐ Billing Management
☐
☐

☐ Others (please specify):

List facilities and locations included in PCI DSS review: Headquarters in McLean, VA, Data Center in McLean, VA, Data Center in Ashburn, VA

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?

Sage Payment Solutions, Inc. receives and processes card-present, card-not-present, and PIN-based transactions on behalf of their clients (merchants). Sensitive authentication data is held temporarily in memory during transaction processing and is purged post-authorization and is never written to disk. Merchant transaction data is transmitted by Sage Payment Solutions, Inc. to upstream processors for authorization and then encrypted post-authorization and stored within Sage Payment Solutions, Inc. databases.

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
Virtual Terminal	N/A	N/A – Internally developed
Gateway/Gateway API	N/A	N/A – Internally developed

Part 3. PCI DSS Validation

Based on the results noted in the Report on Compliance ("ROC") dated July 23, 2013, Verizon Business asserts the following compliance status for the entity identified in Part 2 of this document as of July 23, 2013 (check one):

☒ **Compliant:** All requirements in the ROC are marked "in place[1]," and a passing scan has been completed by the PCI SSC Approved Scanning Vendor Verizon Business thereby Sage Payment Solutions, Inc. 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 *(Service Provider Name)* 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:

☒ The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version *2.0*, 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.

☒ The Service Provider has read the PCI DSS and recognizes that they must maintain full PCI DSS compliance at all times.

☒ 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:*** 7/23/2103
Service Provider Executive Officer Name: Greg Hammermaster	***Title:*** President
Signature of Lead QSA **↑**	***Date:*** 7/23/2013
Lead QSA Name: Matthew Arntsen	***Title:*** QSA

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.	☒ Yes □ No	
2	Do not use vendor-supplied defaults for system passwords and other security parameters.	☒ Yes □ No	
3	Protect stored cardholder data.	☒ Yes □ No	
4	Encrypt transmission of cardholder data across open, public networks.	☒ Yes □ No	
5	Use and regularly update anti-virus software.	☒ Yes □ No	
6	Develop and maintain secure systems and applications.	☒ Yes □ No	
7	Restrict access to cardholder data by business need to know.	☒ Yes □ No	
8	Assign a unique ID to each person with computer access.	☒ Yes □ No	
9	Restrict physical access to cardholder data.	☒ Yes □ No	
10	Track and monitor all access to network resources and cardholder data.	☒ Yes □ No	
11	Regularly test security systems and processes.	☒ Yes □ No	
12	Maintain a policy that addresses information security.	☒ Yes □ No	

AMERICAN EXPRESS DISCOVER JCB MasterCard Worldwide VISA