BigCommerce Pty

Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2

April 2016

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:	BigCommerce Holding Inc.		DBA (doing business as):	BigCommerce Pty. Ltd. BigCommerce Inc.	
Contact Name:	Scott Baker		Title:	VP of IT	
Telephone:	888-699-8911		E-mail:	Scott.Baker@bigcommerce.com	
Business Address:	685 Market St, CA		City:	San Francisco	
State/Province:	CA	Country:	USA	Zip:	94105
URL:	https://www.bigcommerce.com/				

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

Company Name:	Coalfire Systems, Inc.				
Lead QSA Contact Name:	Roshan Boloor		Title:	Senior IT Security Consultant	
Telephone:	303-554-6333		E-mail:	pciqa@coalfire.com	
Business Address:	11000 Westmoor Circle, Suite 450		City:	Westminster	
State/Province:	CO	Country:	USA	Zip:	80021
URL:	www.coalfire.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:	Ecommerce	
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:	N/A

Type of service(s) not assessed:

Hosting Provider:	**Managed Services (specify):**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POS / card present
☐ Hardware	☐ IT support	☐ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Shared Hosting Provider		
☐ Other Hosting (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:	N/A

Part 2b. Description of Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	BigCommerce Pty. Ltd. (BigCommerce) hosts ecommerce websites for their customers, where consumers enter credit card data. Card holder data (CHD) is transmitted over HTTPS TLS 1.2 AES 256 to BigCommerce web server that is hosted in BigCommerce environment. BigCommerce web server transmits the CHD over HTTPS TLS 1.2 AES 256 to client specified payment processor. Client specified payment processor is configured with BigCommerce. BigCommerce does not store CHD. Processor responses return over HTTPS TLS 1.2. Transaction information is logged (CHD is not stored) and response codes are transmitted over HTTPS TLS 1.2 AES 256 to their customers.

Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	BigCommerce is a merchant that accepts new customers via www.bigcommerce.com for trial subscriptions. If they wish to upgrade to a paid subscription, the customer can enter their payment details either on account.bigcommerce.com (legacy WHMCS billing system) or manage.bigcommerce.com (new custom billing system), once entered these details are passed off for processing and subscription related recharging to either GlobalCollect (in the case of WHMCS) or Zuora (in the case of the new billing system). No CHD comes to rest on BigCommerce infrastructure at any time, and online through the billing systems is the only avenue BigCommerce takes card payments for its services. As a platform, BigCommerce allows merchants to configure any of their enabled payment gateways, to connect with their Merchant ID. There are two ways in which the BigCommerce platform allows merchants to take payments, the first is simply via the checkout process on the storefront. A shopper completes the checkout process, specifying their order, and shipping details, and is then prompted for their CHD, for some gateways this is done offsite, via a redirect or iframe, and for other it's done via a direct post to the gateway API. Additionally, CHD may be entered by the merchant via the manual order page in the control panel, in which case it still follows the same steps. The CHD is passed along with the MID and gateway connection information to the gateway from processing, and the returned response is saved (the CHD never comes to rest on BigCommerce infrastructure).

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):
Dallas 1 SoftLayer Datacenter	1	Dallas, TX
Dallas 5 SoftLayer Datacenter	1	Dallas, TX
Dallas 9 SoftLayer Datacenter	1	Richardson, TX
Dallas 10 SoftLayer Datacenter	1	Richardson, TX
Seattle 1 SoftLayer Datacenter	1	Seattle, WA

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)
BigCommerce Platform	Floating Version	BigCommerce	☐ Yes ☒ No	N/A

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.*	BigCommerce hosts their production environment in SoftLayer. SoftLayer sites are Dallas and Seattle. The BigCommerce Environment is physically separate from the corporate offices (which is out of scope). Administrator laptops are used by admin users working remote; there are no workstations within the corporate offices. Admins connect over IPSec VPN tunnel with AES-256-bit encryption.\ into the BigCommerce environment using two-factor authentication with Duo, where they then use SSH to remote into servers. All BigCommerce client websites are hosted in this environment and the consumers credit card data is processed by client specified payment gateways.
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? If Yes: Name of QIR Company: N/A QIR Individual Name: N/A Description of services provided by QIR: N/A	☐ Yes ☒ No
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:**
SoftLayer Technologies, Inc.	Hosting Provider
Stripe	Payment Processing
Ingenico Group E-Commerce Solution	Payment Processing

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:	Ecommerce

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:	☐	☒	☐	**1.2.3 N/A- BigCommerce does not have wireless networks in the BigCommerce E-Commerce environment.**
Requirement 2:	☒	☐	☐	**Full**
Requirement 3:	☐	☒	☐	**3.4.1 N/A – BigCommerce does not store CHD hence Disk Encryption not applicable.** **3.5 N/A – BigCommerce does not store CHD hence procedures to protect encryption keys is not applicable.** **3.6 N/A– BigCommerce does not store CHD hence procedures for key management process is not applicable**
Requirement 4:	☐	☒	☐	**4.1.1 N/A– BigCommerce does not store CHD; hence, Disk Encryption is not applicable.**
Requirement 5:	☒	☐	☐	**Full**
Requirement 6:	☐	☒	☐	**6.4.6 N/A– N/A until January 31, 2018**
Requirement 7:	☒	☐	☐	**Full**
Requirement 8:	☐	☒	☐	**8.7 – BigCommerce does not CHD in any BigCommerce database.**
Requirement 9:	☐	☐	☒	**9.1 – 9.10 BigCommerce does not store cardholder data. No media with cardholder data is produced, and**

				all physical aspects of BigCommerce's architecture are managed by SoftLayer. SoftLayer provided a PCI AOC (Dated June 30 2016).
Requirement 10:	☐	☒	☐	**10.2.1 - BigCommerce does not store CHD. There is no CHD in BigCommerce's environment to access.**
Requirement 11:	☐	☒	☐	**11.1 - *N/A - All physical aspects of BigCommerce's architecture are managed by SoftLayer. SoftLayer performs the unauthorized wireless scanning for BigCommerce, as per their AOC (*Dated June 30 2016*).*** ***11.3.4 N/A- BigCommerce has a flat network architecture that is dedicated to only BigCommerce e-commerce.*** **11.3.4.1 - N/A until January 31, 2018**
Requirement 12:	☐	☒	☐	**12.4.1 - N/A until January 31, 2018** **12.11 – N/A until January 31, 2018**
Appendix A1:	☐	☒	☐	**A1.1 – BigCommerce does not let clients host their own application. BigCommerce only host e-commerce sites.** **A1.2 - BigCommerce do not let clients access system components. Access is only limited to BigCommerce employees for all in scope systems.** **A1.3 – BigCommerce do not let clients access system components or logs. Access is limited to BigCommerce employees for all in scope systems.**
Appendix A2:	☐	☐	☒	**A2.1 N/A – BigCommerce does not support insecure versions of SSL/TLS.** **A2.2 N/A – BigCommerce does not support insecure versions of SSL/TLS.** **A2.3 N/A – BigCommerce does not support insecure versions of SSL/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:	*May 31, 2017*	
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 *5/31/2017.*

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 *BigCommerce Pty. 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
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*, 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 *Qualys (Q2, 2016 & Q3 2016) and, Coalfire Labs (Q1, 2017).*

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	*Date:* **5/31/2017**
Service Provider Executive Officer Name: **Scott Baker**	*Title:* **VP of IT**

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

If a QSA was involved or assisted with this assessment, describe the role performed:	*Conducted pre-onsite, Onsite, and Post onsite interviews, reviewed documentation, evidence, system configurations, policies and procedures. Documented all reviewed processes and findings to the Report on Compliance.*

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* **5/31/2017**
Duly Authorized Officer Name: **Roshan Boloor**	*QSA Company:* **Coalfire**

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. No ISAs were involved with the assessment.*

[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	☒	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS	☒	☐