Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.1

April 2015

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:	Hosting, Inc.		DBA (doing business as):		
Contact Name:	Johan Hybinette		Title:	Chief Information Security Officer	
ISA Name(s) (if applicable):			Title:		
Telephone:	302-224-1672		E-mail:	jhybinette@hosting.com	
Business Address:	900 South Broadway, Suite 400		City:	Denver	
State/Province:	CO	Country:	USA	Zip:	80209
URL:	www.hosting.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	360 Advanced, Inc.				
Lead QSA Contact Name:	Virgil Floresca		Title:	Senior Associate	
Telephone:	866-418-1708		E-mail:	vfloresca@360advanced.com	
Business Address:	4806 W. Gandy Blvd.		City:	Tampa	
State/Province:	FL	Country:	USA	Zip:	33611
URL:	www.360advanced.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:	Hosting Cloud Services	
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.

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:		

Part 2b. Description of Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Hosting does not store, process, and/or transmit cardholder data.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Hosting provides infrastructure and platform services to their customers and does not interface directly with customers' cardholder data. It is the responsbility of their customers to protect and maintain security for their own cardholder data environment. Hosting's Customer Portal website provides customers with limited capabilities to modify rulesets within firewalls they are subscribed to. This interface is performed via secured API calls which was validated against through penetration testing and web application vulnerability scans. Initial firewall rulesets are configured to be PCI compliant, however, it is the responsibility of the customer to review their configurations periodically and ensure compliancy is maintained.

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):
Example: Retail outlets	*3*	*Boston, MA, USA*
Offices	2	Newark, DE, USA Denver, CO, USA
Data Centers	6	Newark, DE, USA Denver, CO, USA Louisville, KY, USA Dallas, TX, USA Irvine, CA, USA San Francisco, CA, USA

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)
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ 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.*	Hosting maintains hardware and software to provide the infrastructure and platforms to support PCI customer environments. This hardware and software ensures a secure CDE from the customer perimeter firewall to the handoff of traffic to telecommunication carriers by Hosting. It also includes services (external to customer CDEs) that support the PCI compliance of said CDEs, in a variety of configurations as requested by each customer. Hosting does not handle cardholder data, but it does support customer CDEs that do. These critical hardware and software components are deemed to be relevant and in scope for the purposes of this assessment.
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 one or more third-party service providers (for example, 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:

Type of service provider:	Description of services provided:

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:	Hosting Cloud Services

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:	☐	☒	☐	**1.1.3 was not applicable. Hosting is not responsible for data-flow diagrams of cardholder data and does not maintain an architecture of systems or applications within their customers' environment.** **1.2.1 was not applicable. Hosting customers are responsible for managing necessary inbound and outbound traffic necessary for their respective cardholder data environments** **1.2.3 was not applicable. Hosting does not provide wireless services within their customers' cardholder data environment (CDE). Wireless scans are performed quarterly to determine and document any unknown or rogue access points.** **1.3.7 was not applicable. Hosting does not store any cardholder data but only provides the infrastructure platform that customer environments are hosted on.** **1.4 was not applicable. Mobile and / or employee-owned devices that connect to the Internet when outside the network are deemed not in scope. These devices cannot connect or interact directly to the infrastructure hosting PCI customers' cardholder data environments. Jump servers with multi-factor authentication using RSA SecurID tokens are implemented to allow centralized and restricted management of devices within this infrastructure.**
Requirement 2:	☐	☒	☐	**2.1.1 was not applicable. Hosting does not provide wireless services within their customers' cardholder data environment (CDE). Wireless scans are**

				performed quarterly to determine and document any unknown or rogue access points. **2.6 was not applicable. Hosting offers no services to PCI customers that would classify it as a shared hosting provider.**
Requirement 3:	☐	☐	☒	**In the context of the service provider role, Hosting is not responsible for cryptographic techniques, tools, or processes to protect their customers' cardholder data. Protection of the storage and transmission of this information within each cardholder data environment is the responsibility of the customer.**
Requirement 4:	☐	☐	☒	**In the context of the service provider role, Hosting is not responsible for cryptographic techniques, tools, or processes to protect their customers' cardholder data. Protection of the storage and transmission of this information within each cardholder data environment is the responsibility of the customer.**
Requirement 5:	☒	☐	☐	
Requirement 6:	☐	☒	☐	**6.4.3 was not applicable. Hosting has no insight or programmatic access into their customer's cardholder data. However, development and testing controls are followed to ensure secure coding practices are in place within the software development life cycle of Hosting's Customer Portal web interface.**
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	**8.1.5 was not applicable. Hosting did not have vendors who accessed system components within the cardholder data environment.** **8.7 is not applicable. Hosting has no involvement in the management or design of databases within their customers' CDE. It is the responsibility of the customer to maintain compliance of their servers once they are deployed.**
Requirement 9:	☐	☒	☐	**9.5.1 is not applicable. No off-site or on-site storage of media backups containing cardholder data existed. Backups are performed and stored in SAN arrays across the different data centers. Hosting does not store cardholder data either on external disks or in paper form.** **9.6.2 and 9.6.3 is not applicable. Media is not moved from secure locations or sent outside Hosting facilities.** **9.8.1 is not applicable. Hosting does not generate or store any hard-copy materials of cardholder data.** **9.9 through 9.9.3 are not applicable. Hosting does not have any point-of-sale locations or devices.**
Requirement 10:	☒	☐	☐	
Requirement 11:	☐	☒	☐	**11.1.1 was not applicable. Hosting does not provide wireless services within their customers' cardholder**

				data environment (CDE). Wireless scans are performed quarterly to determine and document any unknown or rogue access points.
Requirement 12:	☐	☒	☐	**12.8 through 12.8.5 are not applicable. Hosting does not share cardholder data with any service providers.**
Appendix A:	☐	☐	☒	**2.6 was not applicable. Hosting offers no services to PCI customers that would classify it as a shared hosting provider.**

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:	July 1, 2016	
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

Based on the results noted in the ROC dated *July 1, 2016*, 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 as of *July 1, 2016*: (***check one):***

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *Hosting, Inc.* 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 *(Service Provider Company 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.*
☐	**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

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 *3.1*, 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)	
☒	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 *Alert Logic, Inc.*

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↗	*Date:* **July 1, 2016**
Service Provider Executive Officer Name: **Johan Hybinette**	*Title:* **Chief Information Security Officer**

Part 3c. QSA Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	360 Advanced provided PCI DSS assessment and consulting services.

Signature of Duly Authorized Officer of QSA Company ↗	*Date:* **July 1, 2016**
Duly Authorized Officer Name: **Brad Lyons**	*QSA Company:* **360 Advanced, Inc.**

Part 3d. ISA Acknowledgement (if applicable)

If an ISA was involved or assisted with this assessment, describe the role performed:	

Signature of ISA ↗	*Date:*
ISA Name:	*Title:*

[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	☒	☐