Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.0

February 2014

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:	Akamai		DBA (doing business as):	None	
Contact Name:	Jo Guthrie		Title:	Compliance Manager	
ISA Name(s) (if applicable):			Title:		
Telephone:	[redacted]		E-mail:	[redacted]	
Business Address:	8 Cambridge Center		City:	Cambridge	
State/Province:	MA	Country:	USA	Zip:	02142
URL:	www.akamai.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	Cisco Systems, Inc.				
Lead QSA Contact Name:	Patrick Harbauer		Title:	Senior Security Consultant	
Telephone:	[redacted]		E-mail:	[redacted]	
Business Address:	170 West Tasman Drive		City:	San Jose	
State/Province:	CA	Country:	USA	Zip:	95134
URL:	www.cisco.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:	Secure Content Delivery Network (SCDN) and Edge Tokenization	
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): Internet based HTTPS content delivery. Payment card transport for tokenization.		

***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:	Other internet and intranet services described below	
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): Other internet and intranet services, including Web Performance Solutions, Media Delivery Solutions, Cloud Security Solutions, Cloud Networking Solutions, and Network Operator Solutions.		
Provide a brief explanation why any checked services were not included in the assessment:	We instruct our customers that only products running on the SCDN are in-scope for PCI and that no other systems are intended or should be used for the transmission, processing, or storage of cardholder data.	

Part 2b. Description of Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Akamai only proxies and re-transmits cardholder data. It never processes cardholder data or stores cardholder data on durable media.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	None

Part 2c. Locations

List types of facilities and a summary of locations included in PCI DSS review (for example, retail outlets, corporate offices, data centers, call centers, etc.):

Type of facility:	Location(s) of facility (city, country):
Headquarters	Cambridge, MA USA
Data Center	Cambridge, MA USA
Data Center	Chicago, IL 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.*	Akamai only proxies and re-transmits cardholder data. It never processes cardholder data or stores cardholder data on durable media. The Akamai Secure Content Delivery Network (SCDN) is the only in-scope system that transmits cardholder data. The SCDN, comprised of the EdgeSuite SSL (ESSL) distributed computer system, allows Akamai's customers to extend and accelerate their online business infrastructure. An Akamai customer will use the SCDN to transmit cardholder data, either within individual transactions between the end user and the Akamai customer or in an Edge Tokenization transaction in which a payment processor receives the transaction data and the Akamai customer receives a token, which contains no cardholder data.
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	☐ Yes ☒ No

companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?	

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:	Secure Content Delivery Network (SCDN) and Edge Tokenization			
	Details of Requirements Assessed			
PCI DSS Requirement	**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:	☐	☒	☐	**1.3.8.b - N/A - Akamai does not disclose private IP addresses and routing information to unauthorized parties.**
Requirement 2:	☐	☒	☐	**2.1.1 - N/A - Not applicable to the deployed network. These systems are publicly accessible servers that do not store cardholder data. Akamai does not employ wireless networking on these networks. Not applicable for non-deployed networks. All wireless networks are firewalled off from the non-deployed networks and components.** **2.2.2.b - N/A - No enabled insecure services, daemons, or protocols were identified when reviewing systems with network administrators.** **2.3.c - N/A - No web based management interfaces are allowed on any of the sampled servers.** **2.6 - N/A - Akamai is not a shared hosting provider.**
Requirement 3:	☐	☒	☐	**3.1, 3.2, 3.3, 3.4 - N/A - The SCDN only proxies and re-transmits cardholder data, it is not stored on durable media. To ensure this, the Personally Identifiable Information and Sensitive Information Caching and Storage Policy states that Personally Identifiable**

				Information (PII) such as cardholder data should never be cached, should never be written to unencrypted persistent storage, should never be written to log files, and should always be transmitted over encrypted channels. **3.5, 3.6, 3.7 - N/A - Cardholder data was confirmed not to be stored on any Akamai systems therefore there are no such encryption keys in use.**
Requirement 4:	☐	☒	☐	**4.1 - N/A - The SCDN supports strong cryptography and security protocols to safeguard sensitive cardholder data during transmission. It is the responsibility of Akamai customers to use only trusted keys and certificates, use secure configurations and strength appropriate for the encryption methodology in use.** **4.1.1 - N/A - Akamai has no wireless networks transmitting cardholder data or connected to the cardholder data environment.** **4.2 - N/A - It was confirmed that Akamai never processes or stores cardholder data on durable media.** **4.3 - N/A - The SCDN supports strong cryptography and security protocols to safeguard sensitive cardholder data during transmission. It is the responsibility of Akamai customers to use only trusted keys and certificates, use secure configurations and strength appropriate for the encryption methodology in use. It was confirmed that Akamai never processes or stores cardholder data on durable media.**
Requirement 5:	☒	☐	☐	
Requirement 6:	☐	☒	☐	**6.3.1 - N/A - Not applicable to the SCDN. Cardholder data is not stored on the SCDN, and there are no payment card applications with customer accounts, user IDs, or passwords within these systems.** **6.4.3 - N/A - Cardholder data is not stored on durable media on the SCDN. Neither primary account numbers nor any other cardholder data is used for testing or development.** **6.4.4 - N/A - Test data is never moved from the test networks back into production or source control.**

				Cardholder data is never processed or stored on durable media by any Akamai software or application. **6.5.3 - N/A - It was confirmed that Akamai systems never store cardholder data on durable media.** **6.5.7, 6.5.8, 6.5.9, 6.5.10, 6.6 - N/A - Akamai has no web applications that accept cardholder data.**
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	**8.1.3.b - N/A - Gaining access to any Akamai facility or datacenter does not allow anyone to gain access to the SCDN. All those systems are in secured racks that can only be access with a ticket opened and by contacting the NOCC. If a rack is opened without authorization, security cameras in each rack will capture the activity and the NOCC will receive alerts.** **8.5.1 - N/A - Akamai does not have remote access to customer premises systems.** **8.7 - N/A - Akamai has no databases in place that store cardholder data.**
Requirement 9:	☐	☒	☐	**9.1.2 – N/A - There are no publicly accessible network jacks for in-scope systems.** **9.1.3 - N/A - Not applicable to the SCDN. Production servers on these networks do not store cardholder data on durable media and do not employ wireless networking.** **9.2 - N/A - Akamai uses individually secured cabinets for the SCDN above and beyond that of physical access at co-location facilities.** **9.4.1 - N/A - Akamai does not store or maintain cardholder data on durable media.** **9.4.2, 9.4.3, 9.4.4 – N/A - Akamai uses individually secured cabinets for the SCDN above and beyond that of physical access at co-location facilities.** **9.5, 9.5.1, 9.6, 9.6.1, 9.6.2, 9.6.3, 9.7, 9.7.1 - N/A - Not applicable to the SCDN. Akamai does not store cardholder data on any durable media.** **9.8, 9.8.1, 9.8.2 - N/A - Not applicable to the SCDN. Akamai does not store cardholder data on any**

				durable media. Production servers on the SCDN that could have served to proxy or re-transmit cardholder data are destroyed in a secure fashion. **9.9 - N/A - Akamai only proxies and re-transmits cardholder data. It never processes cardholder data or stores cardholder data on durable media.**
Requirement 10:	☐	☒	☐	**10.2.1 - N/A - Akamai only proxies and re-transmits cardholder data. It never processes cardholder data or stores cardholder data on durable media.** **10.6.2.b - N/A - All in-scope systems were observed to have their logs reviewed on a daily basis.**
Requirement 11:	☒	☐	☐	
Requirement 12:	☐	☒	☐	**12.3.9 - N/A - Not applicable to the SCDN. No vendors or business partners are granted remote access privileges.** **12.3.10 - N/A - Akamai only proxies and re-transmits cardholder data. It never processes cardholder data or stores cardholder data on durable media.** **12.7 - N/A - Akamai personnel never handle credit card data.** **12.8 - N/A - Akamai does not share cardholder data with any 3rd parties.**
Appendix A:	☐	☒	☐	**A.1.2.a, A.1.2.b, A.1.2.c, A.1.2.d, A.1.2.e, A.1.3, A.1.4 - N/A: Akamai is not a managed service 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:	*6/17/2015*	
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 *6/17/2015*, 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 *6/26/2015*: (***check one):***

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *Akamai* 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 *3.0*, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of 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.

PCI Security Standards Council

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 *Cisco Systems, Inc.*

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	*Date:* 30 June 2015
Service Provider Executive Officer Name: Andy Ellis	*Title:* CSO

Part 3c. QSA Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	*QSA assessed all PCI DSS requirements.*

DocuSigned by:
Patrick Harbauer
BD6E667E39CD461...

Signature of QSA ↑	*Date:* 6/29/2015
QSA Name: Patrick J. Harbauer	*QSA Company:* Cisco Systems, 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	☒	☐	