Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for
Self-Assessment Questionnaire D –
Service Providers
For use with PCI DSS Version 3.2

April 2016

PCi Security
Standards Council ®

Section 1: Assessment Information

Instructions for Submission

This document must be completed as a declaration of the results of the service provider's self-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:	Optimizely		DBA (doing business as):		
Contact Name:	Pamela Chuang		Title:	Compliance Manager	
Telephone:	(800) 252-9480		E-mail:	pam@optimizely.com	
Business Address:	631 Howard St. Ste. 100		City:	San Francisco	
State/Province:	CA	Country:	USA	Zip:	94105
URL:	https://www.optimizely.com				
Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:					
Lead QSA Contact Name:			Title:		
Telephone:			E-mail:		
Business Address:			City:		
State/Province:		Country:		Zip:	
URL:					

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:	The development and delivery infrastructure for Javascript snippets served to browsers for Optimizely X Web Experimentation, Web Personalization, and Web Recommendations.

Type of service(s) 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): Internet based delivery of JavaScript snippets for the Web Experimentation, Web Personalization, and Web Recommendations products on the Optimizely X platform

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:	Optimizely Classic, Optimizely X Full Stack, Optimizely X Over-The-Top

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): Any systems or services not related to development or delivery of JavaScript snippets for the Web products on the Optimizely X platform. This includes:

- Internet delivery of JavaScript snippets for Optimizely Classic

- Internet based delivery of client code delivered to Optimizely X Full Stack and Optimizely X Over-The-Top (OTT).

Provide a brief explanation why any checked services were not included in the assessment:	Optimizely Classic is our legacy platform and separate from X. Optimizely X Full Stack and OTT do not affect clients' PCI compliance.

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Optimizely 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.	PCI Service Provider status can be applied to any entity that could affect the security of payment cards or transactions. Optimizely can be considered a Service Provider to its merchant customers that wish to use Optimizely products on those checkouts.

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*
Optimizely Headquarters	1	San Francisco, CA, USA

Hosting Providers	Numerous	Various

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	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	
			☐ Yes ☐ No	

Part 2e. Description of Environment

Provide a **_high-level_** description of the environment covered by this assessment.	The software developed at Optimizely's Headquarters and deployed to the Optimizely X Platform using Google Compute Cloud, Microsoft Azure, and Amazon Web Services.
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.*	

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: QIR Individual Name: Description of services provided by QIR:	☐ Yes ☒ No

PCI Security Standards Council ®

Part 2f. Third-Party Service Providers (Continued)

| 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:
Akamai	PCI Compliant CDN, DNS
Amazon Web Services	Infrastructure
Google Cloud Platform	Optimizely App
Microsoft Azure	Infrastructure

Note: Requirement 12.8 applies to all entities in this list.

PCI Security Standards Council ®

Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- Full – The requirement and all sub-requirements were assessed for that Requirement, and no sub-requirements were marked as "Not Tested" or "Not Applicable" in the SAQ.

- Partial – One or more sub-requirements of that Requirement were marked as "Not Tested" or "Not Applicable" in the SAQ.

- None – All sub-requirements of that Requirement were marked as "Not Tested" and/or "Not Applicable" in the SAQ.

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 SAQ

- 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:

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:	☒	☐	☐	
Requirement 2:	☐	☒	☐	**2.1.1 - N/A - The cardholder data environments as administered by AWS, GCP, and Azure do not employ wireless technology.** **2.2.3 - N/A - Optimizely does not employ insecure services, daemons, or protocols.** **2.6 - N/A Optimizely is not a shared hosting provider.**
Requirement 3:	☐	☐	☒	**3 - N/A - Optimizely does not store, process, and/or transmit cardholder data.**
Requirement 4:	☐	☒	☐	**4.1 - N/A - Optimizely does not store, process, and/or transmit cardholder data. Optimizely utilizes strong cryptography to safeguard the integrity of snippets transmitted over the internet.** **4.1.1 - N/A - Optimizely has no wireless networks transmitting cardholder data or connected to the cardholder data environment.** **4.2 - N/A - No PANs used.**
Requirement 5:	☒	☐	☐	
Requirement 6:	☐	☒	☐	**6.4.3 - N/A - No PANs used.**

Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	**8.1.5 - N/A - No vendor with access to in-scope systems.** **8.5.1 - N/A - Optimizely does not employ remote access to the customer's premises.** **8.6 - N/A - No alternative authentication methods.** **8.7 - N/A - Optimizely does not have a database that stores cardholder data.**
Requirement 9:	☐	☒	☐	**9.4.1 - N/A - No cardholder data processing on Optimizely premises or systems.** **9.5 - 9.8 - N/A - No media contains cardholder data.** **9.9 - N/A - No physical devices that capture payment card data.**
Requirement 10:	☐	☒	☐	**10.2.1 - N/A - No cardholder data in scope.**
Requirement 11:	☒	☐	☐	
Requirement 12:	☐	☒	☐	**12.3.9 - N/A - No remote partner access is permitted.** **12.3.10 - N/A - Optimizely does not store or handle cardholder data.** **12.4.1 - N/A - This requirement is a best practice until January 31, 2018, after which it becomes a requirement.** **12.11 - 12.11.1 - N/A - This requirement is a best practice until January 31, 2018 after which it becomes a requirement.**
Appendix A1:	☐	☐	☒	**A1.1-A1.4 - N/A - Optimizely is not a shared hosting provider.**
Appendix A2:	☐	☒	☐	**A2.1 - N/A - No POS POI in scope.**

Section 2: Self-Assessment Questionnaire D – Service Providers

This Attestation of Compliance reflects the results of a self-assessment, which is documented in an accompanying SAQ.

The assessment documented in this attestation and in the SAQ was completed on:	4/28/2017
Have compensating controls been used to meet any requirement in the SAQ?	☒ Yes ☐ No
Were any requirements in the SAQ identified as being not applicable (N/A)?	☒ Yes ☐ No
Were any requirements in the SAQ identified as being not tested?	☐ Yes ☒ No
Were any requirements in the SAQ 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 SAQ D (Section 2), dated *4/28/2017*.

Based on the results documented in the SAQ D 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 SAQ are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *Optimizely Inc.* has demonstrated full compliance with the PCI DSS.
☐	**Non-Compliant:** Not all sections of the PCI DSS SAQ are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby *(Service Provide 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 "No" 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)

☒	PCI DSS Self-Assessment Questionnaire D, Version *3.2*, was completed according to the instructions therein.
☒	All information within the above-referenced SAQ 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 *Managed Security Service Provider*

Part 3b. Service Provider Attestation

DocuSigned by:

William Press

6C1AE6F8AA39490...

Signature of Service Provider Executive Officer ↑	*Date:* Apr-30-2017
Service Provider Executive Officer Name: William Press	*Title:* Sr. Vice President, Engineering

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

If a QSA was involved or assisted with this assessment, describe the role performed:	

Signature of Duly Authorized Officer of QSA Company ↑	*Date:*
Duly Authorized Officer Name:	*QSA Company:*

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:	

[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	☐	☐	