Payment Card Industry (PCI)

Data Security Standard

Attestation of Compliance for Self-Assessment Questionnaire D – Service Providers

For use with PCI DSS Version 3.2.1

July 2018

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:	Lawrence Bruhmuller		Title:	CTO	
Telephone:	1-800-252-9480		E-mail:	lawerence.bruhmuller@optimizely.com	
Business Address:	631 Howard St. Suite 100		City:	San Francisco	
State/Province:	CA	Country:	USA	Zip:	94105
URL:	www.optimizely.com				
Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	NCC Services, Ltd				
Lead QSA Contact Name:	Mark Graziano		Title:	QSA	
Telephone:	1-800-813-3523		E-mail:	mark.graziano@nccgroup.com	
Business Address:	48 W 25th St. 4th Floor		City:	New York	
State/Province:	NY	Country:	USA	Zip:	10010
URL:	www.nccgroup.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:	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:	**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:	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)

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. Additionally, Optimizely does not directly connect to any customer CDE.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	For the purposes of this assessment, Optimizely is classified as a Service Provider. While Optimizely does not participate in the processing, transmission or storage of CHD on behalf of any customer, Optimizely provides a service that, depending on how customers choose to use the service, could affect the security of CHD. Optimizely's service is an experimentation platform that enables customers to conduct A/B testing, which enables businesses to deliver continuous experimentation and personalization across websites, mobile apps and connected devices. Optimizely creates

	these experiments on the customers' sites by delivering and executing JavaScript snippets, configured for a customer's specific account and page. A customer can use these experiments to compare different versions of a webpage or app against each other to determine which one performs better. Since customers could potentially apply these experiments to an e-commerce payment page, Optimizely assesses their main application, app.optimizely.com, against the PCI DSS. Even if an Optimizely experiment is applied to a payment page, the functionality of the experiments is limited to the analysis of web traffic and customer behavior and does not serve any functions that help facilitate the payment process or interact with CHD.

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 - Optimizely's architecture was developed with the principles of high availability and reduncancy

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)
Not Applicable	Not Applicable	Not Applicable	☐ Yes ☐ No	Not Applicable
			☐ 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. *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.*	Optimizely's main application, app.optimizely.com, is built inside a dedicated PCI VPC inside AWS by the CodeBuild and CodePipeline and deployed to Google App Engine (GAE). During the code build process, Optimizely uses Jenkins to pull code from Github and to build the Client Build Server Docker images which are pushed to quay.io. Spinnaker pulls the container directly from quay.io and deploys a cluster of AMIs each running the Client Server Build docker container in Amazon ECS. A customer creating a new optimizely experiment or a personalization campaign will trigger a snippet to be built by a Client Build Server instance. App.optimizely.com hashes each build request with a secret key and the Client Build Server then validates the HMAC of each build request. The build is then passed into Optimzely-hrd running on Google App Engine which uploads the builds to the Optimizely S3 bucket. Akamai CDN downloads the builds from S3 where they are ready for the customer. Optimizely uses a bastion host to manage all traffic into the AWS PCI environment and authentication is enforced with Microsoft Azure Active Directory.
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?	☐ Yes ☐ No
If Yes:	
Name of QIR Company:	Not Applicable
QIR Individual Name:	Not Applicable
Description of services provided by QIR:	Not Applicable

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	Content Delivery Network and DNS
Amazon Web Services	Hosting Provider (Infrastructure)
Google Cloud Platform	Hosting Provider (Optimizely X App)

Microsoft Azure	Hosting Provider (Authenticaiton Infrastructure)

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 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:	☐	☒	☐	**1.1.6 (b) - Optimizely does not use insecure ports, protocols or procedures** **1.2.3 - Optimizely does not use wireless technologies. The infrastructure is hosted by AWS, GCP and Azure**
Requirement 2:	☐	☒	☐	**2.1.1 - Optimizely does not use wireless technologies. The infrastructure is hosted by AWS, GCP and Azure** **2.2.2 (a) - Optimizely does not use insecure ports, protocols or procedures** **2.2.3 - Optimizely does not use insecure ports, protocols or procedures** **2.6 - Optimizely is not a Shared Hosting Provider**
Requirement 3:	☐	☐	☒	**Optimizely does not store CHD**
Requirement 4:	☐	☐	☒	**Optimizely does not transmit CHD**
Requirement 5:	☐	☐	☒	**Optimizely does not have any networks or systems that process, transmit or store CHD**
Requirement 6:	☐	☒	☐	**6.4.3 - Optimizely does not have any networks or systems that process, transmit or store CHD**

Requirement 7:	☐	☒	☐	**7.3 - Optimizely does not have any networks or systems that process, transmit or store CHD**
Requirement 8:	☐	☒	☐	**8.1.5 - Optimizely prohibits all third party access to the CDE** **8.5.1 - Optimizely does not remotely access customer environments** **8.6 - Optimizely does not use alternative authentication methods** **8.7 - Optimizely does not store CHD**
Requirement 9:	☐	☐	☒	**Optimizely does not have any physical locations that process, transmit or store CHD**
Requirement 10:	☐	☐	☒	**Optimizely does not have any networks or systems that process, transmit or store CHD**
Requirement 11:	☐	☐	☒	**Optimizely does not have any networks or systems that process, transmit or store CHD**
Requirement 12:	☐	☒	☐	**12.3.9 - Optimizely prohibits all third party access to the CDE** **12.3.10 - Optimizely does not process, transmit or store CHD**
Appendix A1:	☐	☐	☒	**Optimizely is not a Shared Hosting Provider**
Appendix A2:	☐	☐	☒	**Optimizey does not use SSL/Early TLS or POS devices and does not process, transmit or store CH**

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:	May 1, 2020	
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 *May 1, 2020.*

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)* 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 *Optimizely* 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 *3.2.1)*, 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.

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*

Part 3b. Service Provider Attestation	
DocuSigned by: 14469D36F937423...	
Signature of Service Provider Executive Officer ↑	*Date:* **5/1/2020**
Service Provider Executive Officer Name: **Lawrence Bruhmuller**	*Title:* **CTO**

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)	
If a QSA was involved or assisted with this assessment, describe the role performed:	QSA assisted Optimizely with PCI DSS evidence collection and review for all applicable controls. Additionally, the QSA assisted Optimizely in the completion of the Self Assessment Questionnaire D (Service Provider) and the Attestation of Compliance
DocuSigned by: Mark Graziano 41219FE95CD4405...	
Signature of Duly Authorized Officer of QSA Company ↑	*Date:* **5/1/2020**
Duly Authorized Officer Name: **Mark Graziano**	*QSA Company:* **NCC Services, Ltd.**

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:	Not Applicable

[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 for Card-Present POS POI Terminal Connections.	☒	☐