Payment Card Industry (PCI)

Data Security Standard

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

SAQ-Eligible Service Providers

For use with PCI DSS Version 3.2.1

June 2018

Table of Contents

Document Changes

Date	PCI DSS Version	SAQ Revision	Description
October 2008	1.2		To align content with new PCI DSS v1.2 and to implement minor changes noted since original v1.1.
October 2010	2.0		To align content with new PCI DSS v2.0 requirements and testing procedures.
February 2014	3.0		To align content with PCI DSS v3.0 requirements and testing procedures and incorporate additional response options.
April 2015	3.1		Updated to align with PCI DSS v3.1. For details of PCI DSS changes, see PCI DSS – Summary of Changes from PCI DSS Version 3.0 to 3.1.
July 2015	3.1	1.1	Updated to remove references to “best practices” prior to June 30, 2015, and remove tde PCI DSS v2 reporting option for Requirement 11.3.
April 2016	3.2	1.0	Updated to align with PCI DSS v3.2. For details of PCI DSS changes, see PCI DSS – Summary of Changes from PCI DSS Version 3.1 to 3.2.
January 2017	3.2	1.1	Updated version numbering to align with other SAQs
June 2018	3.2.1	1.0	Updated to align with PCI DSS v3.2.1. For details of PCI DSS changes, see PCI DSS – Summary of Changes from PCI DSS Version 3.2 to 3.2.1

Before You Begin

SAQ D for Service Providers applies to all service providers defined by a payment brand as being SAQ-eligible.

While many organizations completing SAQ D will need to validate compliance with every PCI DSS requirement, some organizations with very specific business models may find that some requirements do not apply. See the guidance below for information about the exclusion of certain, specific requirements.

PCI DSS Self-Assessment Completion Steps

1. Confirm that your environment is properly scoped.
2. Assess your environment for compliance with PCI DSS requirements.
3. Complete all sections of this document:
   - Section 1 (Parts 1 & 2 of the AOC) – Assessment Information and Executive Summary
   - Section 2 – PCI DSS Self-Assessment Questionnaire (SAQ D)
   - Section 3 (Parts 3 & 4 of the AOC) – Validation and Attestation Details and Action Plan for NonCompliant Requirements (if applicable)
4. Submit the SAQ and Attestation of Compliance (AOC), along with any other requested documentation—such as ASV scan reports—to the payment brand, or other requester.

Understanding the Self-Assessment Questionnaire

The questions contained in the "PCI DSS Question" column in this self-assessment questionnaire are based on the requirements in the PCI DSS.

Additional resources that provide guidance on PCI DSS requirements and how to complete the selfassessment questionnaire have been provided to assist with the assessment process. An overview of some of these resources is provided below:

Document	Includes:
PCI DSS (PCI Data Security Standard Requirements and Security Assessment Procedures)	• Guidance on Scoping • Guidance on the intent of all PCI DSS Requirements • Details of testing procedures • Guidance on Compensating Controls
SAQ Instructions and Guidelines documents	• Information about all SAQs and their eligibility criteria • How to determine which SAQ is right for your organization
PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms	• Descriptions and definitions of terms used in the PCI DSS and self-assessment questionnaires

These and other resources can be found on the PCI SSC website (www.pcisecuritystandards.org). Organizations are encouraged to review the PCI DSS and other supporting documents before beginning an assessment.

Expected Testing

The instructions provided in the "Expected Testing" column are based on the testing procedures in the PCI DSS, and provide a high-level description of the types of testing activities that should be performed in order to verify that a requirement has been met. Full details of testing procedures for each requirement can be found in the PCI DSS.

Completing the Self-Assessment Questionnaire

For each question, there is a choice of responses to indicate your company's status regarding that requirement. **Only one response should be selected for each question.**

A description of the meaning for each response is provided in the table below:

Response	When to use this response:
Yes	The expected testing has been performed, and all elements of the requirement have been met as stated.
Yes with CCW (Compensating Control Worksheet)	The expected testing has been performed, and the requirement has been met with the assistance of a compensating control. All responses in this column require completion of a Compensating Control Worksheet (CCW) in Appendix B of the SAQ. Information on the use of compensating controls and guidance on how to complete the worksheet is provided in the PCI DSS.
No	Some or all elements of the requirement have not been met, or are in the process of being implemented, or require further testing before it will be known if they are in place.
N/A (Not Applicable)	The requirement does not apply to the organization's environment. (See Guidance for Non-Applicability of Certain, Specific Requirements below for examples.) All responses in this column require a supporting explanation in Appendix C of the SAQ.
Not Tested	The requirement was not included for consideration in the assessment, and was not tested in any way. (See Understanding the difference between Not Applicable and Not Tested below for examples of when this option should be used.) All responses in this column require a supporting explanation in Appendix D of the SAQ.

Guidance for Non-Applicability of Certain, Specific Requirements

While many organizations completing SAQ D will need to validate compliance with every PCI DSS requirement, some organizations with very specific business models may find that some requirements do not apply. For example, a company that does not use wireless technology in any capacity would not be expected to validate compliance with the sections of the PCI DSS that are specific to managing wireless technology. Similarly, an organization that does not store any cardholder data electronically at any time would not need to validate requirements related to secure storage of cardholder data (for example, Requirement 3.4).

Examples of requirements with specific applicability include:

- The questions specific to securing wireless technologies (for example, Requirements 1.2.3, 2.1.1, and 4.1.1) only need to be answered if wireless is present anywhere in your network. Note that Requirement 11.1 (use of processes to identify unauthorized wireless access points) must still be answered even if you don't use wireless technologies in your network, since the process detects any rogue or unauthorized devices that may have been added without your knowledge.
- The questions specific to application development and secure coding (Requirements 6.3 and 6.5) only need to be answered if your organization develops its own custom applications
- The questions for Requirements 9.1.1 and 9.3 only need to be answered for facilities with "sensitive areas" as defined here: "Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store, but does include retail store back-office server rooms that store cardholder data, and storage areas for large quantities of cardholder data

If any requirements are deemed not applicable to your environment, select the "N/A" option for that specific requirement, and complete the "Explanation of Non-Applicability" worksheet in Appendix C for each "N/A" entry

Understanding the difference between Not Applicable and Not Tested

Requirements that are deemed to be not applicable to an environment must be verified as such. Using the wireless example above, for an organization to select "N/A" for Requirements 1.2.3, 2.1.1, and 4.1.1, the organization would first need to confirm that there are no wireless technologies used in their cardholder data environment (CDE) or that connect to their CDE. Once this has been confirmed, the organization may select "N/A" for those specific requirements,

If a requirement is completely excluded from review without any consideration as to whether it could apply, the "Not Tested" option should be selected. Examples of situations where this could occur may include:

- An organization may be asked by their acquirer to validate a subset of requirements—for example: using the prioritized approach to validate certain milestones.
- An organization may wish to validate a new security control that impacts only a subset of requirements—for example, implementation of a new encryption methodology that requires assessment of PCI DSS Requirements 2, 3 and 4.
- A service provider organization might offer a service which covers only a limited number of PCI DSS requirements—for example, a physical storage provider may only wish to validate the physical security controls per PCI DSS Requirement 9 for their storage facility.

In these scenarios, the organization only wishes to validate certain PCI DSS requirements even though other requirements might also apply to their environment.

Legal Exception

If your organization is subject to a legal restriction that prevents the organization from meeting a PCI DSS requirement, check the "No" column for that requirement and complete the relevant attestation in Part 3.

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:	AudienceView Campus		DBA (doing business as):		
Contact Name:	Derek Mitchell		Title:	Product Manager	
Telephone:	845-764-9800		E-mail:	derek.mitchell@audienceview.com	
Business Address:	4 Union Street, Suite 24		City:	Bangor	
State/Province:	Maine	Country:	USA	Zip:	04401
URL:	www.audienceview.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:

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):		

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 2. Executive Summary (continued)

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:

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:

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.

AudienceView Campus accepts credit card information and transmits this to our gateway or the client-owned gateway for processing.

Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.

AudienceView Campus is involved in the collection and transmission of card information.

Part 2. Executive Summary (continued)

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)
Corporate Office	1	Toronto, Ontario, Canada
Satellite Office	1	Bangor, Maine
Amazon Web Services Data Center	1	Virginia

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)
Stripe, Inc.	3.0.x.y	Stripe.com, Inc.	(•) Yes ( ) No	2020-10-28
CASHNet	30G11 Bui	CASHNet	( ) Yes (•) No	
Authorize.net	UNK	Cybersource Corporati	( ) 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.*

Web and database servers are hosted via Amazon Web Services. The AudienceView Campus application and payment input form, transmission of card information to gateway, and POS hardware as supported by the payment gateway (including the Verifone P400 via Stripe and the Ingenico iSC 250 with Touchnet.)

Does your business use network segmentation to affect the scope of your PCI DSS environment? ( ) Yes (•) No

(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation.)

Part 2. Executive Summary (continued)

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:	
QIR Individual Name:	
Description of services provided by QIR:	

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:**
Clone Systems	PCI Scanning
Authorize.net	Payment Gateway
Stripe	Payment Gateway
Square	Payment Gateway
TouchNet	Payment Gateway
CASHNet	Payment Gateway

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

Part 2. Executive Summary (continued)

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: AudienceView Campus

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:	◉	○	○	
Requirement 3:	◉	○	○	
Requirement 4:	◉	○	○	
Requirement 5:	◉	○	○	
Requirement 6:	◉	○	○	
Requirement 7:	◉	○	○	
Requirement 8:	◉	○	○	
Requirement 9:	◉	○	○	
Requirement 10:	◉	○	○	
Requirement 11:	◉	○	○	
Requirement 12:	◉	○	○	
Appendix A1:	◉	○	○	
Appendix A2:	◉	○	○	

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ D-SP (Section 2), dated (SAQ completion date).

Based on the results documented in the SAQ D-SP 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 D-SP are complete, and all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby (AudienceView Campus) has demonstrated full compliance with the PCI DSS.
○	**Non-Compliant:** Not all sections of the PCI DSS SAQ D-SP are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby () 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-SP, 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.
☑	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 Clone Systems

[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 3b. Service Provider Attestation

Lawrence Franco
Lawrence Franco (Aug 10, 2020 12:30 EDT)

Signature of Service Provider Executive Officer	Date: 2020-08-10
Service Provider Executive Officer Name: Lawrence Franco	Title: Chief Operating Officer

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:

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 payment brand(s) before completing Part 4.

PCI DSS Requirement*	Description of Requirement	Compliance 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.	◉	○	

* PCI DSS Requirements indicated here refer to the questions in Section 2 of the SAQ.