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:	Quavo, Inc		DBA (doing business as):	N/A	
Contact Name:	Nick Facca		Title:	Director of Technology	
Telephone:	(248) 318-1661		E-mail:	nick.facca@quavo.com	
Business Address:	333 Albert St Stuite 210		City:	East Lansing	
State/Province:	MI	Country:	USA	Zip:	48823
URL:	https://www.quavo.com				
Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	Cadence Assurance, LLC				
Lead QSA Contact Name:	Garrett Hendrickson		Title:	QSA	
Telephone:	(816) 401-5140		E-mail:	garrett@thecadencegroup.com	
Business Address:	PO Box 711190		City:	Salt Lake City	
State/Province:	UT	Country:	USA	Zip:	84171
URL:	https://thecadencegroup.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:	QFD	
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): Software-as-a-Service		

***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:	N/A

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.	Quavo offers a hosted SaaS software solution called QFD that assists issuing financial institutions to process exceptions as a result of cardholder disputes after purchase or experiencing fraud. Quavo's platform stores, processes and transmits cardholder data during this process to perform chargebacks through payment networks such as Visa and Mastercard, perform accounting adjustments to cardholder accounts, send communication, etc.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Quavo receives data from issuing financial institutions core banking or processing systems. Data is subsequently retrieved and cases/fraud reports/chargebacks issued to Visa and Mastercard.

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*
Datacenter	1	AWS US East 1 Region

Operations Center	1	Tempe, AZ, 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)
N/A			☐ 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. *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.*	Connections into the CDE included web application traffic for the QFD solution, API traffic containing records from their customer financial institutions' core banking or processing systems, and administrator access for maintaining the environment. Connections out of the CDE included cases/fraud reports and chargebacks issued to Visa and Mastercard. Critical system components within the CDE includec: - Load Balancers - Security Groups - Databases - Web Servers - Web Application Firewall - VPN Concentrators
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:	N/A
QIR Individual Name:	N/A
Description of services provided by QIR:	N/A

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:**
Amazon Web Services	Infrastructure Hosting
Microsoft Azure	Cloud-based Active Directory and SSO Provider
Pega	Custom Code Development
Datadog	Cloud-based SEIM and Log Aggregation
Foxpass	Cloud-based Authentication Provider

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:	QFD

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 - Determined no wireless devices were in-scope.** **2.6; N/A - Determined Quavo was not a shared hosting provider.**
Requirement 3:	☐	☒	☐	**3.2.a - 3.2.c; N/A - Determined that SAD was not received nor stored.** **3.4.1.a - 3.4.1.c; N/A - Determined that full disk encryption was not used.** **3.6.b; N/A - Determined that Quavo did not share encryption keys with customers.** **3.6.6; N/A - Determined that Quavo did not utilize clear-text key-management operations.**
Requirement 4:	☐	☒	☐	**4.1.1; N/A - Determined no wireless devices were in-scope.** **4.2.a; N/A - Determined PAN was not send via end-user messaging technologies.**
Requirement 5:	☒	☐	☐	
Requirement 6:	☐	☒	☐	**6.4.4; N/A - Determined that Quavo did not hardcode test data or accounts that could be migrated in code to production.**

				6.4.6; N/A - As the environment had only recently been implemented, no significant changes had occurred.
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	**8.1.5; N/A - Determined no vendor access was utilized.** **8.1.6.b, 8.2.1.b, 8.2.3.b, 8.2.4.b, 8.2.5.b; N/A- Determined non-consumer customer. accounts were only able to be provisioned through customer-managed SSO providers.** **8.5.1; N/A - Determined Quavo only had access to Quavo-managed infrastructure.**
Requirement 9:	☐	☒	☐	**9.5 - 9.8.2; N/A - CHD was not stored on any removable digital or physical media.** **9.9 - 9.9.3; N/A - POS/POI devices were not in use in the environment.**
Requirement 10:	☒	☐	☐	
Requirement 11:	☐	☒	☐	**11.1, 11.1.1-11.1.2; N/A - Determined that all network infrastructure at in-scope physical locations was out-of-scope for PCI.** **11.2.3; N/A - As this was an initial assessment, no significant changes had taken place.**
Requirement 12:	☒	☐	☐	
Appendix A1:	☐	☐	☒	**A1.1 - A1.4; N/A - Determined Quavo was not a shared hosting provider.**
Appendix A2:	☐	☐	☒	**A2.1 - A2.3; N/A - Determined Quavo did not utilize POS/POI terminals within their CDE.**

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:	August 20, 2021	
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 *August 20, 2021.*

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 *Quavo, 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 *3.2.1*, 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 *Clone Systems, Inc*

Part 3b. Service Provider Attestation

DocuSigned by:
David Chmielewski
56D9790F095A41C...

Signature of Service Provider Executive Officer ↑	*Date:* 8/20/2021
Service Provider Executive Officer Name: **David Chmielewski**	*Title:* **Managing Partner**

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

If a QSA was involved or assisted with this assessment, describe the role performed:	QSA performed validation of scope and testing of all applicable requirements.

DocuSigned by:
Jonathan Smith
96671BBEC5F348D...

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* 8/20/2021
Duly Authorized Officer Name: **Jonathan Smith**	*QSA Company:* **Cadence Assurance, LLC**

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:	N/A

[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.	☒	☐	

DocuSign

Certificate Of Completion

Envelope Id: DBA1D342A8ED48D6A45502F55DA9E75C
Status: Completed
Subject: Please DocuSign: 2021 Quavo AOC-SAQ_D_ServiceProvider-v3_2_1 (1).pdf
Client ID: 822828
Engagement Code (123456.XXXX):
Office Location:
Seattle
Source Envelope:
Document Pages: 12
Signatures: 2
Certificate Pages: 3
Initials: 0
AutoNav: Enabled
EnvelopeId Stamping: Enabled
Time Zone: (UTC-08:00) Pacific Time (US & Canada)

Envelope Originator:
Amy DeHaan
999 Third Avenue
Suite 2800
Seattle, WA 98104
Amy.DeHaan@mossadams.com
IP Address: 174.52.235.108

Record Tracking

Status: Original
8/20/2021 10:02:27 AM
Security Appliance Status: Connected

Holder: Amy DeHaan
Amy.DeHaan@mossadams.com
Pool: Security Pool

Location: DocuSign

Signer Events	Signature	Timestamp
David Chmielewski david.chmielewski@quavo.com Managing Partner Security Level: Email, Account Authentication (None)	DocuSigned by:  56D9790F095A41C... Signature Adoption: Pre-selected Style Using IP Address: 3.224.144.170	Sent: 8/20/2021 10:06:00 AM Viewed: 8/20/2021 10:07:58 AM Signed: 8/20/2021 10:08:23 AM
Electronic Record and Signature Disclosure: Accepted: 8/20/2021 10:07:58 AM ID: 72f02d2d-776a-44c6-bf7f-d66fe7b9eded		
Jonathan Smith jonathan.smith@mossadams.com Security Level: Email, Account Authentication (None)	DocuSigned by:  96671BBEC5F348D... Signature Adoption: Pre-selected Style Using IP Address: 166.70.24.210	Sent: 8/20/2021 10:08:24 AM Viewed: 8/20/2021 10:18:48 AM Signed: 8/20/2021 10:19:02 AM
Electronic Record and Signature Disclosure: Accepted: 8/20/2021 10:18:48 AM ID: 9dfde0d9-6bb9-4e4c-9d98-64c0914ec755		

In Person Signer Events	Signature	Timestamp

Editor Delivery Events	Status	Timestamp

Agent Delivery Events	Status	Timestamp

Intermediary Delivery Events	Status	Timestamp

Certified Delivery Events	Status	Timestamp

Carbon Copy Events	Status	Timestamp

Witness Events	Signature	Timestamp

Notary Events	Signature	Timestamp

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	8/20/2021 10:06:00 AM
Certified Delivered	Security Checked	8/20/2021 10:18:48 AM
Signing Complete	Security Checked	8/20/2021 10:19:02 AM
Completed	Security Checked	8/20/2021 10:19:02 AM

Payment Events	Status	Timestamps

Electronic Record and Signature Disclosure

CONSENT FOR USE OF ELECTRONIC SIGNATURES AND DOCUMENTS

By selecting the "I Accept" button, you are signing this document electronically. You agree your electronic signature is the legal equivalent of your handwritten signature on this document. By selecting "I Accept" using any device, means or action, you consent to the legally binding terms and conditions of this document. You further agree that your signature on this document (your "E-Signature") is as valid as if you signed the document in writing. You also agree that no certification authority or other third party verification is necessary to validate your E-Signature, and that the lack of such certification or third party verification will not in any way affect the enforceability of your E-Signature or any resulting agreement between you and Moss Adams LLP. You are also confirming that you are authorized to sign this document. Finally, you understand and agree that your E-Signature will be legally binding and such transaction will be considered authorized by you.