Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

June 2018

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:	Paya Inc.		DBA (doing business as):	N/A	
Contact Name:	Alex Tan		Title:	Chief Security Officer	
Telephone:	470.489.1155		E-mail:	alex.tan@paya.com	
Business Address:	303 Perimeter Center N #600		City:	Atlanta	
State/Province:	GA	Country:	USA	Zip:	30346
URL:	https://www.paya.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	Coalfire Systems, Inc.				
Lead QSA Contact Name:	Irfan Khawaja		Title:	Sr. Security Consultant	
Telephone:	303.554.6333		E-mail:	coalfiresubmission@coalfire.com	
Business Address:	11000 Westmoor Circle, Suite 450		City:	Westminster	
State/Province:	CO	Country:	USA	Zip:	80021
URL:	https://www.coalfire.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:	Paya – Payment Gateway	
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): Virtual Terminal Applications
☐ 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 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:	Not Applicable	
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):		
Provide a brief explanation why any checked services were not included in the assessment:	Not Applicable	

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Paya is a Level 1 service provider that provides payment gateway services for card-present and card-not-present (eCommerce) transactions for small to mid-size merchants. Paya customers include retail stores, Internet merchants, sales organizations, utility companies, government agencies, Internet Service Providers, trade associations, financial institutions, gas and convenience stores, hotels, restaurants and entertainment outlets, web hosting companies, newspapers, and medical institutions. Paya also provides payment processing gateway services to other companies that resell Paya services to their own customers. Paya does not receive cardholder data directly from payment terminals that are implemented at the merchant locations; track data at the time of card swipe/dip is transmitted directly from the payment terminal to payment processors (TSYS, Paymentech, or First Data) over private MPLS connections. After authorization, payment processors send Paya transactional data that includes first four and last four digits of the PAN data and is stored in SQL databases on the Paya internal network using AES-128 encryption. For the eCommerce side of the business, Paya receives payment card transactions securely over the Internet from merchant client websites using a redirect page from their websites to the Paya gateway at www.sagepayment.net using HTTPS/TLS v1.2 or higher with AES 128-bit encryption. Paya Gateway receives encrypted cardholder data and uses Magensa services to decrypt the CHD. Decrypted data then transmits to a payment processor (TSYS, First Data, or Paymentech) over a dedicated MPLS circuit using TLS v1.2 or higher with AES 128-bit encryption. Payment processors receive and authorize a transaction and return an authorization code to Paya Gateway to be stored in a Paya SQL database. Finally, Paya Gateway submits the authorization code to its customers. No sensitive authorization data is retained after authorization. Paya eCommerce services also include Point of Sales (POS) transaction processing through the Virtual Terminal applications and Gateway API. Merchants can download and install these applications on their POS systems (typically Windows Workstation) to send transactions for processing. These applications include, Virtual Terminal 4 (VT4), Payment Center Virtual Terminal (PCVT), Paya Exchange Virtual Desktop (PEVT), Paya Exchange Virtual Desktop (PEVD), Donate Now, Shopping Cart, and Paya Vault. Paya merchants who use Virtual Terminal can review transactions with truncated PAN through the Virtual Report application. The Paya risk and fraud team uses the TCAT (To Catch a Thief) application to research transactions and review risk flags for merchants.

Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Not Applicable

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):
Paya Headquarters	1	Atlanta, GA
Co-location Datacenters	1	Suwanee, GA

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)
Paya Exchange Desktop (PED)	2.0.2.31	Paya, Inc.	☒ Yes ☐ No	28 Oct 2022
Virtual Terminal Application	061818-9167	Paya, Inc.	☐ Yes ☒ No	Not Applicable
Payment Center Virtual Terminal (PCVT)	062218-1725	Paya, Inc.	☐ Yes ☒ No	Not Applicable
Paya Exchange Virtual Desktop (PEVD)	061918-6791	Paya, Inc.	☐ Yes ☒ No	Not Applicable
Paya Exchange Virtual Terminal (PEVT)	062218-9254	Paya, Inc.	☐ Yes ☒ No	Not Applicable
Paya Vault	062118-9240	Paya, Inc.	☐ Yes ☒ No	Not Applicable
To Catch a Thief (TCAT)	032318-8969	Paya, Inc.	☐ Yes ☒ No	Not Applicable
Sage API	070218-9354	Paya, Inc.	☐ Yes ☒ No	Not Applicable
Shopping Cart	060418-9060	Paya, Inc.	☐ Yes ☒ No	Not Applicable
Donate Now	061818-9167	Paya, Inc.	☐ Yes ☒ No	Not Applicable

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).*	Paya is a Level 1 service provider that provides Payment Gateway services to its merchant clients. Paya headquarters are in Dunwoody, GA and they utilize a co-location datacenter in Suwanee, GA for the cardholder data environment. Paya personnel involved in the management and support of cardholder data environment include

• *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	Systems, Network, and Database Administrators, Application Developers, Security Managers, and Human Resources. Paya does not manage or maintain payment terminals implemented at its merchant clients. Cardholder data from merchant POS systems and from eCommerce websites to the Paya network is transmitted over HTTPS/TLS v1.2 or higher with AES 128-bit encryption. Paya has implemented technologies within its in-scope environment to ensure confidentiality of cardholder data. Technologies include, firewalls, load balancer, IDS/IPS, network segmentation, anti-virus, FIM, patch process, logging and monitoring, pen testing, and vulnerability scanning.
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
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:**
Quality Technology Services, LLC.	Co-location data center hosting provider – Suwanee (GA)
Magensa, LLC.	Encryption and Decryption of PAN Data
Kount Inc.	Fraud Analysis
Splunk	Audit and Systems Logs
TSYS Acquiring Solutions	Payment Processor
First Data Merchant Service	Payment Processor
Chase Paymentech	Payment Processor
Bluefin	Payment Processor

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:	Paya – Payment Gateway

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:	☐	☒	☐	**Not Applicable** **2.1.1 – No wireless network in the CDE** **2.2.3 – No unsecure ports and protocols running** **2.6 – Not a shared hosting provider**
Requirement 3:	☐	☒	☐	**Not Applicable** **3.4.1 – No disk encryption in use** **3.6 – No key sharing with customers** **3.6.2 – No cryptographic key distribution** **3.6.6 – No manual clear-text key management**
Requirement 4:	☐	☒	☐	**Not Applicable** **4.1.1 – No wireless to transmit card data**
Requirement 5:	☐	☒	☐	**Not Applicable** **5.1.2 – No systems that are not commonly affected by malicious software**
Requirement 6:	☐	☒	☐	**Not Applicable** **6.4.6 – No significant changes in the environment**
Requirement 7:	☒	☐	☐	

Requirement 8:	☐	☒	☐	**Not Applicable** **8.5.1 – No remote access to customers**
Requirement 9:	☐	☒	☐	**Not Applicable** **9.5-All– No removable media in the environment** **9.6-All– No removable media in the environment** **9.7-All– No removable media in the environment** **9.8-All– No removable media in the environment** **9.9-All – No payment terminals in the environment**
Requirement 10:	☒	☐	☐	
Requirement 11:	☐	☒	☐	**Not Applicable** **11.2.3 – No significant changes in the environment**
Requirement 12:	☒	☐	☐	
Appendix A1:	☐	☒	☐	**Not Applicable** **Paya is not a shared hosting provider**
Appendix A2:	☐	☒	☐	**Not Applicable** **Paya does not have POI/POS devices in-scope**

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:	*8/3/2020*	
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

This AOC is based on results noted in the ROC dated *8/3/2020.*

Based on the results documented in the ROC 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 ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *Paya, Inc.* 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 *Not Applicable* has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: Not Applicable 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
Not Applicable	Not Applicable
Not Applicable	Not Applicable

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 *3.2.1*, 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.

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 *Tenable Networks*

Part 3b. Service Provider Attestation	
Signature of Service Provider Executive Officer ↑	*Date:* 8/3/2020
Service Provider Executive Officer Name: **Alex Tan**	*Title:* **Chief Security Officer**

DocuSigned by: Alex Tan 5EC9417D0B8D430...

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)	
If a QSA was involved or assisted with this assessment, describe the role performed:	The Coalfire QSA verified scope of the environment, reviewed business processes and policy and procedure documents, examined network and data flow diagrams, and reviewed systems and applications inventory. The Coalfire QSA interviewed subject matter experts to discuss business processes, requested and reviewed evidence such as screenshots and system generated reports of sampled systems, discussed onboarding and off-boarding process with HR, and reviewed processes and procedures to validate PCI DSS v3.2.1 compliance activities. Additionally, the Coalfire QSA performed research on service providers and other critical technologies used within the Paya in-scope environment, conducted follow up meetings, and wrote the PCI DSS v3.2.1 Report on Compliance.

DocuSigned by: Irfan Khawaja 12D34D37AD0D44F...

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* 8/3/2020
Duly Authorized Officer Name: Irfan Khawaja	*QSA Company:* Coalfire Systems, Inc.

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 No ISAs were involved in this assessment.

[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	☒	☐