Payment Card Industry
Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0

Revision 2

Publication Date: August 2023

PCI DSS v4.0 Attestation of Compliance for Report on Compliance – Service Providers

Entity Name: Entity Name: Paya Inc (dba Paya EFT)

Date of Report: June 30, 2024

Assessment End Date: June 30, 2024

Date of Report as noted in the Report on Compliance: June 30, 2024

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance (AOC) must be completed as a declaration of the results of the service provider's assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures (*"Assessment"). Complete all sections. The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which this AOC will be submitted for reporting and submission procedures.

This AOC reflects the results documented in an associated Report on Compliance (ROC). Associated ROC sections are noted in each AOC Part/Section below.

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Report on Compliance Template.

Part 1. Contact Information	
Part 1a. Assessed Entity (ROC Section 1.1)	
Company name:	Paya Inc.
DBA (doing business as):	Paya EFT
Company mailing address:	303 Perimeter Center N, Suite 600, Atlanta GA 30346
Company main website:	https://paya.com
Company contact name:	Alex Tan
Company contact title:	Chief Information Security Officer
Contact phone number:	470-489-1155
Contact e-mail address:	alex.tan@paya.com
Part 1b. Assessor (ROC Section 1.1)	
Provide the following information for all assessors involved in the Assessment. If there was no assessor for a given assessor type, enter Not Applicable.	
PCI SSC Internal Security Assessor(s)	
ISA name(s):	Not Applicable.
Qualified Security Assessor	
Company name:	AARC-360
Company mailing address:	8000 Avalon Boulevard Suite 100, Alpharetta GA 30009
Company website:	https://www.aarc-360.com
Lead Assessor name:	James Spence
Assessor phone number:	(866) 576-4414 ex 108
Assessor e-mail address:	James.Spence@AARC-360.com

Assessor certificate number:	025-041

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the Assessment (select all that apply):

Name of service(s) assessed:	Paya – Payment Gateway

Type of service(s) assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☒ POI / 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-hosting services		Virtual Terminal Applications
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Multi-Tenant Service 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 these categories do not apply to the assessed service, complete "Others." If it is not clear whether a category could apply to the assessed service, consult with the entity(ies) to which this AOC will be submitted.*

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 Assessment (select all that apply):

Name of service(s) not assessed:	Not Applicable

Type of service(s) not assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POI / 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-hosting services		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Multi-Tenant Service 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:	Not Applicable

Part 2b. Description of Role with Payment Cards (ROC Section 2.1)

Describe how the business stores, processes, and/or transmits account data.	**Transmission –** Paya receives payment card transactions securely over the Internet from merchants and Independent Sales Organizations (ISOs) via Paya developed web applications, API integration with third parties, or Class A terminals. ISOs may integrate card present, card not present, and MOTO into their independently developed and assessed solution. Data captured from Class A terminals is encrypted at swipe and is forwarded directly to a third-party

	processor; CHD never touches the Paya network. Paya never has access to any CHD and only stores a reference code as a record of the transaction. **Processing –** Paya receives all payment card transaction data from Internet-based e-commerce transactions and collects and processes payment card transactions required for conducting business. Data may include sensitive data required for payment card transaction authorization and data required for transaction processing with a third-party processor (TSYS, Chase Paymentech, First Data, or Bluefin). No sensitive authentication data is retained for any reason post authorization. **Storage –** Paya stores PAN data within Microsoft SQL database instances using PCI DSS-compliant encryption. Data is retained for 18 months and is automatically deleted using a SQL stored procedure. **Transmission –** Payment card transaction data is securely transported directly to Paya using TLS for processing. **Processing & Storage –** Sensitive authentication data is required for transaction processing with third-party processors (Chase Paymentech, First Data, or TSYS). No sensitive authentication data is retained for any reason post authorization. PAN data may be required for batch processing, customer inquiry, chargebacks and similar customer-based needs. Data is retained for 18 months and is automatically deleted using a SQL stored procedure. Stored data may be used for transaction reference by a customer service representative or for audit by the risk management team if a red flag is issued. A red flag is when internal financial fraud analysis software identifies a transaction as being suspicious and requires additional review. Access to payment card data is limited to specific authorized individuals and typically only one payment card at a time may be reviewed. In special circumstances (i.e., when a customer merchant leaves Paya, the merchant's encrypted data may be exported and provided to the customer – there are formally defined special procedures for that action.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Cardholder data is transmitted from the customers to the processors encrypted end to end with TLS 1.2 or 1.3 and within a private MPLS network across the bankcard environment. Bankcard cannot access cardholder data. Only Tokenized PAN is stored.

Describe system components that could impact the security of account data.	Payment card data passes to the processors encrypted, and the processor sends a token, first 6 or last 4 digits of PAN and the cardholder's name and expiration data.

Part 2. Executive Summary *(continued)*

Part 2c. Description of Payment Card 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 POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.* • *System components that could impact the security of account data.*	Paya is a level 1 service provider and payment gateway that focuses on small to medium size merchants, processing approximately 126 million transactions annually. Paya provides business payment services: • Multiple payment types including credit and debit cards, electronic checks, gift cards, and automatic recurring payments; • Multiple acceptance platforms including **card present** and e-commerce/**Internet payments (card not present)**. • **Card present** transactions are handled using Class A terminals leased to the merchant. Data captured from Class A terminals is encrypted at swipe and is forwarded directly to a third-party processor. CHD never touches the Paya network. Paya never has access to any CHD and stores only a reference code as a record of the transaction. • **Card Not Present** transactions include Merchant services including merchant accounts, equipment, processing solutions for retail, Mail Order/Telephone Order (MOTO), and Internet businesses, and valuable customer retention tools like loyalty cards, online reporting, and financial resources; and Customized payment solutions that integrate with Paya Software and other third-party software. • **Paya Token Vault** assists merchants in being PCI compliant by providing a non-resident encrypted storage solution. The vault employs a Globally Unique Identifier (GUID) also known as an alias or token, which is stored on the merchant's server or host software to represent the encrypted data securely stored behind our firewall. Paya customers include retail stores, MOTO and 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.
Indicate whether the environment includes segmentation to reduce the scope of the Assessment. (Refer to the "Segmentation" section of PCI DSS for guidance on segmentation)	☒ Yes ☐ No

Part 2d. In-Scope Locations/Facilities (ROC Section 4.6)

List all types of physical locations/facilities (for example, corporate offices, data centers, call centers and mail rooms) in scope for this Assessment.

Facility Type	Total Number of Locations (How many locations of this type are in scope)	Location(s) of Facility (city, country)
Example: Data centers	*3*	*Boston, MA, USA*
Paya Headquarters	1	Atlanta, GA
Co-location Datacenters	1	Suwanee, GA

Part 2. Executive Summary *(continued)*

Part 2e. PCI SSC Validated Products and Solutions (ROC Section 3.3)

Does the entity use any item identified on any PCI SSC Lists of Validated Products and Solutions♦?

☐ Yes ☒ No

Provide the following information regarding each item the entity uses from PCI SSC's Lists of Validated Products and Solutions:

Name of PCI SSC-validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which Product or Solution Was Validated	PCI SSC Listing Reference Number	Expiry Date of Listing
Paya Exchange Desktop (PED)	2.0.2.31	PA-DSS		28 Oct 2022
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD

♦ For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components appearing on the PCI SSC website (www.pcisecuritystandards.org)—for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Payment Applications (PA-DSS), Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, and Contactless Payments on COTS (CPoC) solutions.

Part 2f. Third-Party Service Providers **(ROC Section 4.4)**	
For the services being validated, does the entity have relationships with one or more third-party service providers that:	
• Store, process, or transmit account data on the entity's behalf (for example, payment gateways, payment processors, payment service providers (PSPs, and off-site storage))	☒ Yes ☐ No
• Manage system components included in the entity's Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting companies, and IaaS, PaaS, SaaS, and FaaS cloud providers)	☒ Yes ☐ No
• Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).	☒ Yes ☐ No

If Yes:

Name of Service Provider:	**Description of Services Provided:**
Quality Technology Services, LLC. (QTS)	Co-location data center hosting provider – Suwanee (GA)
Magensa, LLC.	Encryption and Decryption of PAN Data
TSYS Acquiring Solutions	Payment Processor
First Data Merchant Service	Payment Processor
Chase Paymentech	Payment Processor
Bluefin	Gateway and ISO

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

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment (ROC Section 1.8.1)

Indicate below all responses provided within each principal PCI DSS requirement.

For all requirements identified as either "Not Applicable" or "Not Tested," complete the "Justification for Approach" table below.

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: ***Bankcard***

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If Below Method(s) Was Used	
	In Place	Not Applicable	Not Tested	Not in Place	Customized Approach	Compensating Controls
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:	☐	☒	☐	☐	☐	☐
Justification for Approach						

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	1.3.3 - No wireless in scope. 1.4.4 - System components that store cardholder data are not directly accessible from untrusted networks. 2.2.5 - No insecure services, protocols, or daemons are present. 2.3.1, 2.3.2 - No wireless environments. 3.3.1 - No SAD is accessible or stored. 3.3.1.1 - 3.3.1.3 - Payment processes are not in scope. No authorization data is accessible or stored. 3.3.2 - Payment processes are not in scope. No authorization data is accessible or stored. 3.3.3 - Bankcard is not an issuer. 3.5.1 - 3.7.9 - Only Tokenized PAN is stored. 4.2.1.1 - Best practice until 31 March 2025. 4.2.1.2 - No Wireless networks in scope. 4.2.2 - PAN is not sent via end user messaging. 5.2.3 - All systems in scope have endpoint protection/AV. 5.3.2.1, 5.3.3, 5.4.1 - Best practice until 31 March 2025. 6.3.2, 6.4.2, 6.4.3 - Best practice until 31 March 2025. 7.2.4, 7.2.5, 7.2.5.1 - Best practice until 31 March 2025. 8.2.3 - Bankcard does not use/need remote access to customer premises. 8.2.7 - Third parties are not granted access. 8.3.6 - Best practice until 31 March 2025. 8.3.10 - 8.3.10.1 - Best practice until 31 March 2025. 8.3.11 - No authentication factors are shared or groups. 8.4.2 - Best practice until 31 March 2025. 8.5.1, 8.6.1, 8.6.2, 8.6.3 - Best practice until 31 March 2025. 9.4.1, 9.4.1.1, 9.4.1.2, 9.4.2-9.4.7.b - No media with cardholder data. 9.5 - 9.5.1.3.b - No POI in scope. 10.4.2.1, 10.7.3 - Best practice until 31 March 2025. 11.2.2 - No wireless in scope 11.3.1.1, 11.3.1.2 - Best practice until 31 March 2025. 11.4.7 - Not a multi-tenant service provider. 11.5.1.1, 11.6.1 - Best practice until 31 March 2025. 12.3.1, 12.3.3, 12.3.4, 12.5.2.1, 12.5.3, 12.6.2, 12.6.3.1, 12.6.3.2, 12.10.4.1, 12.10.7 - Best practice until 31 March 2025. 12.3.2 - Customized approach has not been used. A1 - Bankcard is not a Multi-Tenant Service Provider. A2 - Bankcard does not have Card-Present transactions.

	A3 - Not a Designated Entity.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	None

Section 2 Report on Compliance

(**ROC Sections 1.2 and 1.3.2**)

Date Assessment began: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*			February 2, 2024
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*			June 30, 2024
Were any requirements in the ROC unable to be met due to a legal constraint?			☐ Yes ☒ No
Were any testing activities performed remotely? If yes, for each testing activity below, indicate whether remote assessment activities were performed:			☒ Yes ☐ No
• Examine documentation	☒ Yes	☐ No	
• Interview personnel	☒ Yes	☐ No	
• Examine/observe live data	☒ Yes	☐ No	
• Observe process being performed	☒ Yes	☐ No	
• Observe physical environment	☐ Yes	☒ No	
• Interactive testing	☒ Yes	☐ No	
• Other:	☐ Yes	☐ No	

Section 3 Validation and Attestation Details

Part 3. PCI DSS Validation (ROC Section 1.7)

This AOC is based on results noted in the ROC dated *(Date of Report as noted in the ROC June 30, 2024)*.

Indicate below whether a full or partial PCI DSS assessment was completed:

☒ **Full Assessment** – All requirements have been assessed and therefore no requirements were marked as Not Tested in the ROC.

☐ **Partial Assessment** – One or more requirements have not been assessed and were therefore marked as Not Tested in the ROC. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the ROC noted above, each signatory identified in any of Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document *(select one)**:***

☒	**Compliant:** All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT** rating; thereby ***Bankcard*** has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating; thereby *(Service Provider Company Name)* has not demonstrated compliance with PCI DSS requirements. **Target Date** for Compliance: *YYYY-MM-DD* An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4.
☐	**Compliant but with Legal exception:** One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *(Service Provider Company Name)* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction. This option requires additional review from the entity to which this AOC will be submitted. *If selected, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement from being met

Part 3. PCI DSS Validation *(continued)*

Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:
(Select all that apply)

☒	The ROC was completed according to *PCI DSS*, Version 4.0 and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
☒	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Service Provider Attestation

Alex Tan
Alex Tan (Jul 3, 2024 14:39 EDT)

Signature of Service Provider Executive Officer ↗	Date: 03/07/24
Service Provider Executive Officer Name: Alex Tan	Title: CISO

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this Assessment, indicate the role performed:	☒ QSA performed testing procedures.
	☒ QSA provided other assistance. If selected, describe all role(s) performed: Completed ROC/AOC

Signature of Lead QSA ↗	Date: July 3, 2024
Lead QSA Name: James Spence	

Signature of Duly Authorized Officer of QSA Company ↗	Date: July 3, 2024
Duly Authorized Officer Name: Neil Gonsalves	QSA Company: AARC-360

Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

If an ISA(s) was involved or assisted with this Assessment, indicate the role performed:	☐ ISA(s) performed testing procedures.
	☐ ISA(s) provided other assistance. If selected, describe all role(s) performed:

Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has Non-Compliant results noted in Section 3.

If asked to complete this section, select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement below. For any "No" responses, include the date the entity expects to be compliant with the requirement and provide a brief description of the actions being taken to meet the requirement.

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 network security controls	☐	☐	
2	Apply secure configurations to all system components	☐	☐	
3	Protect stored account data	☐	☐	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	☐	☐	
5	Protect all systems and networks from malicious software	☐	☐	
6	Develop and maintain secure systems and software	☐	☐	
7	Restrict access to system components and cardholder data by business need to know	☐	☐	
8	Identify users and authenticate access to system components	☐	☐	
9	Restrict physical access to cardholder data	☐	☐	
10	Log and monitor all access to system components and cardholder data	☐	☐	
11	Test security systems and networks regularly	☐	☐	
12	Support information security with organizational policies and programs	☐	☐	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	☐	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☐	☐	

PCI DSS AOC - Service Providers

Final Audit Report 2024-07-03

Created:	2024-07-03
By:	Neil Gonsalves (neil.gonsalves@aarc-360.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAmXNK8EDU8yB5kqNtra0BGQkSysKCsG1L

"PCI DSS AOC - Service Providers" History

Document created by Neil Gonsalves (neil.gonsalves@aarc-360.com)
2024-07-03 - 6:18:54 PM GMT- IP address: 73.237.24.159

Document emailed to Alex Tan (alex.t@nuvei.com) for signature
2024-07-03 - 6:19:00 PM GMT

Email viewed by Alex Tan (alex.t@nuvei.com)
2024-07-03 - 6:19:20 PM GMT- IP address: 54.194.216.147

Document e-signed by Alex Tan (alex.t@nuvei.com)
Signature Date: 2024-07-03 - 6:39:47 PM GMT - Time Source: server- IP address: 162.206.225.33

Agreement completed.
2024-07-03 - 6:39:47 PM GMT