PCI Security Standards Council®

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: Monek Ltd

Assessment End Date: 14th December 2023

Date of Report as noted in the Report on Compliance: 14th December 2023

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:	Monek Ltd
DBA (doing business as):	Monek
Company mailing address:	Sterling House, Davidson Road, Lichfield, WS14 9DZ
Company main website:	monek.com
Company contact name:	Gareth Berry
Company contact title:	Operations Director
Contact phone number:	+44 (0) 345 2696645
Contact e-mail address:	gareth.berry@monek.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:	Teamwork IMS Ltd
Company mailing address:	200 Brook Drive, Green Park, Reading, RG2 6UB
Company website:	www.teamworkims.co.uk
Lead Assessor name:	Kim Long
Assessor phone number:	+44 (0) 7788 510000
Assessor e-mail address:	kim.long@teamworkims.co.uk
Assessor certificate number:	QSA 204-310

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:	Payment Gateway / Processor

Type of service(s) assessed:

Hosting Provider:

☒ Applications / software
☐ Hardware
☒ Infrastructure / Network
☐ Physical space (co-location)
☒ Storage
☒ Web-hosting services
☐ Security services
☐ 3-D Secure Hosting Provider
☐ Multi-Tenant Service Provider
☐ Other Hosting (specify):

Managed Services:

☐ Systems security services
☐ IT support
☐ Physical security
☐ Terminal Management System
☐ Other services (specify):

Payment Processing:

☒ POI / 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):		

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:

□ Applications / software
□ Hardware
□ Infrastructure / Network
□ Physical space (co-location)
□ Storage
□ Web-hosting services
□ Security services
□ 3-D Secure Hosting Provider
□ Multi-Tenant Service Provider
□ Other Hosting (specify):

Managed Services:

□ Systems security services
□ IT support
□ Physical security
□ Terminal Management System
□ Other services (specify):

Payment Processing:

□ POI / 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:	

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

Describe how the business stores, processes, and/or transmits account data.	Monek provides payment solutions for merchants which support online payment and card machines services. Card details are stored, processed, and transmitted to allow Monek to provide payment services to merchants. Incoming cardholder data from merchant websites / browsers and payment terminals is via TLS v1.2. Transmission of cardholder data is via secure connections to acquiring banks for authorisation and settlement.

	Storage of encrypted cardholder data in the secure database service hosted in MS Azure.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Not Applicable
Describe system components that could impact the security of account data.	Web, loadbalancer, transaction, and database servers along with a lambda serverless architecture are located in the PCI DSS certified AWS and Azure Cloud. Incoming transactions are via TLS1.2, and authorisation & settlement of transaction via secure connections to acquiring banks. A management network within the CDE supports management functions including FIM, vulnerability scanning and monitoring. System Administrators manage the production environment via a zero trust connection through a bastion host to an RDS server. The software development support team manage updates to the environment via the software development pipeline.

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.*	The Environment includes: Web, loadbalancer, transaction & database servers along with a lambda serverless archtitecture located in the PCI DSS certified AWS and Azure Cloud. Incoming transactions via TLS1.2, and authorisation & settlement of transaction via secure connections to acquiring banks. System Administrators manage the production environment via a zero trust connection through a bastion host to an RDS server. Software development support team managing updates to the environment via the software development pipeline.
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*
Data Centre / AWS Region	1	UK, London
Data Centre / Azure Region	1	UK, London

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
				YYYY-MM-DD
				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:**
AWS	Cloud Hosting Platform
Azure	Database Service
BT Cardway	Authorisation routes to the banks for transaction processing.
First Data / FiServ	Authorisation routes to the banks for transaction processing.
CloudFlare	Web Application Firewall / DDoS / Zero Trust software

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: Payment Gateway / Processor

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.	2.3.1, 2.3.2 No wireless networks are connected to the CDE or transmit cardholder data. 3.3.1.3 No PIN data is handled, processed or stored. 3.3.2 Best practice until 31 March 2025 3.3.3 Entity is not an issuer and does not support issuing services 3.5.1.1 Best practice until 31 March 2025 3.5.1.3 Disk or partition level encryption is not used as the primary method for rendering PAN unreadable 4.2.1.2 No wireless networks transmit PAN or are connected to the CDE 5.3.3 Best practice until 31 March 2025 6.4.3 Best practice until 31 March 2025 7.2.5.1 Best practice until 31 March 2025 8.2.3 Not Applicable to the service provided. 8.2.7 Third parties are not given access to the Monek CDE. 8.3.9 All access is via multi factor authentication 8.3.10 No customer user access to cardholder data 8.3.10.1 Best practice until 31 March 2025 9.4 - 9.4.7.b No media is used in the CDE 11.4.7 Not a multi-tenant service provider 11.5.1.1 Best practice until March 31st 2025 11.6.1 Best practice until March 31st 2025 12.3.2 No requirements used the Customized Approach. 12.3.4 Best practice until 31 March 2025 12.10.4.1 Best practice until 31 March 2025 Appendix A1 Not a multi-tenant service provider Appendix A2 No POS POI terminals using SSL and / or early TLS in scope
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	Not Applicable

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.*			2023-12-14
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*			2023-12-14
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 2023-12-14)*.

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 *(Service Provider Company Name)* 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

Signature of Service Provider Executive Officer ↑	Date: 14/12/23
Service Provider Executive Officer Name: Gareth Berry	Title: Operations Director

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:

KLong

Signature of Lead QSA ↑	Date: 2023-12-14
Lead QSA Name: Kim Long	

Signature of Duly Authorized Officer of QSA Company ↑	Date: 2023-12-14
Duly Authorized Officer Name:	QSA Company: Teamwork IMS Ltd

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-v4-0-ROC-AOC-r2-Monek Dec 2023

Final Audit Report 2023-12-14

Created:	2023-12-14
By:	Kim Long (kim.long@teamworkims.co.uk)
Status:	Signed
Transaction ID:	CBJCHBCAABAA_XJzWFI0DdOHOhi7Fkmq9MliXX6xt6n4

"PCI-DSS-v4-0-ROC-AOC-r2-Monek Dec 2023" History

Document created by Kim Long (kim.long@teamworkims.co.uk)
2023-12-14 - 10:23:43 AM GMT- IP address: 84.70.171.100

Document emailed to Oliver Brown (oliver.brown@teamworkims.co.uk) for signature
2023-12-14 - 10:23:48 AM GMT

Email viewed by Oliver Brown (oliver.brown@teamworkims.co.uk)
2023-12-14 - 10:40:14 AM GMT- IP address: 104.47.30.126

Document e-signed by Oliver Brown (oliver.brown@teamworkims.co.uk)
Signature Date: 2023-12-14 - 10:42:16 AM GMT - Time Source: server- IP address: 86.176.116.216

✓ Agreement completed.
2023-12-14 - 10:42:16 AM GMT