Payment Card Industry

Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0.1

Publication Date: August 2024

PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance – Service Providers

Entity Name: Nochex Limited

Date of Report as noted in the Report on Compliance: 19th December, 2024

Date Assessment Ended: 2nd December, 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:	Nochex Limited (“Nochex”)
DBA (doing business as):	Nochex Limited
Company mailing address:	Richmond House, Lawnswood Business Park, Redvers Close, Leeds, LS16 6QY, UK
Company main website:	www.nochex.com
Company contact name:	Khalid Hussain
Company contact title:	Chief Information Officer
Contact phone number:	+447725071291
Contact e-mail address:	Khalid.Hussain@nochex.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:	Data Protection People Limited
Company mailing address:	25-27 The Tannery, 91 Kirkstall Road, Leeds. LS3 1HS., United Kingdom
Company website:	www.dataprotectionpeople.com
Lead Assessor name:	Kenechi Obillor
Assessor phone number:	+447876041412
Assessor e-mail address:	Kene.obillor@dataprotectionpeople.com
Assessor certificate number:	206-571

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:	Nochex Payment Services	
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 Sections 2.1 and 3.1)

Describe how the business stores, processes, and/or transmits account data.	Nochex is a payment facilitator that acts as a conduit between merchant customers and acquiring financial institutions. Merchant customers are provided with a hosted payment page that enables the acceptance of both e-commerce and, in some cases, MOTO payments. Merchant customers can integrate with the hosted payment page using a simple URL redirect link or by embedding the secure.nochex.com page into their website through widget integration. In the interest of security, no other integration options are available. These options ensure that account data is processed

	securely without merchants handling sensitive information. Through secure.nochex.com, Nochex also supports modern payment options such as Apple Pay and Click to Pay, enabling merchants to offer their customers additional payment methods options using Apple Pay and Mastercard wallets. In addition to a control panel for managing merchant account, a feature is also provided to Merchant that allows for the configuration of style elements on the hosted payment page.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Nochex collects cardholder data on the hosted payment page secure.nochex.com, where it is temporarily held in volatile memory before being securely transmitted to acquiring financial institutions through one of the payment gateways. After transmission, the cardholder data is permanently truncated, and only the truncated data is stored within a transactional database. Nochex does not store any un-truncated cardholder data or any sensitive authentication data within its cardholder data environment.
Describe system components that could impact the security of account data.	Nochex maintains web servers, network components, and payment applications that facilitate payment processing and support customer business operations. These system components play a critical role in the security of account data. Nochex takes full responsibility for the protection of cardholder data once it is received.

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.*	Nochex operates a number of web application servers within the CDE that host a payment page. The web application servers sit within a DMZ. All external connections to and from the web application servers are made via both a physical and web application firewall. All internal connections to and from the web application servers are made via a physical firewall. A number of critical components support the CDE systems, including authentication services, logging, and patch management.
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*
Corporate Head Office	1	Richmond House, Leeds, United Kingdom
Data Centre	1	Serverbank (Asanti) Data Centre, Bank House, Faulkner Street, Manchester, M1 4EH, United Kingdom.

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
Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable
				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, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions), and Mobile Payments on COTS (MPoC) products.

Part 2. Executive Summary *(continued)*

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:**
Cardstream	Payment service provider
ACI Worldwide GmbH	Payment service provider
Daisy Group plc	Data Center Colocation Provider

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 Service Provider

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If a Compensating Control(s) Was Used
	In Place	Not Applicable	Not Tested	Not in Place	
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.	Requirement 1 1.2.6 Nochex does not allow any insecure services, protocols, or ports within its CDE. 1.3.3 No wireless network is present or in use within the Nochex environment. 1.4.4 Nochex does not store cardholder data, including Full PAN or SAD. Requirement 2 2.2.5 Nochex does not allow any insecure services, protocols, or ports within its CDE. 2.3.1 and 2.3.2 No wireless networks are deployed within the CDE. Requirement 3 3.2.1 Nochex does not store cardholder data. 3.3.1.1 and 3.3.1.3 Nochex does not process card-present transactions or use PTS POI devices. 3.3.2 Nochex does not store Sensitive Authentication Data (SAD). 3.3.3 Nochex is not an issuer or company that supports issuing services and does not store sensitive authentication data. 3.4 Nochex does not store Full PAN or cleartext PAN. 3.5.1.1 This requirement is considered best practice until 31 March 2025. 3.5.1.2 and 3.5.1.3 Nochex does not use disk-level or partition-level encryption to render PAN unreadable. 3.6 and 3.7 No full PAN is stored within the CDE. Nochex only stores hashed PAN and truncated PAN, which are maintained in separate databases. Requirement 4 4.2.1.2 Nochex does not utilize wireless networks within its Cardholder Data Environment (CDE). 4.2.2 No PAN is transmitted using end-user messaging technologies. Requirement 5 5.2.3 and 5.2.3.1 All systems within the PCI DSS scope for Nochex have AVG Business antimalware installed and active. Requirement 6 6.3.2 and 6.4.3 This requirement is considered best practice until 31 March 2025. Requirement 7 7.2.6 Nochex does not store unhashed or untruncated PAN in its environment.

	Requirement 8 8.2.2 Nochex does not use group, shared, or generic accounts. 8.2.3 Nochex does not have remote access to customer premises. 8.2.7 No third-party organizations have system-level access to systems within the CDE. 8.3.10 and 8.3.10.1 Nochex does not store a full PAN and does not need to provide access to cardholder data. 8.6.1 and 8.6.2 The system and application account cannot be used for interactive login. Requirement 9 9.2.2 No public network jacks are accessible. 9.4 No cardholder data is stored, so there are no drives or physical media in scope. 9.5 Nochex does not process card-present transactions. Requirement 10 10.2.1.1 Nochex does not store unhashed or untruncated PAN in its environment. 10.4.2 and 10.4.2.1 Logs of all system components within the CDE are reviewed daily. Requirement 11 11.3.1.1 This requirement is considered best practice until 31 March 2025. 11.4.4 No open exploitable vulnerabilities were recorded during the review. 11.4.7 Nochex is not a multi-tenant service provider. 11.5.1.1 This requirement is considered best practice until 31 March 2025. 11.6.1 This requirement is considered best practice until 31 March 2025. Requirement 12 12.3.2 No part of the requirement is met using a customized approach. 125.3 No Significant changes to organizational structure noted Appendix A1: Nochex is not a Multi-Tenant Service Provider. Appendix A2: Nochex does not operate POI Terminals.
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**)

Date Assessment began: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*	2024-11-25
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	2024-12-02
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes ☒ No
Were any testing activities performed remotely?	☒ 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 2024-12-19)*.

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 Nochex Limited 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 4.0.1 and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of 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

khalid hussain

khalid hussain (Dec 20, 2024 11:32 GMT)

Signature of Service Provider Executive Officer ↑	Date: 20-Dec-2024
Service Provider Executive Officer Name: Khalid Hussain	Title: CIO

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:

kobillor

Signature of Lead QSA ↑	Date: 20 Dec 2024
Lead QSA Name: KENECHI OBILLOR	

Signature of Duly Authorized Officer of QSA Company ↑	Date: 20 Dec 2024
Duly Authorized Officer Name: PHILIP BRINING	QSA Company: DATA PROTECTION PEOPLE LIMITED

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	□	□	

Note: The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance accepting organization to ensure that this form is acceptable in their program. For more information about PCI SSC and our stakeholder community please visit: https://www.pcisecuritystandards.org/about_us/