Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

Revision 2

September 2022

Document Changes

Date	Version	Description
September 2022	3.2.1 Revision 2	Updated to reflect the inclusion of UnionPay as a Participating Payment Brand.

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:	Nochex Limited ("Nochex")		DBA (doing business as):		
Contact Name:	Khalid Hussain		Title:	Chief Information Officer/Jnt Chief Technical Officer	
Telephone:	+447725071291		E-mail:	Khalid.Hussain@nochex.com	
Business Address:	Richmond House, Lawnswood Business Park, Redvers Close, Leeds, LS16 6QY, UK		City:	Leeds	
State/Province:	Leeds	Country:	United Kingdom	Zip:	LS16 6QY
URL:	www.nochex.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:	Data Protection People Limited				
Lead QSA Contact Name:	Kenechi Obillor		Title:	Qualified Security Assessor	
Telephone:	+447876041412		E-mail:	Kene.obillor@dataprotectionpeople.com	
Business Address:	The Tannery, 91 Kirkstall Road, Leeds. LS3 1HS		City:	Leeds	
State/Province:	Leeds	Country:	United Kingdom	Zip:	LS3 1HS
URL:	www.dataprotectionpeople.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:	Nochex payment services	
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):		

***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: all services provided by the service provider are within the scope of the assessment

Type of service(s) not assessed:

Hosting Provider:	**Managed Services (specify):**	**Payment Processing:**
☐ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☐ Other Hosting (specify):	☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	☐ 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:	

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Nochex is a payment facilitator, specializing in facilitating secure financial transactions for business. Nochex acts as a conduit between merchants and several acquiring financial institutions. Merchants are provided with a hosted payment page that enables the acceptance of both e-commerce, and in some cases MOTO, payments. Merchant may only integrate their websites and applications with this hosted payment page using a simple redirect link. In the interests of security, no other integration options are present. Nochex processing payment through level 1 PCI DSS Validated payment gateways. Nochex also enables Apple users to make payments through Apple Pay on its platform. When using Apple Pay, Nochex doesn't transmit or store Cardholder Data or sensitive Authentication Data. During transaction, Apple Pay provides payment token to Nochex, which is securely sent to payment gateway. Importantly, the obtained token doesn't contain PAN or Sensitive Authentication Data.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Nochex collects cardholder data on the hosted payment page, where it is held in volatile memory before being transmitted to one of a number of acquiring financial institutions. After transmission, the cardholder data is permanently truncated, before being stored in this truncated form within a transactional database. Nochex does not store any un-truncated cardholder data or any sensitive authentication data within its cardholder data environment.

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*
Head Office	1	Leeds, United Kingdom
Data Centre	1	Manchester, United Kingdom

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)
			☐ 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.*	Nochex's environment includes two dedicated web servers operating within the secure Cardholder Data Environment (CDE). These servers, hosted within the DMZ, handle the payment application. All external connections to and from the web application servers are routed through both a physical and a web application firewall. Similarly, all internal connections to and from the web application servers are managed through a physical firewall. Several critical components support the CDE systems, including VPN authentication services, FIM, Log management, and Patch management
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:	
QIR Individual Name:	
Description of services provided by QIR:	

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:**
Axcess Payment Services	Payment Service Provider
Cardstream	Payment Service Provider
Asanti (Daisy Group Plc)	Hosting Provider
Pentest People	CREST Penetration Tester
Qualys	Approved Scanning Vendor
ACI Worldwide GmbH	Payment Service 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 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:	Nochex Payment Service Provider			
	Details of Requirements Assessed			
PCI DSS Requirement	**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:	☐	☒	☐	**1.1.6 - not applicable: Nochex does not allow any insecure, services protocols or ports.** **1.2.3 - not applicable: Nochex has no wireless networks within the CDE.** **1.3.6 - not applicable: Nochex does not store CHD.**
Requirement 2:	☐	☒	☐	**2.1.1 - not applicable Nochex has no wireless networks within the CDE.** **2.2.1.b - not applicable: Nochex has no virtualisation technologies in the CDE.** **2.2.2.b - not applicable: Nochex does not allow any insecure, services protocols or ports.** **2.2.3 - not applicable: Nochex does not allow any insecure, services protocols or ports.** **2.6 - not applicable: Nochex is not a shared hosting provider.**
Requirement 3:	☐	☒	☐	**3.1 - not applicable - Nochex does not store CHD.** **3.2a and 3.2.b - not applicable: Nochex does not issue nor support the issue of payment cards** **3.3 - not applicable: Nochex does not store and does not display PAN.** **3.4.c - not applicable: Nochex does not utilise removable media in the CDE.**

				3.4.1 - Not applicable: Nochex does not use disk encryption in the CDE. **3.5 - Not applicable: Only truncated and Hashed Cardholder data exist within the CDE. no encryption and key management is required.** **3.6 - Not applicable: Nochex does not use nor share cryptographic keys.**
Requirement 4:	☐	☒	☐	**4.1.1 - not applicable: Nochex does not use wireless networks in the CDE.**
Requirement 5:	☐	☒	☐	**5.1.2 - not applicable: Nochex does not utilise systems not commonly affected by malware in the CDE.**
Requirement 6:	☒	☐	☐	
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	**8.1.5 - not applicable: no third-party organisations have system-level access to the CDE.** **8.1.6.b - not applicable: no customer accounts exist within the CDE.** **8.2.1.d - not applicable: no non-consumer customer accounts exist within the CDE.** **8.2.1.e - not applicable: no non-consumer customer accounts exist within the CDE.** **8.2.3.b - not applicable: no non-consumer customer accounts exist within the CDE.** **8.2.4.b - not applicable: no non-consumer customer accounts exist within the CDE.** **8.2.5.b - not applicable: no non-consumer customer accounts exist within the CDE.** **8.3.2.a - not applicable: Nochex does not permit any third party access to the CDE.** **8.5.1 - not applicable: Nochex does not perform remote access to customer premises.** **8.7 - not applicable: Nochex does not have a schema that enables the storage of CHD.**
Requirement 9:	☐	☒	☐	**9.1.2 - not applicable: Nochex does not have any accessible public network jacks.** **9.1.3 - not applicable: Nochex does not have any wireless networks in the CDE.** **9.3.c - not applicable: Nochex has not terminated any employees within the last 12 months.** **9.5 to 9.8 - not applicable: Nochex does not store any CHD.** **9.9 - not applicable: Nochex does not use any POI devices.**

Requirement 10:	☐	☒	☐	**10.2.1 - not applicable: Nochex does only stores truncated or hashed CHD in the CDE.**
Requirement 11:	☒	☐	☐	
Requirement 12:	☐	☒	☐	**12.3.9 - Not Applicable: QSA verified that no third-party has access to the CDE.** **12.3.10 - Not applicable; Nochex does not store cardholder data within its CDE**
Appendix A1:	☐	☐	☒	**A1 - not applicable: Nochex is not a shared hosting provider.**
Appendix A2:	☐	☐	☒	**A2 - not applicable: Nochex does not have any POS devices in the CDE.**

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:	*18th December, 2023*	
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 *18th December, 2023.*

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 *Nochex* 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 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 "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

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, CVN2, CVV2, or CID 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 *Qualys*

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	*Date:* **18th December, 2023**
Service Provider Executive Officer Name: **Khalid Hussain**	*Title:* **Chief Information Officer/Jnt Chief Technical Officer**

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

If a QSA was involved or assisted with this assessment, describe the role performed:	*The Assessor conducted a formal assessment, including both on-site and remote assessments, and produced a Report on Compliance.*

Signature of Duly Authorized Officer of QSA Company ↑	*Date: 18th December, 2023*
Duly Authorized Officer Name: Kenechi Obillor	*QSA Company:* Data Protection People

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*

[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	☐	☐