



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:	Nochex Limited ("Nochex")		DBA (doing business as):		
Contact Name:	Andrew Baiden		Title:	Project Director	
Telephone:	0113 819 7210		E-mail:	Andrew.baiden@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:	Philip Brining		Title:	QSA	
Telephone:	+44 113 869 1290		E-mail:	philip.brining@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 provide by the service provider are within the scope of the assessment
----------------------------------	---

Type of service(s) not assessed:

Hosting Provider:	Managed Services (specify):	Payment Processing:
<input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Shared Hosting Provider <input type="checkbox"/> Other Hosting (specify):	<input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify):	<input type="checkbox"/> POS / card present <input type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):
<input type="checkbox"/> Account Management <input type="checkbox"/> Back-Office Services <input type="checkbox"/> Billing Management <input type="checkbox"/> Clearing and Settlement <input type="checkbox"/> Network Provider	<input type="checkbox"/> Fraud and Chargeback <input type="checkbox"/> Issuer Processing <input type="checkbox"/> Loyalty Programs <input type="checkbox"/> Merchant Services	<input type="checkbox"/> Payment Gateway/Switch <input type="checkbox"/> Prepaid Services <input type="checkbox"/> Records Management <input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> 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: the company acts as a conduit between merchant customers and a number of acquiring financial institutions.

These 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 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.

In addition to a 'control panel' that customers use to manage their merchant account, a feature is provided that allows for the configuration of style elements on the hosted payment page.

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):
<i>Example: Retail outlets</i>	3	<i>Boston, MA, USA</i>
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)
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	

Part 2e. Description of Environment

Provide a **high-level** description of the environment covered by this assessment.

For example:

Nochex operates a number of web application servers within the CDE that host a payment page. The web application servers sit within a

<ul style="list-style-type: none"> • <i>Connections into and out of the cardholder data environment (CDE).</i> • <i>Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.</i> 	<p>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.</p>
<p>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)</p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p>

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
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:		Payment service provider		
PCI DSS Requirement	Details of Requirements Assessed			Justification for Approach (Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)
	Full	Partial	None	
Requirement 1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	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:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	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:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	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.

				<p>3.4.c - not applicable: Nochex does not utilise removable media in the CDE.</p> <p>3.4.1 - not applicable: Nochex does not use disk encryption in the CDE.</p> <p>3.5 - not applicable: Nochex does not store CHD in the CDE and therefore does not use cryptography to protect it.</p> <p>3.6 - not applicable: Nochex does not use nor share cryptographic keys.</p>
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	4.1.1 - not applicable: Nochex does not use wireless networks in the CDE.
Requirement 5:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	5.1.2 - not applicable: Nochex does not utilise systems not commonly affected by malware in the CDE.
Requirement 6:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	6.4.6 - not applicable: no significant changes occurred within the CDE in the preceeding 12 months.
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 8:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>8.1.5 - not applicable: no third-party organisations have system-level access to the CDE.</p> <p>8.1.6.b - not applicable: no customer accounts exist within the CDE.</p> <p>8.2.1.d - not applicable: no non-consumer customer accounts exist within the CDE.</p> <p>8.2.1.e - not applicable: no non-consumer customer accounts exist within the CDE.</p> <p>8.2.3.b - not applicable: no non-consumer customer accounts exist within the CDE.</p> <p>8.2.4.b - not applicable: no non-consumer customer accounts exist within the CDE.</p> <p>8.2.5.b - not applicable: no non-consumer customer accounts exist within the CDE.</p> <p>8.3.2.a - not applicable: Nochex does not permit any third party access to the CDE.</p> <p>8.5.1 - not applicable: Nochex does not perform remote access to customer premises.</p> <p>8.7 - not applicable: Nochex does not have a schema that enables the storage of CHD.</p>
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	9.1.2 - not applicable: Nochex does not have any accessible public network jacks.

				<p>9.1.3 - not applicable: Nochex does not have any wireless networks in the CDE.</p> <p>9.3.c - not applicable: Nochex has not terminated any employees within the last 12 months.</p> <p>9.5 to 9.8 - not applicable: Nochex does not store any CHD.</p> <p>9.9 - not applicable: Nochex does not use any POI devices.</p>
Requirement 10:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10.2.1 - not applicable: Nochex does not store any trunkated or hashed CHD in the CDE.
Requirement 11:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>11.2.3.a to 11.2.3.c - not applicable: three were no significant changes to the CDE in the preceeding 12 months.</p> <p>11.3.1.b - not applicable: three were no significant changes to the CDE in the preceeding 12 months.</p> <p>11.3.2.b - not applicable: three were no significant changes to the CDE in the preceeding 12 months.</p>
Requirement 12:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	A1 - not applicable: Nochex is not a shared hosting provider.
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	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:	23 rd December 2022	
Have compensating controls been used to meet any requirement in the ROC?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the ROC identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Were any requirements not tested?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated 23rd December 2022.

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**):

<input checked="" type="checkbox"/>	<p>Compliant: All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby <i>Nochex</i> has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p>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.</p> <p>Target Date for Compliance:</p> <p>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. <i>Check with the payment brand(s) before completing Part 4.</i></p>						
<input type="checkbox"/>	<p>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.</p> <p><i>If checked, complete the following:</i></p> <table border="1"> <thead> <tr> <th>Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met				
Affected Requirement	Details of how legal constraint prevents requirement being met						

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

<input checked="" type="checkbox"/>	The ROC was completed according to the <i>PCI DSS Requirements and Security Assessment Procedures</i> , Version 3.2.1, and was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
<input type="checkbox"/>	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
<input checked="" type="checkbox"/>	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
<input checked="" type="checkbox"/>	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)

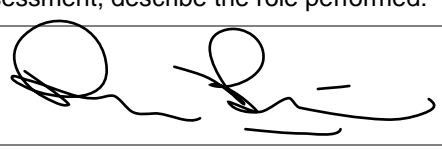
<input checked="" type="checkbox"/>	No evidence of full track data ¹ , CAV2, CVC2, CID, or CVV2 data ² , or PIN data ³ storage after transaction authorization was found on ANY system reviewed during this assessment.
<input checked="" type="checkbox"/>	ASV scans are being completed by the PCI SSC Approved Scanning Vendor <i>Qualys</i>

Part 3b. Service Provider Attestation

A. Baiden

Signature of Service Provider Executive Officer ↑	Date: 23rd December 2022
Service Provider Executive Officer Name: Andrew Baiden	Title: Project Director

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 on-site and remote assessment and produced a report on compliance.
	
Signature of Duly Authorized Officer of QSA Company ↑	Date: 23rd December 2022
Duly Authorized Officer Name: Philip Brining	QSA Company: Data Protection People Limited

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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems against malware and regularly update anti-virus software or programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify and authenticate access to system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10	Track and monitor all access to network resources and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	<input type="checkbox"/>	<input type="checkbox"/>	

