Payment Card Industry
Data Security Standard

Attestation of Compliance for Self-Assessment Questionnaire D for Service Providers

For use with PCI DSS Version 4.0

Revision 2

Publication Date: August 2023

Section 1: Assessment Information

Instructions for Submission

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

This AOC reflects the results documented in an associated Self-Assessment Questionnaire (SAQ).

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Self-Assessment Questionnaire.

Part 1. Contact Information	
Part 1a. Assessed Entity	
Company name:	NOBEDS
DBA (doing business as):	JUST TRADE Ltd.
Company mailing address:	Zveju str. 5 - 14, LT-91247, Klaipeda
Company main website:	www.nobeds.com
Company contact name:	Saulius Chomentauskas
Company contact title:	Owner
Contact phone number:	+370 611 54444
Contact e-mail address:	saulius.chomentauskas@nobeds.com
Part 1b. Assessor	
Provide the following information for all assessors involved in the assessment. If there was no assessor for agiven assessor type, enter Not Applicable.	
PCI SSC Internal Security Assessor(s)	
ISA name(s):	
Qualified Security Assessor	
Company name:	
Company mailing address:	
Company website:	
Lead Assessor Name:	
Assessor phone number:	
Assessor e-mail address:	
Assessor certificate number:	

Part 2. Executive Summary

Part 2a. Scope Verification

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

Name of service(s) assessed:		
Type of service(s) assessed:		
Hosting Provider: ☒ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web-hosting servicesSecurity services ☐ 3-D Secure Hosting Provider Multi-Tenant Service ☐ ProviderOther Hosting ☐ (specify):	**Managed Services:** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify): ☐ ☐	**Payment Processing:** ☐ POI / card present ☐ Internet / e-commerceMOTO / 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 PCI DSS Assessment (select all that apply):

Name of service(s) not assessed:	

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-
☐ Infrastructure /	☐ Physical security	☐ commerceMOTO /
☐ Network	☐ Terminal Management System	☐ Call Center ATM
☐ Physical space (co-location)	☐ Other services (specify):	☐ Other processing (specify):
☐ Storage		
☐ Web-hosting		
☐ servicesSecurity		
☐ services		
☐ 3-D Secure Hosting Provider		
Multi-Tenant Service		
☐ ProviderOther 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:	

Part 2b. Description of Role with Payment Cards

Describe how the business stores, processes, and/or transmits account data.	Nobeds processes less than 100 cardholder transactions per day. Cardholder data is stored in database with encryption. Each client has its own encryption key, ensuring that the data is segregated and protected on a per-location basis. Transmission of cardholder data is performed securely over encrypted communication channels, using protocols like TLS/SSL to protect the data from unauthorized interception. Cardholder data is stored in compliance with PCI-DSS guidelines, ensuring that sensitive information such as credit card numbers is encrypted and access is restricted to authorized personnel only. No sensitive authentication data, such as CVV codes, is stored after authorization.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	The business does not store CVV codes after authorization, which significantly reduces the risk of sensitive cardholder data exposure. Though the business cannot directly impact the security of the data beyond its storage and processing environment, it partners with PCI-compliant payment gateways to ensure the secure

	processing of transactions. Regular security audits and adherence to PCI-DSS standards ensure that all security measures are continually assessed and updated as needed.
Describe system components that could impact thesecurity of account data.	Encryption Mechanisms: Separate encryption keys are used for each client, which protects data at rest. Access Control Systems: The business uses role-based access controls to restrict employee access to any sensitive payment 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.*	Cardholder Data Environment (CDE): The CDE consists of the SQL databases where cardholder data is stored, encrypted using distinct encryption keys for each client. These databases are critical to the secure storage of payment information. System Components that Could Impact Security: Regular backups of data are performed, and backups are encrypted to prevent unauthorized access. Antivirus and anti-malware software are deployed across all systems that interact with the CDE to prevent malicious activity and data breaches.
Indicate whether the environment includes segmentation to reduce the scope of the assessment. *(Refer to "Segmentation" section of PCI DSS for guidance on segmentation.)*	☐ Yes ☒ No

Part 2d. In-Scope Locations/Facilities

List all types of physical locations/facilities—for example, corporate offices, data centers, call centers, andmail rooms—in scope for the PCI DSS assessment.

Facility Type	Total number of locations (How many locationsof this type are in scope)	Location(s) of facility (city, country)
Example: Data centers	*3*	*Boston, MA, USA*

Part 2. Executive Summary *(continued)*

Part 2e. PCI SSC Validated Products and Solutions

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 ValidatedProducts 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)

♦ 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 2. Executive Summary *(continued)*

Part 2f. Third-Party Service Providers

For the services being validated, does the entity have relationships with one or more third-party serviceproviders 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 scope of the entity's PCI DSS assessment—for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers,web-hosting services, and IaaS, PaaS, SaaS, and FaaS cloud providers.	☐ Yes ☒ No
• Could impact the security of the entity's CDE—for example, vendors providingsupport via remote access, and/or bespoke software developers.	☐ Yes ☒ No

If Yes:

Name of service provider:	Description of service(s) provided:

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

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment

(SAQ Section 2 and related appendices)

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:

PCI DSS Requirement	Requirement Responses *More than one response may be selected for a given requirement. Indicate all responses that apply.*				
	In Place	In Place with CCW	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.	Not a shared hosting provider
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	

Section 2: Self-Assessment Questionnaire D for Service Providers

Self-assessment completion date:	2025-09-04
Were any requirements in the SAQ 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 SAQ D (Section 2), dated (Self-assessment completion date *2024-09-11 17:10)**.***

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

- ☒ **Full** – All requirements have been assessed therefore no requirements were marked as Not Tested in the SAQ.
- ☐ **Partial** – One or more requirements have not been assessed and were therefore marked as Not Tested in the SAQ. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the SAQ D 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 SAQ are complete, and all assessed requirements are marked as being either 1) In Place, 2) In Place with CCW, or 3) Not Applicable, resulting in an overall **COMPLIANT** rating; thereby *(Service Provider Company Name)* has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted as Not Tested above.
☐	**Non-Compliant:** Not all sections of the PCI DSS SAQ 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 the PCI DSS requirements includedin this SAQ. **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 *beforecompleting Part 4.*
☐	**Compliant but with Legal exception:** One or more assessed requirements in the PCI DSS SAQ are marked as Not in Place due to a legal restriction that prevents the requirement from being met and allother assessed requirements are marked as being either 1) In Place, 2) In Place with CCW, or 3) NotApplicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *(Service Provider Company Name)* has demonstrated compliance with all PCI DSS requirements included in this SAQ 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 3a. Service Provider Acknowledgement

Signatory(s) confirms:

(Select all that apply)

☒	PCI DSS Self-Assessment Questionnaire D, Version *4.0* was completed according to the instructions therein.
☒	All information within the above-referenced SAQ and in this attestation fairly represents the results of the entity's 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: 2025-09-04*
Service Provider Executive Officer Name: Saulius Chomentauskas	*Title: Owner*

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:

Signature of Lead QSA ↑	*Date:*
Lead QSA Name:	

Signature of Duly Authorized Officer of QSA Company ↑	*Date: 2025-09-04 09:10*
Duly Authorized Officer Name:	*QSA Company:*

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 a Non-Compliant status 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 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 securitycontrols	☒	☐	
2	Apply secure configurations to allsystem components	☒	☐	
3	Protect stored account data	☒	☐	
4	Protect cardholder data with strong cryptography during transmission overopen, public networks	☒	☐	
5	Protect all systems and networks frommalicious software	☒	☐	
6	Develop and maintain secure systems and software	☒	☐	
7	Restrict access to system components and cardholder data by business needto know	☒	☐	
8	Identify users and authenticate access to system components	☒	☐	
9	Restrict physical access to cardholderdata	☒	☐	
10	Log and monitor all access to systemcomponents and cardholder data	☒	☐	
11	Test security systems and networksregularly	☒	☐	
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	☒	☐