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: DNA Payments

Date of Report as noted in the Report on Compliance: 2025-11-10

Date Assessment Ended: 2025-11-10

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:	DNA Payments Limited
DBA (doing business as):	DNA Payments
Company mailing address:	10 Lower Grosvenor Place, London, SW1W 0EN, United Kingdom.
Company main website:	http://dnapayments.com
Company contact name:	Mr. Nurlan Zhagiparov
Company contact title:	Director
Contact phone number:	+44 208 102 8100
Contact e-mail address:	nurlan@dnapayments.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):	N/A
Qualified Security Assessor	
Company name:	SRC Security Research & Consulting GmbH.
Company mailing address:	Emil-Nolde-Str. 7, Bonn, Germany 53113
Company website:	http://www.src-gmbh.de/
Lead Assessor name:	Andrey Shcherbakov
Assessor phone number:	+49-228-2806-213
Assessor e-mail address:	andrey.shcherbakov@src-gmbh.de
Assessor certificate number:	205-213

PCI Security Standards Council

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:	POS transactions processing, E-commerce gatewa and processing services

Type of service(s) assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☒ POI / card present
☐ Hardware	☐ IT support	☒ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web-hosting services		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Multi-Tenant Service Provider		
☐ Other 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): Acquirer functions which were not specifically indicated in the services list above

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:	N/A - the assessment covered all PCI DSS relevant services provided by DNA Payments

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

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.	DNA Payments implements processing functions for the POS terminals and e-commerce transactions processing. DNA Payments uses OpenWays' Way4 TransactionSwitch which performs the main functions of the solution. All POS processing and e-commerce processing functions are implemented with help of the ISO8583 calls processed by the Way4 TransactionSwitch.

Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	The DNA Payments have a need to store and to process the cardholder data to enable their customers with interconnectivity capabilities to support the access of the customer banks and/or acquirers with no direct interaction with the cardholder data.
Describe system components that could impact the security of account data.	Database storage Connections from/to the Internet

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.*	POS terminals establish connections to the TransactionSwitch via PCI DSS validated infrastructure of OptoMany and the cardholder data is transmitted for authorizations via VPN connections. OptoMany is the DNA Payments subsidiary with its own PCI DSS compliant environment operated. E-commerce solutions enable the customers to enter their sensitive data via payment page rendered by 'EPAY' e-commerce system, and after that the data is sent TLS-protected from the cardholder's browser to the processing server of 'EPAY' to be routed for authorization to the TransactionSwitch. The SAD (CVV2/CVC2 and equivalent) is available for the short time only in the RAM of the application servers, and is never stored nor written to the logs. The full PAN is only available in the database appropriately encrypted. The full PAN is recorded in the TDE-protected Oracle database (AES256) or PostgreSQL database operating the enrypted storage.
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 Headquarters	1	London, United Kingdom
Equinix Datacenters	2	London, United Kingdom (LD8) Manchester, United Kingdom (MA1)
Oracle Cloud Infrastructure	1	Cloud infrastructure

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
Way4 Transaction Switch	1.3.77-4087	N/A	N/A	N/A
Way4 MPI Standalone	1.2.448-7269	N/A	N/A	N/A

* 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:
Oracle Corporation	Oracle Cloud Infrastructure (virtualized systems, incl. database)
Equinix	Physical co-location (datacenter services)
OptoMany	Management of the POS network and transactions processing

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:

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.	1.2.6, 2.2.5 – no insecure services, protocols and ports are allowed or used. 1.3.3 – no wireless access points are operated in the CDE. 2.3.1, 2.3.2 – there are no wireless access points connected to the CDE. 3.3.2, 3.3.3 – no SAD is being stored. 3.4.1 – the function to display the PAN even masked is not necessary and not implemented. 3.4.2 – no access to the systems storing the CHD is permitted using the remote access technologies. 3.5.1.2, 3.5.1.3 – there is no disk-level or partition-level encryption as in sense of this requirement. 3.7.2 – no distribution of the keys is performed. 3.7.6 – no clear-text cryptographic key-management operations are performed. 3.7.9 – the keys are not shared with the third parties. 4.2.1.2 – no wireless technology is used in the CDE. 4.2.2 – end-user messaging technologies are not used for CHD transmission. 5.2.3, 5.2.3.1 – all system components in scope contain anti-malware solution. 5.3.3 – the AUP forbids the usage of the removable media. 6.4.1 – the requirement has been superseded by 6.4.2. 6.5.2 – no significant changes occurred in the past year. 8.2.3 – there is no access to customers' environments. 8.2.7 – no accounts are used by third parties. 8.3.10, 8.3.10.1 – there are no non-consumer customer accounts available with only password authentication factor. 8.3.11 – there are no such physical or logical security tokens, smart cards or certificates. 9.4.1 – there is no media relevant to this requirement. 9.4.1.1, 9.4.1.2 – no offline media backups exist. 9.4.2 – there is no offline media with CHD. 9.4.3, 9.4.4 – cardholder information is not distributed by any kind of media. 9.4.5, 9.4.5.1, 9.4.6, 9.4.7 – there is no media relevant to this requirement. 9.5.* – the entity isn't managing the devices which directly capture the payment data via direct physical interaction. 10.7.1 – the requirement has been superseded by 10.7.2. 11.3.2.1 – no significant changes occurred in the CDE relevant environment in the last year. 11.4.7, 12.5.3 – the entity is not a multi-tenant service provider in sense of this requirement. 12.3.2 – no requirements were addressed using a customized approach.

	A1 – the entity is not a multi-tenant service provider. A2 – the entity is not operating POS/POI devices in the CDE.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	N/A

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.*	2025-10-08
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	2025-11-10
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 2025-11-10).*

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 DNA Payments 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 N/A has not demonstrated compliance with PCI DSS requirements.

Target Date for Compliance: N/A

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 N/A 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
N/A	N/A

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

DocuSigned by:
Nurlan Zhagiparov
36669C2778E8435...

Signature of Service Provider Executive Officer ↑	Date: 2025-12-15
Service Provider Executive Officer Name: Nurlan Zhagiparov	Title: 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:

Signature of Lead QSA ↑	Date: 2025-12-15
Lead QSA Name: Andrey Shcherbakov	

Signature of Duly Authorized Officer of QSA Company ↑	Date: 2025-12-15
Duly Authorized Officer Name: Andrey Shcherbakov	QSA Company: SRC Security Research & Consulting GmbH

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/