



# **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: BCH Digital Limited**

**Date of Report as noted in the Report on Compliance: 16th June 2026**

**Date Assessment Ended: 21st May 2026**

## 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:	BCH Digital Limited
DBA (doing business as):	BCH Digital
Company mailing address:	Eagle Tower, Montpellier Drive, Cheltenham, GL50 1TA
Company main website:	www.bchdigital.co.uk
Company contact name:	Chris Johnson
Company contact title:	Chief Information Security Officer (CISO)
Contact phone number:	0333 202 9990
Contact e-mail address:	chris.johnson@bchdigital.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:	Philip Brining
Assessor phone number:	01138691250
Assessor e-mail address:	philip.brining@dataprotectionpeople.com
Assessor certificate number:	205-590

## 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:	Telephone Payment Services
------------------------------	----------------------------

Type of service(s) assessed:

Hosting Provider:	Managed Services:	Payment Processing:
<input type="checkbox"/> Applications / software	<input type="checkbox"/> Systems security services	<input type="checkbox"/> POI / card present
<input type="checkbox"/> Hardware	<input type="checkbox"/> IT support	<input type="checkbox"/> Internet / e-commerce
<input type="checkbox"/> Infrastructure / Network	<input type="checkbox"/> Physical security	<input checked="" type="checkbox"/> MOTO / Call Center
<input type="checkbox"/> Physical space (co-location)	<input type="checkbox"/> Terminal Management System	<input type="checkbox"/> ATM
<input type="checkbox"/> Storage	<input type="checkbox"/> Other services (specify):	<input type="checkbox"/> Other processing (specify):
<input type="checkbox"/> Web-hosting services		
<input type="checkbox"/> Security services		
<input type="checkbox"/> 3-D Secure Hosting Provider		
<input type="checkbox"/> Multi-Tenant Service Provider		
<input type="checkbox"/> Other Hosting (specify):		
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input type="checkbox"/> Payment Gateway/Switch
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services
<input type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management
<input type="checkbox"/> Clearing and Settlement	<input type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> Network Provider		
<input type="checkbox"/> 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:	Hosted PBX Contact Centre Services Pay by link
----------------------------------	--

Type of service(s) not assessed:

<b>Hosting Provider:</b> <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-hosting services <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Multi-Tenant Service Provider <input type="checkbox"/> Other Hosting (specify):	<b>Managed Services:</b> <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):	<b>Payment Processing:</b> <input type="checkbox"/> POI / card present <input type="checkbox"/> Internet / e-commerce <input checked="" type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input type="checkbox"/> Payment Gateway/Switch
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services
<input type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management
<input type="checkbox"/> Clearing and Settlement	<input type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> Network Provider		
<input type="checkbox"/> Others (specify): Telephony services		

Provide a brief explanation why any checked services were not included in the Assessment:

BCH does not process, transmit or store cardholder data on BCH Digital system components and they can not impact the security of cardholder data.

**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.

BCH Digital's business is that of a payment service provider, whereby they act as a conduit between their customers and a number of acquiring financial institutions. These customers are ultimately accountable for the security of the cardholder data collected, transmitted, and processed under their merchant identification number. However, BCH Digital provides an opportunity for these customers to remove this cardholder data from their telephony systems and

	<p>call centre operations by instead utilising a secure payment line and backend infrastructure provided by BCH Digital.</p> <p>BCH Digital processes cardholder data and sensitive authentication data, as well as transmitting that data to acquiring financial institutions.</p>
<p>Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.</p>	<p>Not applicable</p>
<p>Describe system components that could impact the security of account data.</p>	<p>Not applicable</p>

**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.

After receiving incoming DTMF tone data from a Tier 1 telecoms carrier, BCH Digital transforms these tone data into digital data before processing it within volatile memory and then subsequently transmitting the resultant cardholder data to one of a number of acquiring financial institutions.

BCH Digital does not store any cardholder data, or any sensitive authentication data within its cardholder data environment or wider business systems.

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
Not applicable	Not applicable	Not applicable

**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
				YYYY-MM-DD
				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](http://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 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:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 2:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 3:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 4:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 5:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 6:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 7:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 8:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 9:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 10:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 11:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 12:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

#### Justification for Approach

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.

- 1.2.6 There are no services, protocols, and ports that are in use and considered to be insecure
- 1.3.3 AWS IaaS CDE, so no wireless network in scope
- 1.4.4 BCH Digital does not store cardholder data
- 2.2.5 There are no services, protocols, and ports that are in use and considered to be insecure
- 2.3.1 and 2.3.2 AWS IaaS CDE, so no wireless network in scope
- 3.3.1.1 only cardholder not-present transactions are processed within the BCH Digital cardholder data environment, and as such no Track data could be present.
- 3.3.1.3 only cardholder not-present transactions are processed within the BCH Digital cardholder data environment, and as such no PIN data could be present.
- 3.3.3 - BCH Digital does not issue or support the issuing of payment cards.
- 3.4, 3.5, 3.6 and 3.7 no PAN is stored or displayed within the cardholder data environment.
- 4.2.1.2 AWS IaaS CDE, so no wireless networks in scope
- 4.2.2 no PAN is sent using end-user messaging
- 5.2.1.b, 5.2.3 and 5.2.3.1 All system components operating within the cardholder data environment are commonly affected by malware and as such are configured to use anti-virus software.
- 5.3.2.1 Realtime scans are in place
- 6.4.1, 6.4.2 and 6.4.3 public-facing web applications are not present within the cardholder data environment
- 7.2.6 no PAN is stored within the cardholder data environment.
- 8.2.3 BCH Digital does not have remote access to customer premises
- 8.2.7 no third-parties have accounts to access the cardholder data environment.
- 8.3.10 non-consumer customer accounts are not present in cardholder data environment or on in-scope systems.
- 8.3.11.c physical controls are not used
- 8.4.2 only Administrators have access to the cardholder data environment
- 8.5.1c requests to bypass MFA are not permitted and would not be granted
- 8.6.1, 8.6.2 and 8.6.3 application accounts do not have permissions for interactive logins.
- 9.2 to 9.5.1.3 BCH Digital utilizes a validated PCI DSS level 1 compliant service provider to meet all sensitive processing area physical security requirements and other environmental security controls of the cardholder data environment. Also, BCH Digital does not print cardholder or sensitive authentication data within the cardholder data environment or other in-scope systems. Finally, no

	<p>POI devices exist within the cardholder data environment.</p> <p>10.2.1.1 Individual users do not have access to cardholder data.</p> <p>10.7.3.b No critical control failures could be identified</p> <p>11.2.1 and 11.2.2 AWS IaaS CDE, so no wireless network in scope</p> <p>11.3.1.2.c no authenticated scan accounts have interactive login enabled</p> <p>11.4.5, 11.4.6 no segmentation is used to isolate the cardholder data environment from other networks.</p> <p>11.4.7 BCH Digital is not a multi-tenant service provider</p> <p>11.6.1 no payment scripts exist within the cardholder data environment.</p> <p>12.3.2 no PCI DSS requirements have been met with a customized approach</p> <p>12.5.3 there were no significant changes to the organisational structure in the last twelve months.</p> <p>12.10.1.b - there have been no reported incidents over the last twelve months</p> <p>12.10.7.b - there have been no reported incidents over the last twelve months</p> <p>All of Appendix A1-A3 - BCH Digital is not a shared hosting provider.</p>
<p>For any Not Tested responses, identify which sub-requirements were not tested and the reason.</p>	<p>Not applicable</p>

## Section 2 Report on Compliance

**(ROC Sections 1.2 and 1.3)**

Date Assessment began: <i>Note: This is the first date that evidence was gathered, or observations were made.</i>	2026-05-11
Date Assessment ended: <i>Note: This is the last date that evidence was gathered, or observations were made.</i>	2026-05-21
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any testing activities performed remotely?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> 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 YYYY-MM-DD).

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 (BCH Digital 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



Signature of Service Provider Executive Officer ↑	Date: 2026-06-17
Service Provider Executive Officer Name: Chris Johnson	Title: CISO

#### 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: 2026-06-17
Lead QSA Name: Philip Brining	



Signature of Duly Authorized Officer of QSA Company ↑	Date: 2026-06-17
Duly Authorized Officer Name: Kenechi Obillor	QSA Company: Data Protection People

#### 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	<input type="checkbox"/>	<input type="checkbox"/>	
2	Apply secure configurations to all system components	<input type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored account data	<input type="checkbox"/>	<input type="checkbox"/>	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	<input type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems and networks from malicious software	<input type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and software	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to system components and cardholder data by business need to know	<input type="checkbox"/>	<input type="checkbox"/>	
8	Identify users and authenticate access to system components	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
10	Log and monitor all access to system components and cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
11	Test security systems and networks regularly	<input type="checkbox"/>	<input type="checkbox"/>	
12	Support information security with organizational policies and programs	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service 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"/>	

*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/](https://www.pcisecuritystandards.org/about_us/)*