Payment Card Industry
Data Security Standard

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

For use with PCI DSS Version 4.0.1

Revision 1

Publication Date: December 2024

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 reporting and 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:	Fidelity Payment Processing Limited
DBA (doing business as):	Blink Payment
Company mailing address:	123 Pentonville Road, London, N1 9LG
Company main website:	www.BlinkPayment.co.uk
Company contact name:	Raphi Katz
Company contact title:	Head of Technology
Contact phone number:	+44 (0)203 910 2994
Contact e-mail address:	R.Katz@BlinkPayment.co.uk
Part 1b. Assessor	
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:	3B Data Security Limited
Company mailing address:	Level 1, Brockbourne House, 77 Mount Ephraim, Tunbridge Wells, Kent, England, TN4 8BS
Company website:	www.3BDataSecurity.com
Lead Assessor Name:	Majid Ali
Assessor phone number:	+44 (0) 1223 298 333
Assessor e-mail address:	Majid.Ali@3BDataSecurity.com
Assessor certificate number:	202-751

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

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:	Blink Payment Portal

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):		

***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.*

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

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:	POS Terminal Solutions

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:	The POS terminal solutions currently utilise Ingenico and Miura devices. Blink Payment's merchant fullfilment team has access to the Ingenico terminal management systems, where devices are confgured with the approriate Merchant ID and Terminal ID prior to shipment. Once deployed within the merchant's environment, the terminals connect directly to the PSP. After this point, Blink Payment have no further involvement in or control over the terminals.

Part 2b. Description of Role with Payment Cards

Describe how the business stores, processes, and/or transmits account data.	N/A - No CHD processed, stored or transmitted within Blink Payment's environment.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Blink Payment operates an online portal for their clients that enables them to process online payments. There are two ways to facilitate payment. The first method is "Pay by Link," where a unique link is generated that directs users to a payment form. The second method

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

	involves a payment form within the portal, allowing Blink Payment 's customers to enter payment information directly into the provided fields. The payment fields are completely hosted within an iframe, displayed directly in the user's web browser by the payment service providers. Blink Payment is involved in or can impact the security of its customers' account data through the security measures implemented on the web page hosting the iframe with the payment fields
Describe system components that could impact the security of account data.	Blink Payment consider their production web servers and web application to be in scope of the assessment.

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.*	The environment covered by this assessment is as follows: • Blink Payment portal application and its associated hosting environment. • Connections in and out of the cardholder data environment. • Review of services and infrastructure provided by third-party service providers
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, and mail rooms—in scope for the PCI DSS 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*
Head Office	1	London, UK
Amazon Web Services	1	Ireland

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

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 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)

♦ 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.

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

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 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 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 providing support via remote access, and/or bespoke software developers.	☒ Yes ☐ No

If Yes:

Name of service provider:	**Description of service(s) provided:**
Amazon Web Services	Cloud Hosting
Cardstream	Payment Gateway
Capital Numbers	Web Development
Stripe	Payment Gateway

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

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

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: Blink Payments Portal

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

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	1.3.3 - Shared responsbility 1.4.4 - Mobile devices not used 2.2.5 - No usage requiring insecure functions 2.3.1 - No console access 2.3.2 - Encrypted admin access is not managed by Blink Payment 3.1.1 - Blink Payment does not store, process or transmits CHD 3.1.2 - Blink Payment does not store, process or transmit CHD. 3.2.1 - Blink Payment does not store, process or transmit CHD. 3.3.1 - Blink Payment does not store, process or transmit CHD. 3.3.1.1 - Blink Payment does not store, process or transmit CHD. 3.3.1.2 - Blink Payment does not store, process or transmit CHD. 3.1.1.3 - Blink Payment does not store, process or transmit CHD. 3.3.2 - Blink Payment does not store, process or transmit CHD. 3.3.3 - Blink Payment does not store, process or transmit CHD. 3.4.1 - Blink Payment does not store, process or transmit CHD. 3.4.2 - Blink Payment does not store, process or transmit CHD. 3.5.1 - Blink Payment does not store, process or transmit CHD. 3.5.1.1 - Blink Payment does not store, process or transmit CHD. 3.5.1.2 - Blink Payment does not store, process or transmit CHD. 3.5.1.3 - Blink Payment does not store, process or transmit CHD. 3.6.1 - Blink Payment does not store, process or transmit CHD. 3.6.1.1 - 3.6.1.4 - Blink Payment does not store, process or transmit CHD. 3.7.1 - 3.7.9 - Blink Payment does not store, process or transmit CHD. 4.2.1- 4.2.2 - Blink Payment does not store, process or transmit CHD. 5.2.1- 5.2.3 - Blink Payment utilise Linux-based operating systems 5.3.1 - 5.3.5 - Blink Payment utilise Linux-based operating systems. 7.2.6 - Blink Payment do not have any access to cardholder data. No cardholder data is transmitted, processed or stored 8.2.3 - Blink Payment do not have any remote access to customer environments.

© 2006—2024 PCI Security Standards Council, LLC. All Rights Reserved.

	8.2.7 - The QSA noted that Blink Payment did not have any third-party accounts during this assessmen 8.3.10 - There is no customer user access to cardholder data. 9.2.1 - Blink Payment do not have any physical access to cardholder data. No cardholder data is transmitted, processed or stored. All systems are located in AWS datacentres which are PCI compliant and have a valid AOC 9.2.1.1- 9.5.1.3 - Blink Payment does not have POI devices 10.2.1.1 - Blink Payment do not have any access to cardholder data. No cardholder data is transmitted, processed or stored 11.2.1 - 11.2.2 - No wireless networks were in scope during this assessment, as all in-scope systems are hosted within the environment operated by AWS, a compliant PCI DSS Service Provider. 11.3.1.3 - The QSA reviewed internal scan reports. No significant changes have occurred in the last 12 months where rescans were needed. 11.3.2.1 - The QSA reviewed internal scan reports. No significant changes have occurred in the last 12 months where rescans were needed. 11.4.7 - Not Applicable - Blink Payment is not a multi-tenant or shared hosting service provider. A1 - Blink Payment is not a multi-tenant or shared hosting service provider. A2 - Blink Payment do not utilise a card present payment channel
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	N/A

© 2006—2024 PCI Security Standards Council, LLC. All Rights Reserved.

Section 2: Self-Assessment Questionnaire D for Service Providers

Self-assessment completion date:	02/03/2026
Were any requirements in the SAQ unable to be met due to a legal constraint?	☐ Yes ☒ No

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

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 *2026/03/02*).

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 *Fidelity Payment Processing Limited* 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 included in 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 *before completing 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 all other assessed requirements are marked as being either 1) In Place, 2) In Place with CCW, or 3) 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 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

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:

(Select all that apply)

☒	*PCI DSS Self-Assessment Questionnaire D, Version 4.0.1,* 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

Raphi Katz

Signature of Service Provider Executive Officer ↑	*Date:* 2026-03-02
Service Provider Executive Officer Name: **Raphi Katz**	*Title:* **Head of Technology**

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:

Majid Ali

Signature of Lead QSA ↑	*Date: 2026-03-02*
Lead QSA Name: **Majid Ali**	

N. Shenfield

Signature of Duly Authorized Officer of QSA Company ↑	*Date: 2026-03-02*
Duly Authorized Officer Name: **Nick Shenfield**	*QSA Company:* **3B Data Security**

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:

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

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 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 its program. For more information about PCI SSC and our stakeholder community please visit: https://www.pcisecuritystandards.org/about_us/.*

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.