



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: Shift4 Limited

Date of Report as noted in the Report on Compliance: 2025/07/01

Date Assessment Ended: 2025/07/01



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:	Shift4 Limited
DBA (doing business as):	–
Company mailing address:	Palazzo Homedes, 80 Strait Street, Valletta VLT 1436
Company main website:	https://www.shift4.com/
Company contact name:	Oren Gur
Company contact title:	Global VP of Enterprise Security & Compliance
Contact phone number:	+972529245381
Contact e-mail address:	oren.gur@Shift4.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:	Kyte Consultants Ltd
Company mailing address:	170, Pater House, Psaila Street, Birkirkara BKR 9077, Malta
Company website:	https://kyte.global/
Lead Assessor name:	Kevin Campbell
Assessor phone number:	+356 27595000
Assessor e-mail address:	Kevin@kyte.global
Assessor certificate number:	205-036



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: *Payment processing and acquiring*

Type of service(s) assessed:

Hosting Provider:

- ☐ Applications / software
- ☐ Hardware
- ☐ Infrastructure / Network
- ☐ Physical space (co-location)
- ☐ Storage
- ☐ Web-hosting services
- ☐ Security services
- ☒ 3-D Secure Hosting Provider
- ☐ Multi-Tenant Service Provider
- ☐ Other Hosting (specify):

Managed Services:

- ☐ Systems security services
- ☐ IT support
- ☐ Physical security
- ☐ Terminal Management System
- ☐ Other services (specify):

Payment Processing:

- ☐ POI / 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): *Acquiring, Token services and Fraud*

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: None

Type of service(s) not assessed:

Hosting Provider:

- ☐ Applications / software
- ☐ Hardware
- ☐ Infrastructure / Network
- ☐ Physical space (co-location)
- ☐ Storage
- ☐ Web-hosting services
- ☐ Security services
- ☐ 3-D Secure Hosting Provider
- ☐ Multi-Tenant Service Provider
- ☐ Other Hosting (specify):

Managed Services:

- ☐ Systems security services
- ☐ IT support
- ☐ Physical security
- ☐ Terminal Management System
- ☐ Other services (specify):

Payment Processing:

- ☐ POI / 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): N/A

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.

Shift4 Limited provides services such as card schemes token services, gateway services, alternative payment methods (out of entity's PCI scope), 3D secure services, fraud prevention services (SmartGuard), payment page services, PaybyLink, token management, and account updater.

The entity is also an acquirer and receives requests from merchants and partners via an API (hosted at third-party Data Centres) and hosted page with 3D Secure facilities (at leading cloud provider).



	<p><i>Some partners accept transactions via VPOS terminals (out of entity's PCI scope) by linking to entity's API. The entity uses its own platform to connect to the card brands or to third parties (if needed).</i></p> <p><i>Merchants and partners have access to a back-office application (out of scope) to track their transactions, but PANs are not accessible on it. PANs are stored encrypted within the platform. PANs may be displayed internally to follow up chargebacks and other problematic transactions.</i></p>
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	<p><i>Entity has full control over applications. Physical infrastructure is located at third-party Data Centres and handles API and PAN storage. Cloud infrastructure handles hosted page application.</i></p>
Describe system components that could impact the security of account data.	<p><i>The system components involved in security of CHD are quite vary including:</i></p> <ul style="list-style-type: none"> <i>• Network devices</i> <i>• Network Management</i> <i>• Firewalls</i> <i>• Storage</i> <i>• Servers</i> <i>• Hypervisors</i> <i>• Databases</i> <i>• Brain and Way4 Application</i> <i>• HSM</i>



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 entity operates via 2 Data Centres each intended to server requests from separate geographical regions. The entity, via cloud infrastructure, is providing hosted page type of services which receive CHD from the cardholder and pass it on to the main infrastructure (the physical) for processing. The physical platform is integrated with the card brands and third-party processors. The CDE is built in a way to support various security zones so that webserver and databases exist in separate zones. Multiple VLANs and firewalls are in use. Redundancy exists across the different Data Centres. HSMs are in use for encryption of PANs.

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
Amazon Web Services (AWS)	1	Ireland
Google Cloud Platform (GCP)	1	Europe
Markley Boston LLC	1	Boston, MA, USA
Telehouse	1	Frankfurt, Germany
Elasticsearch. Inc.	1	Europe
CrowdStrike, Inc.	1	Europe
Cloudflare, Inc	1	Europe
Computop Paygate GmbH	1	Aschheim, Germany
Cybersource Corporation (Cybersource)	1	Ireland



<i>eMerchantPay Limited (UK) (ECP)</i>	<i>1</i>	<i>Europe</i>
<i>Redsys</i>	<i>1</i>	<i>Europe</i>
<i>Worldpay</i>	<i>1</i>	<i>USA</i>
<i>Yaad Sarid - HYP</i>	<i>1</i>	<i>Rosh Haayin, Isreal</i>
<i>TSYS Merchant Solutions LLC (Global Payment)</i>	<i>1</i>	<i>USA</i>
<i>Corporate Office</i>	<i>1</i>	<i>Valletta, Malta</i>
<i>Operations Office</i>	<i>1</i>	<i>Herzliya, Israel</i>



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	03.57.30	Secure Software Standard v1.2	23-45.01357.005	22 Jan 2027

* 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))	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> 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)	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
• Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

If Yes:

Name of Service Provider:	Description of Services Provided:
Amazon Web Services (AWS)	Transmission
Google Cloud Platform (GCP)	Transmission
Markley Boston LLC	Transmission and colocation
Telehouse	Transmission and colocation
Elasticsearch. Inc.	Log analysis services provided.
CrowdStrike, Inc.	AV security services
Cloudflare, Inc	Cloud security services
Computop Paygate GmbH	Transmission and processing
Cybersource Corporation (Cybersource)	Transmission and processing
eMerchantPay Limited (UK) (ECP)	Transmission and processing
Redsys	Transmission and processing
Worldpay	Transmission and processing
Visa Europe Ltd	Acquiring (card brand)
Mastercard	Acquiring (card brand)
Amex	Acquiring (card brand)

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: Payment processing and acquiring

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 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



<p>For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.</p>	<p>1.3.3 - N/A - No wireless Networks are in scope. 2.3.1 - N/A - No wireless Networks are in scope. 2.3.2 - N/A - No wireless Networks are in scope. 3.3.3 - N/A - Entity is not an issuer or supporting issuing services. 3.5.1.1 - N/A – No Hashing is used. 3.7.2 - N/A - No Distribution of cryptographic keys used to protect stored account data. 3.7.6 - N/A - No Distribution of cryptographic keys used to protect stored account data. 4.2.1.2 - N/A - No wireless Networks are in scope. 4.2.2 - N/A - No end-user messaging used to send PAN. 5.2.3.1 - N/A - All systems have been deployed with Anti-Malware solution. 5.3.2.1 - N/A - Updates and continuous behavioral analysis are used. 6.4.1 - N/A - this requirement is superseded by requirement 6.4.2, furthermore, the automated technical solutions used is a WAF. 8.2.3 - N/A - No Service providers with remote access. 8.3.10 - N/A - No Customers have access to the CDE. 8.3.10.1 - N/A - No Customers have access to the CDE. 9.4 - N/A - No Media in scope. 9.5 - N/A - No POI Devices in scope. 10.7.1 - N/A - This requirement is superseded by Requirement 10.7.2. 11.4.7 - N/A - Entity is not a multi-tenant service provider. 12.3.2 - N/A - No requirement has been met with a customized approach.</p>
<p>For any Not Tested responses, identify which sub-requirements were not tested and the reason.</p>	<p>N/A</p>



Section 2 Report on Compliance

(ROC Sections 1.2 and 1.3)

Date Assessment began: Note: <i>This is the first date that evidence was gathered, or observations were made.</i>	2025-06-09
Date Assessment ended: Note: <i>This is the last date that evidence was gathered, or observations were made.</i>	2025-07-01
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 2025-07-01). 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 Shift4 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

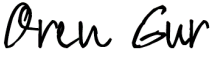
Signatory(s) confirms:

(Select all that apply)

<input checked="" type="checkbox"/>	The ROC was completed according to <i>PCI DSS</i> , Version 4.0.1 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 the Assessment in all material respects.
<input checked="" type="checkbox"/>	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Service Provider Attestation

Signed by:


7199D2CAFE73492...

Signature of Service Provider Executive Officer ↑	Date: 2025-07-01
Service Provider Executive Officer Name: Oren Gur	Title: <i>Global VP of Enterprise Security & Compliance</i>

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:

Signed by:


A0066905F49C4FF...

Signature of Lead QSA ↑	Date: 2025-07-01
Lead QSA Name: <i>Kevin Campbell</i>	

DocuSigned by:


DA9183992C8C4CD...

Signature of Duly Authorized Officer of QSA Company ↑	Date: 2025-07-01
Duly Authorized Officer Name: <i>Trevor Axiak</i>	QSA Company: <i>Kyte Consultants Ltd</i>



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/