Payment Card Industry

Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0

Revision 2

Publication Date: August 2023

PCI DSS v4.0 Attestation of Compliance for Report on Compliance – Service Providers

Entity Name: Online Payments Group AG d/b/a SecurionPay

Assessment End Date: 31-JUL-2024

Date of Report as noted in the Report on Compliance: 31-JUL-2024

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:	Online Payments Group AG
DBA (doing business as):	SecurionPay
Company mailing address:	3501 Corporate Center Valley, PA 18034, USA
Company main website:	www.Shift4.com
Company contact name:	Andrew Soriano
Company contact title:	Director, Enterprise Security and Compliance
Contact phone number:	+1 949.307.7912
Contact e-mail address:	asoriano@@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):	Not applicable
Qualified Security Assessor	
Company name:	Payment Software Company (d/b/a PSC)
Company mailing address:	11 E Adams St, Suite 400, Chicago, IL. 60603
Company website:	www.paysw.com
Lead Assessor name:	Michael Arends
Assessor phone number:	+1 800 813 3523 #5
Assessor e-mail address:	mcox@paysw.com
Assessor certificate number:	QSA, CISA, CISSP

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:	SecurionPay Payment Gateway	
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):		

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:	**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:	Not Applicable

Part 2b. Description of Role with Payment Cards (ROC Section 2.1)

Describe how the business stores, processes, and/or transmits account data.	Client is an online Payment Gateway providing a comprehensive range of payment and back office services to a wide range of merchants. Client requires cardholder data to facilitate payment processing for their merchant portfolio. Client provides both integration tools and API gateways to their merchant portfolio to support the

	processing and onward transmission of card data to the acquirer.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Not applicable
Describe system components that could impact the security of account data.	Vault database stores cardholder data to accept transactions and passed on to processors. The cardholder data is stored encrypted and the SAD is stored until authorization is complete then purged. AWS is the hosting provider for the CDE.

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.*	**Payment Channels:** e-commerce **People reviewed:** All personnel involved in the management of servers and support functions. Developers working on the applications in scope. Client management with oversight of the processes. **Processes reviewed:** All technical operations, whether involved in managing third party providers or internally managed systems, development processes, incident management and compliance monitoring processes. Technologies reviewed: AWS Security Groups, hosted servers, applications and security tools, network connections and systems configurations, Service Provider AOCs for outsourced services. **Locations reviewed:** Amazon Web Services Data Center via AOC review.
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*
Data centers	2	AWS eu-west-1

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
Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable

♦ 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 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:**
Amazon Web Services	Cloud Hosting Provider
Cloudflare	Traffic management and security facilities

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: SecurionPay Payment Gateway

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If Below Method(s) Was Used	
	In Place	Not Applicable	Not Tested	Not in Place	Customized Approach	Compensating Controls
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.	1.3.3 - Wireless is not in-scope 1.4.5 - Mobile devices are not used to connect directly to the CDE. 1.5.1 - Mobile devices do not have direct connectivity to the CDE hosted in cloud environment. 2.2.5 - The entity does not have any insecure services, protocols, or daemons. 2.3.1 - Wireless does not connect to the CDE. 2.3.2 - Wireless does not connect to the CDE. 3.3.3 - Entity is not an issuer or supports issuing services 3.4.2 - Best practice until March 31, 2025 3.5.1 - Best practice until March 31, 2025 3.5.1.1 - Truncated or hashed PANs are not used 3.5.1.2 - Disk-level or partition-level is not used to render PAN unreadable 3.5.1.3 - Disk-level or partition-level is not used to render PAN unreadable 3.6.1.3 - Clear text keys are not used. 3.7.2 - Keys are not distributed to external entities. 3.7.6 - Entity does not store, process or transmit CHD, PAN or SAD as part of their service offering. 3.7.9 - Entity does not share keys with customers. 4.2.1.1 - Best practice until March 31, 2025 4.2.1.2 - Best practice until March 31, 2025 4.2.2 - PAN is not sent by end user technologies. 5.2.1 - Entity does not have any systems that were deemed exempt from anti-malware protection. 5.2.3 - Entity does not have any systems that were deemed exempt from anti-malware protection 5.2.3.1 - Entity deployed a malware solution that performs behavioral based/continuous scanning. 5.3.2.1 - Entity deployed a malware solution that performs behavioral based/continuous scanning. 5.3.3 - Entity does not utilize removable media. 5.4.1 - Best practice until March 31, 2025 6.3.2 - Best practice until March 31, 2025 6.4.3 - Best practice until March 31, 2025 6.5.2 - No significant changes were identified. 7.2.4 - Best practice until March 31, 2025 7.2.5 - Best practice until March 31, 2025 8.2.2 - Entity does not use shared or group accounts. 8.2.3 - Entity does not have access to customer premises. 8.2.5 - Entity did not have any separated users within the assessment period. 8.2.7 - Third-parties do not have access, support, or maintain system components. 8.3.9 - Passwords/passphrases are not used as the only authentication factor

	8.3.10 - Customers do not have access to cardholder data. 8.3.10.1 - Customers do not have access to cardholder data. 8.6.1 - Best practice until March 31, 2025 8.6.2 - Best practice until March 31, 2025 8.6.3 - Best practice until March 31, 2025 9.4.1 - Removable media is not used. 9.4.1.1 - Removable media is not used. 9.4.1.2 - Removable media is not used. 9.4.2 - Removable media is not used. 9.4.3 - Removable media is not used. 9.4.4 - Removable media is not used. 9.4.5 - Removable media is not used. 9.4.5.1 - Removable media is not used. 9.4.6 - Hard copy materials do not store cardholder data. 9.4.7 - Removable media is not used. 9.5.1 - Entity does not manage POI/POS Devices 9.5.1.1 - Entity does not manage POI/POS Devices 9.5.1.2 - Entity does not manage POI/POS Devices 9.5.1.2.1 - Entity does not manage POI/POS Devices 9.5.1.3 - Entity does not manage POI/POS Devices 10.4.2 - All system components are covered by AWS AOC 10.4.2.1 - All systems and associated logs are reviewed as defined in Requirement 10.4.1 10.7.1- Best practice until March 31, 2025 10.7.2 - Best practice until March 31, 2025 10.7.3 - Best practice until March 31, 2025 11.2.1 - Wireless is not in-scope 11.2.2 - Wireless is not in-scope 11.3.1.1 - Best practice until March 31, 2025 11.3.1.2 - Best practice until March 31, 2025 11.3.1.3 - Best practice until March 31, 2025 11.3.2.1 - No significant changes occurred this assessment period. 11.4.7 - Entity is not a multi-tenant service provider. 11.5.1.1 - Best practice until March 31, 2025 11.6.1 - Payment pages are not part of the service offering. 12.3.1 - Best practice until March 31, 2025 12.3.2 - Best practice until March 31, 2025 12.3.3 - Best practice until March 31, 2025 12.3.4 - This requirement is a best practice until 31 March 2025 12.5.3 - No significant changes have occurred. 12.6.3.1 - Best practice until March 31, 2025 12.6.3.2 - Best practice until March 31, 2025

	12.10.4.1 - Best practice until March 31, 2025 12.10.7 - Best practice until March 31, 2025 A1.1.2 - A1.2.3 - Entity is not a multi-tenant hosting provider. A2.1.1 through A2.1.3 - POS/POI devices are not used in this assessment.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	Not Applicable

Section 2 Report on Compliance

(**ROC Sections 1.2 and 1.3.2**)

Date Assessment began: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*			28-MAY-2024
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*			31-JUL-2024
Were any requirements in the ROC unable to be met due to a legal constraint?			☐ Yes ☒ No
Were any testing activities performed remotely? If yes, for each testing activity below, indicate whether remote assessment activities were performed:			☒ Yes ☐ No
• Examine documentation	☒ Yes	☐ No	
• Interview personnel	☒ Yes	☐ No	
• Examine/observe live data	☒ Yes	☐ No	
• Observe process being performed	☒ Yes	☐ No	
• Observe physical environment	☐ Yes	☒ No	
• Interactive testing	☒ Yes	☐ No	
• Other:	☐ 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 31-JUL-2024)*.

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 *Online Payments Group AG d/b/a SecurionPay* 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 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

Robb Kulin

Digitally signed by Robb Kulin
Date: 2024.08.08 07:04:08 -07'00'

Signature of Service Provider Executive Officer ↑	Date: August 8, 2024
Service Provider Executive Officer Name: Robb Kulin	Title: CIO

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 ↑ Michael Arends box SIGN 4W67RXW5-1XX26K26	Date: Aug 9, 2024
Lead QSA Name: Michael Arends	
Patrick Billman box SIGN 4LWKLX2K-1XX26K26	Aug 9, 2024
Signature of Duly Authorized Officer of QSA Company ↑	Date:
Duly Authorized Officer Name: Patrick Billman	QSA Company: Payment Software Company (d/b/a PSC)

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	☐	☐