Payment Card Industry (PCI)

Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

Revision 2

September 2022

Document Changes

Date	Version	Description
September 2022	3.2.1 Revision 2	Updated to reflect the inclusion of UnionPay as a Participating Payment Brand.

© 2006-2022 PCI Security Standards Council, LLC. All Rights Reserved.

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS).* Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

Part 1. Service Provider and Qualified Security Assessor Information					
Part 1a. Service Provider Organization Information					
Company Name:	Online Payments Group AG		DBA (doing business as):		
Contact Name:	Andrew Soriano		Title:	Sr. Compliance Program Manager	
Telephone:	+1.949.307.7912		E-mail:	ASoriano @shift4.com	
Business Address:	2202 N Irving St		City:	Allentown	
State/Province:	PA	Country:	USA	Zip:	18109
URL:	www.shift4.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	Payment Software Company (d/b/a PSC)				
Lead QSA Contact Name:	Patrick Billman		Title:	Director	
Telephone:	1-800-813-3523		E-mail:	patrick@paysw.com	
Business Address:	6081 Meridian Avenue, Suite 70 - #149		City:	San Jose	
State/Province:	CA	Country:	USA	Zip:	95120
URL:	www.paysw.com				

© 2006-2022 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 (check all that apply):

Name of service(s) assessed:	SecurionPay Payment Gateway

Type of service(s) assessed:

Hosting Provider:	**Managed Services (specify):**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POS / 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		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Shared Hosting 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 you feel these categories don't apply to your service, complete "Others." If you're unsure whether a category could apply to your service, consult with the applicable payment brand.*

© 2006-2022 PCI Security Standards Council, LLC. All Rights Reserved.

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 (check 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 ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☐ Other Hosting (specify):	**Managed Services (specify):** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☐ POS / 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):		
Provide a brief explanation why any checked services were not included in the assessment:	Not applicable	

Part 2b. Description of Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder 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 cardholder data to the acquirer. Cardholder data is retained when requested by merchants for reoccuring billing. CHD is contained in a database that masks the PAN and stored with disk encryption. The database storing the CHD is used for tokenization and sent to their merchants and acquirer.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Not applicable

© 2006-2022 PCI Security Standards Council, LLC. All Rights Reserved.

Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility:	Number of facilities of this type	Location(s) of facility (city, country):
Example: Retail outlets	*3*	*Boston, MA, USA*
Client offices	1	Wroclaw, Poland
Data Centers	1	AWS - Ireland
Development centers	1	Wroclaw, Poland

Part 2d. Payment Applications

Does the organization use one or more Payment Applications? ☐ Yes ☒ No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
Not applicable	Not applicable	Not applicable	Not applicable	Not applicable

Part 2e. Description of 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 POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	Payment Channels: eCommerce, MOTO 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 service 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: Development and technical functions in Wroclaw, Poland
Does your business use network segmentation to affect the scope of your PCI DSS environment? *(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*	☒ Yes ☐ No

© 2006-2022 PCI Security Standards Council, LLC. All Rights Reserved.

Part 2f. Third-Party Service Providers		
Does your company have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated?		☐ Yes ☒ No
If Yes:		
Name of QIR Company:	Not applicable	
QIR Individual Name:	Not applicable	
Description of services provided by QIR:	Not applicable	
Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?		☒ Yes ☐ No
If Yes:		
Name of service provider:	**Description of services provided:**	
Amazon Web Services (AWS)	Cloud Hosting Provider	
Cloudflare	Web Application Firewall	
Note: *Requirement 12.8 applies to all entities in this list.*		

© 2006-2022 PCI Security Standards Council, LLC. All Rights Reserved.

Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as "Not Tested" or "Not Applicable" in the ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as "Not Tested" or "Not Applicable" in the ROC.
- **None** – All sub-requirements of that requirement were marked as "Not Tested" and/or "Not Applicable" in the ROC.

For all requirements identified as either "Partial" or "None," provide details in the "Justification for Approach" column, including:

- Details of specific sub-requirements that were marked as either "Not Tested" and/or "Not Applicable" in the ROC
- Reason why sub-requirement(s) were not tested or not applicable

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	Details of Requirements Assessed			
	Full	**Partial**	**None**	**Justification for Approach** (Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)
Requirement 1:	☐	☒	☐	Not applicable: Req: 1.1.6.b - There are no insecure services Req: 1.1.6.c - There are no insecure services Req: 1.2.2.a - Routers are not in scope Req: 1.2.2.b - Routers are not in scope Req: 1.2.3.a – Wireless does not exist Req: 1.2.3.b – Wireless does not exist
Requirement 2:	☐	☒	☐	Not applicable: Req: 2.1.1.a - Wireless is not in scope Req: 2.1.1.b - Wireless is not in scope Req: 2.1.1.c - Wireless is not in scope Req: 2.1.1.d - Wireless is not in scope Req: 2.1.1.e - Wireless is not in scope Req: 2.2.2.b - There are no insecure services Req: 2.2.3 - There are no insecure services Req: 2.6 - Entity is not a hosting provider
Requirement 3:	☐	☒	☐	Not applicable: Req: 3.2.a - Client is not an issuer Req: 3.2.b - Client is not an issuer Req: 3.4.c – Removable media is not used Req: 3.4.e - Hashed and truncated PANs are not stored Req: 3.4.1.a - Disk encryption is not used Req: 3.4.1.b - Disk encryption is not used Req: 3.4.1.c - Disk encryption is not used

© 2006-2022 PCI Security Standards Council, LLC. All Rights Reserved.

				Req: 3.6.a - Client does not share keys with customers Req: 3.6.2.b – Cryptographic keys are not distributed Req: 3.6.6.a - Manual key management is not used Req: 3.6.6.b - Manual key management is not used
Requirement 4:	☐	☒	☐	Not applicable: Req: 4.1.d - Entity does not accept certificates Req: 4.1.1 - There are no wireless networks in scope Req: 4.2.a - End user messaging technology is not used to transmit CHD
Requirement 5:	☒	☐	☐	
Requirement 6:	☐	☒	☐	Not applicable: Req 6.4.6 - There have not been any significant changes
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	Not applicable: Req: 8.1.3.b – Client has had no terminated employees within the past six months Req: 8.1.5.a - Remote vendor access is not allowed Req: 8.1.5.b - Remote vendor access is not allowed Req: 8.1.6.b - Entity does not manage customer passwords. Req: 8.2.1.d - Entity does not manage customer passwords. Req: 8.2.1.e - Entity does not manage customer passwords. Req: 8.2.3.b - Entity does not manage customer passwords. Req: 8.2.4.b - Entity does not manage customer passwords. Req: 8.2.5.b - Entity does not manage customer passwords. Req: 8.5.1 - Entity does not have remote access to customer environments
Requirement 9:	☐	☒	☐	Not applicable: Req: 9.5 – Media is not used Req: 9.5.1 - Media is never sent offsite Req: 9.6 – Media is not used Req: 9.6.1 – Media is not used Req: 9.6.2.a - Media is never sent offsite Req: 9.6.2.b - Media is never sent offsite Req: 9.6.3 - Media is never sent offsite Req: 9.7 – Media is not used Req: 9.7.1 – Media is not used Req: 9.8 – Media is not used Req: 9.8.1.a – Media is not used Req: 9.8.1.b – Media is not used Req: 9.8.2 – Media is not used

© 2006-2022 PCI Security Standards Council, LLC. All Rights Reserved.

				Req: 9.9 - Client does not manage POS terminals Req: 9.9.1.a - Client does not manage POS terminals Req: 9.9.1.b - Client does not manage POS terminals Req: 9.9.1.c - Client does not manage POS terminals Req: 9.9.2.a - Client does not manage POS terminals Req: 9.9.2.b - Client does not manage POS terminals Req: 9.9.3.a - POS systems are not used by the entity Req: 9.9.3.b - POS systems are not used by the entity
Requirement 10:	☐	☒	☐	Not applicable: Req: 10.8.1.b – There have been no critical security control failures
Requirement 11:	☐	☒	☐	Not applicable: Req: 11.2.3.a – There have not been any significant changes Req: 11.2.3.b - There have not been any significant changes Req: 11.2.3.c - There have not been any significant changes Req: 11.3.1.b - The external penetration test was not performed by an internal resource Req: 11.3.2.b – The internal penetration test was not performed by an internal resource
Requirement 12:	☒	☐	☐	
Appendix A1:	☐	☐	☒	All not applicable: Entity is not a shared hosting provider
Appendix A2:	☐	☐	☒	All not applicable: POS systems are not used

© 2006-2022 PCI Security Standards Council, LLC. All Rights Reserved.

Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	*21-July-2023*	
Have compensating controls been used to meet any requirement in the ROC?	☐ Yes	☒ No
Were any requirements in the ROC identified as being not applicable (N/A)?	☒ Yes	☐ No
Were any requirements not tested?	☐ Yes	☒ No
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes	☒ No

© 2006-2022 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 the ROC dated *21 July 2023.*

Based on the results documented in the ROC noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document (***check one):***

☒	**Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby *Online Payments Group AG d/b/a SecurionPay* has demonstrated full compliance with the PCI DSS.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby *(Service Provider Company Name)* has not demonstrated full compliance with the PCI DSS. **Target Date** for Compliance: An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with the payment brand(s) before completing Part 4.*
☐	**Compliant but with Legal exception:** One or more requirements are marked "Not in Place" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand. *If checked, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement being met

Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

☒	The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version *3.2.1*, and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
☒	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
☒	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
☒	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

© 2006-2022 PCI Security Standards Council, LLC. All Rights Reserved.

Part 3a. Acknowledgement of Status (continued)	
☒	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☒	ASV scans are being completed by the PCI SSC Approved Scanning Vendor *AlertLogic, Inc.*

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	*Date:* July 25, 2023
Service Provider Executive Officer Name: **Mike Russo**	*Title:* ***CTO***

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	*Patrick Billman performed the PCI assessment.*

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* 25 Jul 2023
Duly Authorized Officer Name: Patrick Billman - Director	*QSA Company:* Payment Software Company (d/b/a PSC)

Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	*Not applicable*

[1] Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

[2] The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

[3] Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

© 2006-2022 PCI Security Standards Council, LLC. All Rights Reserved.

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement. If you answer "No" to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

Check with the applicable payment brand(s) before completing Part 4.

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 a firewall configuration to protect cardholder data	☒	☐	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☒	☐	
3	Protect stored cardholder data	☒	☐	
4	Encrypt transmission of cardholder data across open, public networks	☒	☐	
5	Protect all systems against malware and regularly update anti-virus software or programs	☒	☐	
6	Develop and maintain secure systems and applications	☒	☐	
7	Restrict access to cardholder data by business need to know	☒	☐	
8	Identify and authenticate access to system components	☒	☐	
9	Restrict physical access to cardholder data	☒	☐	
10	Track and monitor all access to network resources and cardholder data	☒	☐	
11	Regularly test security systems and processes	☒	☐	
12	Maintain a policy that addresses information security for all personnel	☒	☐	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	☒	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☒	☐	

© 2006-2022 PCI Security Standards Council, LLC. All Rights Reserved.