Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.1

April 2015

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:	PayU - internet based payment gateway service provider	
Type of service(s) 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):		

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.

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*
Head Office	1	South Africa, Cape Town
Data Center "Optinet"	1	South Africa, Johannesburg

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)
SafeShop Application	v3.0	PayU	☐ Yes ☒ No	N/A
PayU Application	v4.8	PayU	☐ Yes ☒ No	N/A
			☐ Yes ☐ No	

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 Card transactions are e-commerce only (card not present). Payments are made through the online store via a secure connection established via HTTPS and for which the server has www.payu.co.za TLS v1.2 - certificate issued by Entrust CA. Sensitive authentication data from the website (CVV2, CVC2) is transmitted via PayU servers to the acquiring bank, for authorization and the SAD is not stored in local databases nor in any other format. All applications are card-not-present from the following sources: phone order, internet order, authenticated Mobile App ("AMT") via Oltio branded "PayD", debit and credit cards mobile assisted internet order (Card PIN and/or CVV2 communicated directly from cardholder handset via encrypted session to Oltio switch). On successful authorization the PAN is encrypted and stored in an MS SQL 2005, MySQL databases. All displays of PAN are masked. Links to the acquiring banks for authorization are encrypted.
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

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:	PayU - internet based payment gateway service provider			
	Details of Requirements Assessed			
PCI DSS Requirement	**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:	☐	☒	☐	**1.2.3 - No wireless in company's LAN.**
Requirement 2:	☐	☒	☐	**2.1.1 - No wireless environments connected to the CDE** **2.2.3 - No insecure services, protocols, or daemons found.** **2.6 - Entity is not a shared hosting provider.**
Requirement 3:	☐	☒	☐	**3.2 - Entity is not an issuer** **3.4.1 – No disk encryption is used.** **3.6 - Entity does not share keys with their customers for transmission and storage of cardholder data.**
Requirement 4:	☐	☒	☐	**4.1.1 - No wireless in CDE.**
Requirement 5:	☒	☐	☐	
Requirement 6:	☒	☐	☐	
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	**8.1.5 - As a service provider entity does not provide access to the vendors.** **8.5.1 - Entity is a service provider, but does not have any remote access to customer premises**
Requirement 9:	☐	☒	☐	**9.8.1 - Entity environment does not interact with card-reading devices.**

Section 2: Report on Compliance

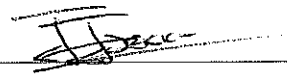
This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	8 October 2015
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

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 *Qualys, (ref 3728-01-10)*

Part 3b. Service Provider Attestation



Signature of Service Provider Executive Officer ↑	*Date:* **8 October 2015**
Service Provider Executive Officer Name: **Johan Dekker**	*Title:* **COO**

Part 3c. QSA Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	Conduct formal assessment of compliance for PayU.

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* **8 October 2015**
Duly Authorized Officer Name: **Bogdan Bondar**	*QSA Company:* **Sysnet Global Solutions**

Part 3d. ISA Acknowledgement (if applicable)

If an ISA was involved or assisted with this assessment, describe the role performed:	Not Applicable

Signature of ISA ↑	*Date:*
ISA Name:	*Title:*

[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.