Security
Standards Council

Payment Card Industry (PCI)
Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

June 2018

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:	Tucasi Ltd		DBA (doing business as):	Tucasi	
Contact Name:	Nathan Foley		Title:	Head of Development and Infrastructure	
Telephone:	+44 02380 016 564		E-mail:	nfoley@tucasi.com	
Business Address:	Wessex House, Upper Market St		City:	Eastleigh	
State/Province:	Hampshire	Country:	United Kingdom	Zip:	SO50 9FD
URL:	www.tucasi.com				

Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:	Sec-1 Ltd				
Lead QSA Contact Name:	Stuart Pilkington		Title:	Senior Security Consultant	
Telephone:	+44 1924 284240		E-mail:	stuartp@sec-1.com	
Business Address:	Unit 1 Centre 27 Business Park, Bankwood Way		City:	Birstall	
State/Province:	West Yorkshire	Country:	United Kingdom	Zip:	WF17 9TB
URL:	www.sec-1.com				

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:	Scopay	
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 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:	Not Applicable

Type of service(s) not assessed:

Hosting Provider:	**Managed Services (specify):**	**Payment Processing:**
□ Applications / software □ Hardware □ Infrastructure / Network □ Physical space (co-location) □ Storage □ Web □ Security services □ 3-D Secure Hosting Provider □ Shared Hosting Provider □ Other Hosting (specify):	□ Systems security services □ IT support □ Physical security □ Terminal Management System □ Other services (specify):	□ 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:	

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Not Applicable as Tucasi support payments on behalf of their clients using iframe and redirect techniques, therefore, never receive CHD.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Tucasi is a service provider, that provides an e-commerce site for clients to make payments. The in-scope e-commerce website provided by Tucasi covered in this assessment (www.scopay.com) is hosted with CWCS, and will only serve either a web redirect or an iframe when payments are to be taken. Only Tucasi staff will have access to the in-scope webservers - never Tucasi client's staff - so only Tucasi's staff will be able to impact on the security of CHD.

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*
Development Office	1	Eastleigh, Hampshire, United Kingdom

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)
			□ Yes □ No	
			□ Yes □ No	
			□ Yes □ No	
			□ Yes □ No	
			□ Yes □ No	
			□ Yes □ No	
			□ Yes □ No	
			□ 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.*	Tucasi's in-scope e-commerce service does not receive cardholder data, therefore Tucasi does not have a cardholder data environment. The two in-scope webservers provide an iframe or redirect mechanism and therefore is in scope for applicable requirements from SAQ A. Technical staff within Tucasi are responsible for the management and hosting of the solution (Scopay) and the payment pages, which are dependent on which payment gateway is used by the customer. The colocation webservers are hosted with an external hosting provider called CWCS, but are fully managed by Tucasi. The in-scope e-

	commerce website is located at www.scopay.com.
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 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:	
QIR Individual Name:	
Description of services provided by QIR:	
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:**
CWCS	Web Hosting
Braintree	Payment processor
Worldpay	Payment processor
Optomany	Payment Processor

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

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:	Scopay

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:	□	□	☒	All requirements in Requirement 1 are marked as not applicable as the assessment is aligned with the requirements from SAQ A.
Requirement 2:	□	☒	□	All requirements apart from 2.1 and 2.5 were marked as not applicable as the assessment is aligned to the requirements from SAQ A.
Requirement 3:	□	☒	□	All requirements apart from 3.2.1, 3.2.2 and 3.2.3 were marked as not applicable as the assessment is aligned to the requirements from SAQ A.
Requirement 4:	□	□	☒	All requirements in Requirement 4 are marked as not applicable as the assessment is aligned with the requirements from SAQ A.
Requirement 5:	□	□	☒	All requirements in Requirement 5 are marked as not applicable as the assessment is aligned with the requirements from SAQ A.
Requirement 6:	□	☒	□	All requirements apart from 6.2 and 6.7 were marked as not applicable as the assessment is aligned to the requirements from SAQ A.
Requirement 7:	□	□	☒	All requirements in Requirement 7 are marked as not applicable as the assessment is aligned with the requirements from SAQ A.

Requirement 8:	□	☒	□	All requirements apart from 8.1, 8.2, 8.5 and 8.8 were marked as not applicable as the assessment is aligned to the requirements from SAQ A.
Requirement 9:	□	□	☒	All requirements in Requirement 9 are marked as 'not applicable' as the assessment is aligned with the requirements from SAQ A. The requirements from Requirement 9 that are in-scope for SAQ A are also marked as not applicable as they are concerned with CHD on paper media, and Tucasi will never come into contact with CHD belonging to clients.
Requirement 10:	□	□	☒	All requirements in Requirement 10 are marked as not applicable as the assessment is aligned with the requirements from SAQ A.
Requirement 11:	□	☒	□	All requirements apart from 11.2 were marked as not applicable as the assessment is aligned to the requirements from SAQ A and Tucasi is conducted quarterly ASV scans
Requirement 12:	□	☒	□	All requirements apart from 12.8, 12.9 and 12.10 were marked as not applicable as the assessment is aligned to the requirements from SAQ A.
Appendix A1:	□	□	☒	All requirements in Appendix A1 are marked as not applicable as Tucasi is not a shared hosting provider.
Appendix A2:	□	□	☒	All requirements in Appendix A2 are marked as not applicable as the solution under assessment does not involve the use of SSL/Early TLS for Card-Present POS POI Terminal Connections.

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:	20th May 2022	
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

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated 20th May 2022.

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 Tucasi 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.

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

Part 3b. Service Provider Attestation

Nathan F *Signature of Service Provider Executive Officer ↑*	*Date:* 20/05/2022
Service Provider Executive Officer Name: Nathan Foley	*Title:* Head of Development and Infrastructure

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

If a QSA was involved or assisted with this assessment, describe the role performed:	Performed a partial ROC assessment against applicable requirements from SAQ A after confirming the in scope e-commerce service only supports iframe and web redirect payment technology.

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* 20th May 2022
Duly Authorized Officer Name: Stuart Pilkington	*QSA Company:* Sec-1 Ltd

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:	

[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.

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	□	□	

AMERICAN EXPRESS DISCOVER JCB mastercard VISA