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:	Bamcard d.d.		DBA (doing business as):	Bamcard	
Contact Name:	Merima Đozic		Title:	CISO	
Telephone:	+387 61 739 583		E-mail:	merima.dozic@bamcard.ba	
Business Address:	Trg Heroja 10/II		City:	Sarajevo, Bonsia	
State/Province:		Country:	Bonsia and Herzegovina	Zip:	71000
URL:	merima.dozic@bamcard.ba				

Part 1b. Qualified Security Assessor Company Information (if applicable)					
Company Name:	Sovereign Secure Limited				
Lead QSA Contact Name:	Cetin Guldali		Title:	Senior Security Consultant	
Telephone:	+90 533 0 933 100		E-mail:	cetin.guldali@sovereignsecure.co.uk	
Business Address:	79 Market Street, Farnworth		City:	Bolton	
State/Province:	Greater Manchester	Country:	United Kingdom	Zip:	BL4 7NS
URL:	https://sovereignsecure.co.uk				

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:	Authorisation Clearing Settlement and Card Issuance	
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	☐ 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):

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.	Bamcard is a processor that providing services to financial institution clients, which are the banks. It receives all transactions, such as e-commerce, MOTO and/or bricks and mortar, from its client banks for acquiring/settling or access to the Visa VAP and MasterCard MIP. The following services are provided: • ATM acquiring. • POS cash advance. • Retail POS transactions including Card-Not-Present transactions for issued cards - clearing processing only. • Clearing and settlement data processing. • Card data generation; and • Payment cards personalization.

	All payment card transactions are routed through Bamcard' s financial institution clients, which mean Bamcard receives those transactions directly from the banks.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Bamcard provides real-time authorization and switching for card present transactions from ATMs and POSs that belonged to their clients, which are the banks.

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*
Data centers	1	Sarajevo, Bosnia and Herzegovina

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).*	All card transactions are routed through the banks networks before reaching Bamcard's systems. Bamcard stores, processes and transmits cardholder data.

• *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*	Cardholder Not Present (CNP) transactions are only applicable for issuing cards of Bamcard' s clients. The network in which the CHD is located is protected behind 3 firewalls, the first is a Checkpoint Firewall which is used for IDS/IPS, an external CISCO ASA firewall which also used for IDS/IPS and the third firewall is the CISCO ASA Inner Firewall.
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:**
MasterCard	Payment Processors
VISA	Payment Processors

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:	

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:	☐	☒	☐	1.2.3. Not Applicable. wireless scan reports confirmed that there is no wireless networks within scope of this assessment.
Requirement 2:	☐	☒	☐	2.2.1 Not Applicable. wireless scan reports confirmed that there is no wireless networks within scope of this assessment. 2.2.2, 2.2.3 Not Applicable insecure services, daemons, or protocols are not enabled 2.6 Not applicable Bam Card are not a shared hosting service provider.
Requirement 3:	☐	☒	☐	3.2.c, 3.2.d Not Applicable No sensitive authentication data is received. 3.2.1 Not Applicable – Bamcard do not store the full contents of any track 3.2.2 Not Applicable – Bamcard do not store the card verification code 3.2.3 Not Applicable – Bamcard do not store the personal identification number (PIN) or the encrypted PIN block after authorization. 3.4.c Not Applicable Bamcard is not using any removable media for any purposes.

Requirement 4:	☐	☐	☒	4 Not applicable Bamcard is not transmitting or receiving any cardholder data via over open, public networks.
Requirement 5:	☒	☐	☐	
Requirement 6:	☐	☒	☐	6.3, 6.4, 6.5, 6.6. Not Applicable Bamcard does not develop software applications
Requirement 7:	☒	☐	☐	
Requirement 8:	☐	☒	☐	8.1.5. Not Applicable – No vendors are permitted to access, support or maintain the system components in the cardholder data environment through remote access. 8.1.6. 8.2.3.b, 8,2,4.b, 8.2.5.b Not Applicable Bamcard do not use non-consumer customer user accounts 8.2.2 Not Applicable non-face-to-face methods are not allowed 8.3.2.Not Applicable – Remote access is not allowed 8.5.1. Not Applicable – Bamcard don't have remote access to each customers' environment.
Requirement 9:	☐	☒	☐	9.6.2 Not Applicable - Media were not allowed to be sent out of the facility. 9.9 Not Applicable - no cardholder data capturing device is in the environment under current assessment and POS devices were not the responsibility of Bamcard.
Requirement 10:	☒	☐	☐	
Requirement 11:	☐	☒	☐	11.1.1 Not Applicable. wireless scan reports and confirmed that there is no wireless network into assessment scope.
Requirement 12:	☐	☒	☐	12.8 Not Applicable. Cardholder data was not shared with service providers.
Appendix A1:	☐	☐	☒	Not applicable Bam Card are not a shared hosting service provider.
Appendix A2:	☐	☐	☒	Not applicable Bam Card do not manage POS 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:	14/04/2023	
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

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated 14/04/2023 **.**

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 Bamcard d.d. 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 Atsec

Part 3b. Service Provider Attestation

Signature of Service Provider Executive Officer ↑	*Date:* 16/04/2023
Service Provider Executive Officer Name: Asim Avdagić	*Title:* CEO

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

If a QSA was involved or assisted with this assessment, describe the role performed:	Assessor role

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* 16/04/2023
Duly Authorized Officer Name: Cetin Guldali	*QSA Company:* Sovereign Secure Limited

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	☒	☐