Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ D-SP (Section 2), dated (SAQ completion date).

Based on the results documented in the SAQ D-SP 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 SAQ D-SP are complete, and all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby (Usmon FinTech LLC) has demonstrated full compliance with the PCI DSS.
○	**Non-Compliant:** Not all sections of the PCI DSS SAQ D-SP are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby () 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 "No" 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)

☑	PCI DSS Self-Assessment Questionnaire D-SP, Version 3.2.1, was completed according to the instructions therein.
☑	All information within the above-referenced SAQ 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.
☑	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 Clone Systems

[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 3b. Service Provider Attestation

Signature of Service Provider Executive Officer	Date: 27/02/2024
Service Provider Executive Officer Name: Beknazarov Abdullo	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:

Signature of Duly Authorized Officer of QSA Company	Date:
Duly Authorized Officer Name:	QSA Company:

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:

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 payment brand(s) before completing Part 4.

PCI DSS Requirement*	Description of Requirement	Compliance 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.	◉	○	

* PCI DSS Requirements indicated here refer to the questions in Section 2 of the SAQ.