COMPLIANCE
CONTROL

CERTIFICATE OF PCI DSS COMPLIANCE

This is confirmation that the Entity:

CJSC «Markazi Tekhnologiyahoi Muosir»

Has been assessed by Compliance Control Ltd. and was found to be compliant with
Payment Card Industry Data Security Standards 3.2.1
It was confirmed by annual security assessment performed by QSAs of Compliance Control Ltd.

Certificate is valid till:	**7 December 2024**
PCI DSS version:	**3.2.1**
Certificate No.	**TA8A-IO4L-78F7**

Issue date:
8 December 2023

Ivan Tverdokhlebov
Director

Signature

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.

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:	CJSC “Markazi Tekhnologiyahoi Muosir”	DBA (doing business as):	MTM		
Contact Name:	Olim Karimov	Title:	Head of Information Security Department		
Telephone:	+992880009099	E-mail:	o.karimov@mtm.tj		
Business Address:	37/1a Bokhtar str.	City:	Dushanbe		
State/Province:	Dushanbe	Country:	Tajikistan	Zip:	734000
URL:	https://mtm.tj/				

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

Company Name:	Compliance Control Ltd.				
Lead QSA Contact Name:	Yevhen Koshelkov	Title:	QSA/QPA/3DSA		
Telephone:	+380633853243	E-mail:	ykoshelkov@compliance-control.team		
Business Address:	Punane tn. 16/1-414	City:	Tallinn		
State/Province:	Harju	Country:	Estonia	Zip:	13619
URL:	https://www.compliance-control.eu				

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:	MTM Payment Processing	
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:		
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:		

Part 2b. Description of Payment Card Business	
Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	The main direction of CJSC “Markazi Tekhnologiyahoi Muosir” is the implementation of multiple projects of Local cards and electronic wallets, which simultaneously participate in the domestic program for unifying acquiring networks called “Imcon”. The main priorities of these projects for issuing Local cards are Electronic Wallets, virtual cards and modern Internet technologies, making payments and transferring funds in addition to traditional banking products and services. CJSC "Markazi Technologyhoi Muosir" is the only third-party Processing center in the Republic of Tajikistan. Current transaction amount for CNP and CP operations is 1.319.919 for last year.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Currently, the entity utilizes BPC AG SmartVista 2.2.25.R-ACS approved by VISA, Reference No. 3DS2.2.0BPC1254ACS / 2.2.25.R-3DSS approved by VISA, Reference No. 3DS2.2.0BPC12343DSS, a complex solution that ensures secure payment cards usage in Internet. The solution supports inter-host interaction with issuers and acquirers, as well as with international payment systems.

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 and own data center	1	37/1a Bokhtar str, Business Center “Bokhtar” building, office #906, Dushanbe, Tajikistan

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)
BPC SmartVista FE	2.2.10	BPC	☒ Yes ☐ No	28.10.2022
			☐ 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.*	The scope of this assessment includes: • main payment and infrastructure systems - processing system SmartVista, Oracle virtual infrastructure, security systems, and components of these systems; - hypervisors, web servers, application servers, database servers, authentication servers, time servers (NTP), firewalls, switches, routers, network security devices (IPS); • Computing network of MTM, segmentation of the computer network and external network connections; • information security management processes required by PCI DSS; • personnel who has access to the information environment and / or data on payment card holders: administrators, payment system operators, security staff.
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:**
Payment-guide	Termination service for Bank's devices

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:	MTM Payment Processing

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 - There are no wireless networks in the provider's cardholder data environment.**
Requirement 2:	☐	☒	☐	**2.1.1 - There are no wireless environments connected to cardholder data environment or transmitting cardholder data.** **2.6 - The organization is not a shared hosting provider.**
Requirement 3:	☐	☒	☐	**3.4.1 - Disk encryption is not used.**
Requirement 4:	☐	☒	☐	**4.1.1 - There are no wireless networks transmitting cardholder data and even connected to cardholder data environment.** **4.2 - PANs are not sent via end-user message services.**
Requirement 5:	☒	☐	☐	
Requirement 6:	☐	☒	☐	**6.3, 6.3.1, 6.3.2, 6.5, 6.5.1 - 6.5.10 - The entity uses payment application from its vendor BPC and does not use internally developed payment applications. Therefore, software development processes are not in the scope of this PCI DSS assessment.** **6.4.6 - No significant change occurred within the past 12 month.**
Requirement 7:	☒	☐	☐	

Requirement 8:	☐	☒	☐	**8.1.5 - No active vendor accounts for remote access** **8.5.1 - The entity's business services don't expect any type of access to customers.**
Requirement 9:	☐	☒	☐	**9.6.2 and 9.6.3 - No media with CHD are sent ouside the facility.**
Requirement 10:	☒	☐	☐	
Requirement 11:	☐	☒	☐	**11.1.1 - There are no wireless networks and technologies used in the cardholder data environment.**
Requirement 12:	☐	☒	☐	**12.3.9 - The organization prohibits the remote-access technologies usage for vendors and business partners.**
Appendix A1:	☐	☒	☐	**The organization is not a shared hosting provider.**
Appendix A2:	☐	☒	☐	**The organization does not use SSL / early TLS.**

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:	*08/12/2023*	
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 ***08/12/2023*** **.**

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 *CJSC "Markazi Tekhnologiyahoi Muosir"* 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, CVN2, CVV2, or CID 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, Inc. PCI cert. #4262-01-16.*

Part 3b. Service Provider Attestation	
Signature of Service Provider Executive Officer ↑	*Date:* **08/12/2023**
Service Provider Executive Officer Name: **Olim Karimov**	*Title:* **Head of Information Security Department**

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)	
If a QSA was involved or assisted with this assessment, describe the role performed:	*Compliance Control Ltd. performed the assessment*
Signature of Duly Authorized Officer of QSA Company ↑	*Date: 08/12/2023*
Duly Authorized Officer Name: Yevhen Koshelkov	*QSA Company:* Compliance Control 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 Global Network JCB UnionPay 银联 VISA