Joint-Stock Company
«Common Republican
Processing Center»

APPROVED
by the Supervisory Board of JSC
“Common Republican Processing Centre”
(Minutes of Meeting dated 26 January 2026)
and by Order of the Executive Body
(Order No. 15 dated 29 January 2026)

RULES OF THE UZCARD PAYMENT SYSTEM

(Version: 2.3.)

Tashkent - 2026

TABLE OF CONTENTS

1. PURPOSE OF THE DOCUMENT 5
2. GENERAL INFORMATION 6
3. STANDARDS AND REGULATIONS OF PS 6
4. TERMS AND DEFINITIONS 7
5. DETAILS OF THE OPERATOR 12
6. REQUIREMENTS TO OPERATION OF THE PS 12
7. APPLICATION AND SCOPE OF THE RULES 15
8. TYPES AND CRITERIA OF PARTICIPATION, SUSPENSION OF PARTICIPATION IN PS 19
9. RESPONSIBILITY FOR FAILURE TO FULFILL THE PS RULES 23
10. REGISTRATION OF PARTICIPANTS, AFFILIATES AND BRANCHES. ASSIGNING BIN 24
11. ISSUE 25
12. INFORMING AND AUTHENTICATION IN THE FRAMEWORK OF PS 29
13. TYPES OF BC 30
14. ACQUIRING 39
15. OPERATOR SERVICE PRICE AND SETTLEMENT OF ACCOUNTS 44
16. INTERSYSTEM INTERACTION OF PS AND PPS 45
17. PROCEDURE OF IMPLEMENTING OPERATIONS IN PS 46
18. ONLINE INTERFACE WITH ABS OF PARTICIPANTS, INTERFACES BETWEEN PS AND ABS OF PARTICIPANTS 47
19. STATEMENT UPLOADING FORMAT 47
20. COMMISSION 48
21. MSE CANCEL AND REFUND TRANSACTIONS 49
22. PROCESSING OF AUTHORIZED TRANSACTIONS IN PS 50
23. GENERATING AND SENDING NET POSITIONS TO SETTLEMENT BANK 50
24. INTER-BANK SETTLEMENT PROCESS. ORGANIZATION OF INTERACTION OF SETTLEMENT BANK WITH PS 50
25. TIME AND PROCEDURE OF SENDING FILES FROM PS 51
26. REQUIREMENTS TO SETTLEMENT BANK 51
27. TRANSACTION DAY. CLOSE OF TRANSACTION DAY 51
28. CLOSING AND OPENING OF FISCAL YEAR 52
29. COLLECTION OF INFORMATION ABOUT FRAUDULENCE WITH BC 52
30. ENSURING SECURITY AND INFORMATION PROTECTION 52
31. PROCEDURE OF IDENTIFYING ABUSE AND APPLYING ENFORCEMENT ACTIONS 57

32. SETTLEMENT OF DISPUTES BETWEEN THE PARTICIPANTS OF PS 63
33. REQUIREMENTS TO PARTICIPANTS' COMPLIANCE WITH AML/CFT/FPWMD LAWS .65
34. ANTI-CORRUPTION REQUIREMENTS TO PS PARTICIPANTS 67
35. ANTI-FRAUD REQUIREMENTS TO PARTICIPANTS 68
36. SETTLEMENT OF DISPUTABLE SITUATIONS 69
37. RISK MANAGEMENT SYSTEM IN PS 69
38. LIMITATION OF LIABILITY OF PS 70

1. PURPOSE OF THE DOCUMENT

1.1. These Rules have been developed by Joint-Stock Company “Common Republican Processing Centre” – the Operator of the UZCARD Payment System, in accordance with the Law of the Republic of Uzbekistan "On Payments and Payment Systems," the Law of the Republic of Uzbekistan "On Banks and Banking Activities," other regulatory legal acts of the Republic of Uzbekistan, and applicable international law.

1.2. The UZCARD Payment System Rules (hereinafter referred to as the Rules) determine the functioning procedures of the UZCARD payment system, including the payment procedure, the use of payment message formats, the operating schedule, the risk management system, description of services, payment order revocation procedure, the insolvency resolution procedure for participants, the procedure for compliance with information security and cybersecurity requirements, and the measures applied to participants for violating these Rules.

1.3. These Rules are addressed to and binding on all Participants of the UZCARD Payment System. They are aimed at minimizing and managing risks, ensuring uninterrupted operation and creating uniform standards for the efficient and secure execution of payments throughout the Republic of Uzbekistan.

1.4. The Rules are published on the website of JSC “Common Republican Processing Centre” (hereinafter referred to as the Operator) within three (3) business days of their approval by the Operator. The Rules are applied by the Operator and Participants of the UZCARD Payment System fifteen (15) calendar days after their publication on the Website.

1.5. Accession to these Rules means that the Participant of the UZCARD Payment System accepts all the terms of these Rules without any exceptions or limitations.

1.6. The Operator reserves the right to unilaterally amend and supplement the effective Rules in the manner specified in the clauses 1.4 and 1.5 above.

1.7. The Operator reserves the right to unilaterally amend the internal regulatory documents of the UZCARD Payment System. The Operator shall notify Participants about changes to these internal regulatory documents by posting a notice on the Website. The

Operator reserves the right to use other available means of notifying the Participants.

1.8. If, as a result of changes in the legislation of the Republic of Uzbekistan, individual provisions of the Rules contradict to the imperative norms of the laws, such provisions shall cease to be effective, and the provisions of the laws shall prevail. In case of a conflict between the Rules and provisional rules of the laws, the provisions of the Rules shall apply. Clauses that conflict with imperative norms of the laws shall not affect the legal validity of the remaining clauses of the Rules. The Operator reserves the right, at its sole discretion, to amend the Rules to replace invalid clauses with new clauses of similar content that do not conflict with the laws.

2. GENERAL INFORMATION

2.1. The Rules apply to:

- Participants' activities in the Republic of Uzbekistan;
- implementation of Transactions and provision of payment services in the Republic of Uzbekistan;
- operational services provided by the Operator, in accordance with the terms of the Rules.

2.2. The Rules describe the principles and requirements that apply to participants of the payment system:

- creating a fundamental document outlining the rules and procedures for smooth and efficient operation;
- using these principles as general guidelines or principles in business negotiations, transactions, and business decisions for which separate chapters or sections are not established;
- ensuring consistency and smooth operation of the payment system.

3. STANDARDS AND REGULATIONS OF PS

3.1. Standards and Regulations are an integral part of the Rules and regulate:

a) the principles for applying remuneration, determining the rates and terms of collection;

b) the principles for interaction between Participants, payment organizations, and other entities that are not UZCARD Payment

System Participants but provide payment services and interact with the Operator;

c) the principles for resolving disputes arising between UZCARD Payment System Participants, including those involving payment organizations and other entities that are not UZCARD Payment System Participants but provide payment services and interact with the Operator;

d) the procedure for applying to the Operator, the rights and obligations of UZCARD Payment System Participants, payment organizations, and other entities that are not UZCARD Payment System Participants but provide payment services and interact with the Operator.

3.2. Participants of the UZCARD Payment System who join the Rules, join the Standards and Regulations without any exceptions.

3.3. The Operator reserves the right to unilaterally amend and supplement the current Standards and Regulations in the manner and within the timeframes specified in the clauses 1.4 and 1.5 of the Rules.

3.4. The Standards and Regulations of the UZCARD Payment System are published on the official website of JSC “Common Republican Processing Centre” within the timeframe and in the manner specified in the Rules.

3.5. The Standards and Regulations shall be effective and apply by the Operator and Participants of the UZCARD Payment System 15 (fifteen) calendar days from the date of publication on the Website.

4. TERMS AND DEFINITIONS

4.1. For the purposes of these Rules, the terms and definitions have the meanings established by the Law of the Republic of Uzbekistan "On Payments and Payment Systems," the Law of the Republic of Uzbekistan "On Banks and Banking Activities," and other legislative acts of the Republic of Uzbekistan.

4.2. In addition to the terms defined elsewhere in these Rules, capitalized terms used in these Rules and not otherwise defined therein shall have the meanings specified below.

4.3. In these Rules, unless the context otherwise requires, words used in the singular shall include the plural and vice versa, and words used

in the masculine gender shall also include the feminine and neuter gender, and vice versa.

4.4. Except where otherwise specified in these Rules, the following terms shall have the meanings specified below:

4.4.1. **UZCARD Payment System (the PS)** is a set of relationships that facilitate payments through interaction between the Operator, Participants, and/or PSP through application of the procedures, infrastructure, and Rules. The PS has the right to use the words "payment system" and derivatives thereof in its name and/or trademark, indicating that it is engaged in activities to ensure functioning of the PS.

4.4.2. **Payment System Operator (Operator)** means JSC “Common Republican Processing Centre”, a legal entity that operates the PS in the Republic of Uzbekistan and is licensed to operate as a payment system operator.

4.4.3. **Website** – the Operator's information resource (corporate website) on the Internet at: https://uzcard.uz.

4.4.4. **RCI** (Restricted circulation information) means personal data (PD) recorded on electronic, paper, and/or other tangible media, information related to a particular BC holder or enabling identification thereof, as well as information constituting the bank secret (BS) of that BC holder.

4.4.5. **RCI processing** means actions as defined in the Laws of the Republic of Uzbekistan "On Banking Secrecy" (BS) and "On Personal Data" (PD).

4.4.6. **UZCARD Payment System Participant (Participant)** means a bank of the Republic of Uzbekistan that holds the appropriate license from the Central Bank of the Republic of Uzbekistan, carries out settlement of accounts and has entered into an agreement with the Operator for participation in the PS.

4.4.7. **UZCARD EMV** means a software package operating on the SmartVista EMV technological platform.

4.4.8. **Settlement Bank** means the Settlement Center of the Central Bank of the Republic of Uzbekistan (Interbank Universal Netting Information System – MUNIS) which provides services to Participants for settlement of accounts for transactions conducted within Participants' infrastructures using BC.

4.4.9. **Bank Card (BC)** means a payment instrument, including that in electronic form, containing the required payment details and

enabling its holder to make payments through payment infrastructures and in accordance with the Rules, as well as perform other transactions on the BC Account established by the Participant.

4.4.10. Terminal (POS, E-POS, M-POS) means a device or software that allows a BC Holder to perform payment transactions and generates slips (in paper or electronic form) for completed transactions;

4.4.11. Issue means the activity of issuing and providing BCs for use, which consists of embossing and personalizing the BC chip by assigning the CREF-3 status and displaying the BC in the Front-End System with the correctly assigned personal data of BC Holder.

4.4.12. ATM is a device designed to perform, without the participation of an authorized employee of the Acquirer, cash dispensing (acceptance) Transactions using BC, other Transactions in accordance with these Rules, and to transmit instructions to the Issuer to transfer funds from the account of a BC holder.

4.4.13. Cash dispensing/depositing point (CDP) is a bank service point equipped with a POS terminal for cash withdrawal and/or acceptance Transactions with use of BC.

4.4.14. Payment service provider (PSP) is a legal entity other than a bank that holds the appropriate license from the Central Bank of the Republic of Uzbekistan and is authorized to provide payment services.

4.4.15. Issuer is a participant that issues BCs, owns BCs issued by it, and bears obligations on its own behalf to their holders and acquirers regarding the exercise of their settlement rights using BCs.

4.4.16. SMS service is a notification service for BC holder, a type of issuer service used in UZCARD EMV.

4.4.17. Acquirer – a Participant performing Acquiring, or a PSP that provides Acquiring services to the Participant.

4.4.18. Acquiring – settlement of accounts for transactions with sellers of goods (works, services, etc.) via the Cardholder, as well as cash withdrawals directly to BC holder via a CDP or ATM;

4.4.19. MSE (merchant and service enterprise) means a legal entity and/or an individual engaged in entrepreneurial activity without forming a legal entity and/or a self-employed person selling goods (works, services) via BC based on an agreement concluded with Acquirer;

4.4.20. **BC Holder** – a client (an individual or a legal entity) or a person authorized by the client, using BC based on the client's agreement with the Issuer or bank distributing bank cards.

4.4.21. **Transaction** is an action initiated by a BC Holder,

a) resulting in the movement of funds using a BC – a financial transaction;

b) not related to the movement of funds (balance inquiry, PIN change, etc.) – a non-financial transaction.

4.4.22. **Clearing** – collecting and processing financial transactions and preparing a set of documents containing complete information on each performed financial transaction for a BC and distributing to Participants the information on interbank Transactions executed by BC holders of one Participant at the service points of another PS Participant, necessary for subsequent interbank settlements between PS Participants.

4.4.23. **Processing** – ensuring the collection and processing of information used when Participants and other PSPs execute Transactions, as well as the maintenance of issuance and/or acquiring performed by Participants.

4.4.24. **BIN (Bank Identification Number)** – a sequence of several digits of the BC number located on the front of BC, used to identify the Participant within the PS during authorization, processing, and clearing of Transactions;

4.4.25. **BIN List** – a set of structured data containing a list of BINs used to identify Participants during the authorization, routing, processing, and clearing of Transactions.

4.4.26. **PIN** means personal identification number (secret code) of a BC holder, certifying the right to manage funds held on a card account and confirming that an order was given by BC holder.

4.4.27. **Transaction Day** is the period of time between the launch of the previous and subsequent procedures for closing a transaction day.

4.4.28. **Front-End System** is a hardware and software set that ensures the processing of Transactions in real time.

4.4.29. **Back-End System** is a hardware and software that ensures management of BC Holders, BCs, MSE and Terminals, supporting the Issue and Personalization procedures, as well as settlements between Participants for interbank Transactions.

4.4.30. **BTRT** files contain applications for BC issuance and applications for registering MSEs and Terminals in UZCARD EMV.

4.4.31. **Posting File** is a file with financial and non-financial authorization records. This file contains Transactions for a specified period of time. Posting File is generated in the Front-End System at least once a day during Transaction Day, depending on the volume of Transactions.

4.4.32. **OBI file** is Transaction file for Acquirers and Issuers.

4.4.33. **IBI file** is a file uploaded to the Back-End System to increase or decrease BC Accounts generated in the ABS.

4.4.34. **Automated Banking System (ABS)** is hardware and software set designed to automate all banking operations, including accounting, finance management, payment processing, client account management and other banking processes.

4.4.35. **BC Account** is a bank account of an individual person or legal entity, which funds can be managed either through or without a BC. The UZCARD EMV system displays current information about BC Account status.

4.4.36. **OTP (One-Time Password)** is a password valid for only one transaction authentication session.

4.4.37. **Partner Payment System (PPS)** is a payment system operated by a legal entity, resident or non-resident of the Republic of Uzbekistan, that has entered into an agreement with the Operator on the interaction of payment systems.

4.4.38. **Intersystem Interaction** is the interaction between the PS and the PPS for the purpose of executing intersystem payment transactions using payment instruments issued by the PS Participants in the network of PS and/or PPS devices based on agreements signed between the Operator and PPS operators participating in the intersystem interaction.

4.4.39. **Virtual Card** is a virtual BC of the PS in electronic form, linked to a BC account, which is a payment instrument containing the mandatory BC details required to execute Transactions.

4.4.40. **QR code** is dynamic, encoded data displayed on Terminals/online cash registers/virtual cash registers, ATMs and used to facilitate payment for Goods and cash withdrawals by scanning the code using a mobile app.

4.4.41. **MCC code** is a merchant category code assigned to a Terminal, classifying the type of trading and service activity as a 4-digit number.

4.4.42. **Personalization** is a set of services performed using technological interaction between the Operator's and the Participant's hardware and software systems, aimed at assigning the BC the mandatory details required for its issuance and release for use. This process includes the procedures for reading and/or writing data to the BC's microprocessor chip and/or magnetic stripe, mechanically embossing information on the BC's front side, and more.

4.4.43. **BC Passport** is an electronic and/or paper document approved by the Operator and/or Issuer, containing regulated information about relevant BC, including its issuance parameters, purpose, technical and functional characteristics, validity period, usage procedure, restrictions and other conditions.

5. DETAILS OF THE OPERATOR

Legal address:

100011, Tashkent, Shayhontohur District, A. Qadiry Street, 78.

Call center: 71-200-28-28

Phone: 71-202-11-18

E-mail: info@uzcard.uz

Web site: https://uzcard.uz/

Bank details:

TIN 202042939

OKED 63110

Code 00974

Account No. 2020 8000 2006 0030 2001 in Operations Dept. of JSCB “Kapitalbank”

6. REQUIREMENTS TO OPERATION OF THE PS

6.1. The functions of the Operator are performed by Joint-Stock Company “Common Republican Processing Centre”, the main goal of which is to ensure the implementation of transactions in a unified transaction mode using BCs in the Operator's acquiring infrastructure, regardless of which Participant they are served by.

6.2. The Operator:

- determines the Rules, organizes and monitors compliance with them by Participants;
- ensures control over the provision of payment infrastructure services to Participants;
- notifies Participants in accordance with the procedure established by the Rules and the current legislation of the Republic of Uzbekistan;
- organizes the risk management system in the PS, including defining requirements for PS Participants to manage risks in the PS;
- assesses and manages risks in the PS;
- ensures the uninterrupted provision of payment infrastructure services to PS Participants;
- ensures a guaranteed level of uninterrupted and secure service provision;
- ensures the exchange of electronic messages between Participants and their clients,
- determines payment clearing positions on a net basis, including the proper establishment of technical calculation parameters for payment clearing positions for each Participant;
- transfers to the Settlement Bank a register of net positions compiled for each transaction day;
- sends confirmations to Participants regarding acceptance for execution, as well as transmits confirmations regarding the execution of Participants' instructions;
- conducts analysis of the needs of Participants and users of payment services to determine their satisfaction with the quality of services provided;
- ensures the functioning of the feedback mechanism for Participants and users of payment services;
- once a year, no later than the first quarter following the reporting period, publishes the results of analysis of the payment system's performance to determine the satisfaction of Participants and users of payment services on the Website, taking into account the results of the review of inquiries and requests received during the reporting year through the feedback mechanism;
- creates the risk management body for the payment system and uses at least two risk management methods;
- determines in the internal documents:

1) the operating regulations of the payment system risk management body, including its powers;
2) the criteria for ensuring the effectiveness of the payment system, which are used to assess the satisfaction of Participants' needs with the quality of services provided;
3) the procedure for pre-trial dispute resolution with Payment System Participants.

- performs other actions related to the use of information and communication technologies necessary for the functioning of the PS and stipulated by the Rules;
- informs Participants of the cases and reasons for the suspension (termination) of payment infrastructure services on the day of such suspension (termination) by sending a notice using a communication method that ensures prompt availability of information by posting on the Website, sending a notice by email, fax, or other means.

6.3. Participants must monitor the execution of collection orders presented by the Settlement Bank to Participants' bank accounts opened with the Settlement Bank. Each Participant is liable to the Operator for losses resulting from their actions or inactions, including failure to comply with the Rules or applicable law. The Settlement Bank manages all risks associated with the provision of settlement services.

6.4. The Settlement Bank:

- ensures the uninterrupted and secure provision of settlement services;
- accepts Participants' orders subject to execution;
- performs daily monitoring of settlement results;
- conducts its activities in accordance with the Rules.

6.5. The Settlement Bank shall be liable to the Participants for:

- any disruptions in the provision or failure to provide settlement services;
- timely settlement of accounts within the PS.

6.6. In case of any discrepancies, the Participant is obligated to immediately notify the Operator. The Rules are an integral part of the agreements between the Operator and the Participant "for the registration and connection of a new Participant" and "for services at the processing center."

6.7. The Operator and the Settlement Bank shall:

- when exchanging information with the Settlement Bank, use file formats in accordance with the established requirements;
- carry out control procedures for the net position register before sending it to the Settlement Bank;
- as part of the provision of services and the Clearing services, carry out control procedures for each Transaction in the Republic of Uzbekistan to ensure compliance with the requirements of the Rules;
- suspend the provision of payment clearing services to a Participant with an uncovered position and immediately notify the Operator thereof;
- resume the provision of payment clearing services to a Participant with an uncovered position from the date of receipt of notification from the Settlement Bank regarding the resumption of services to this Participant;
- stop accepting the Participant's BCs in the acquiring network of the PS, whose banking license has been revoked by the Central Bank of the Republic of Uzbekistan;
- resume the acceptance of the Participant's BCs within 12 hours of receiving the corresponding notice from the Participant. For the purpose of risk management in the PS, the Operator has the right to apply restrictive measures to Participants whose financial situation analysis indicates increased risk.
- be liable for failure to provide (or improper provision of) settlement services in accordance with the agreements concluded with Participants.

7. APPLICATION AND SCOPE OF THE RULES

7.1. Participants are obliged to comply with the applicable legislation, and all transactions conducted must comply with and be permitted by the laws of the Republic of Uzbekistan. In case of any conflict between the Rules and any provisions of applicable laws, the latter shall prevail. Participants shall adhere to the Rules only by accepting them in their entirety.

7.2. The Rules may be considered or applied only when using the PS services within the Republic of Uzbekistan. The Rules regulate the relations between the Operator and Participants within the

Republic of Uzbekistan. Relations outside the Republic of Uzbekistan are governed, among other things, by the rules of the relevant national and international payment systems, separate agreements and treaties, and international law.

7.3. The Operator shall notify Participants of all duly approved amendments and additions. These notices have the same legal force as the Rules.

7.4. Participants are obligated to:

- strictly adhere to the terms of confidentiality of the PS information;
- not disclose confidential PS information that is not subject to disclosure in accordance with the requirements of the legislation of the Republic of Uzbekistan;
- store and process confidential PS information in a manner that prevents its unauthorized disclosure;
- make every reasonable effort to protect confidential PS information and observe at least the same precautions as when handling their own confidential information;
- provide confidential PS information only to those employees who need it to perform their official duties.

7.5. The information and communications infrastructure of the PS utilizes confidential information that is the property of the PS. Each Participant is obligated to take appropriate measures to ensure that all its employees with access to the information and communications infrastructure of the PS:

- have been informed that confidential information is being used;
- do not provide access to or disclose confidential information to any third parties if it is not subject to disclosure in accordance with the requirements of the legislation of the Republic of Uzbekistan;
- do not use the information and communication infrastructure of the PS for any purposes other than those established by the Rules.

7.6. The objectives of the PS Operator are:

a) creation and storage of master system-forming keys;

b) implementation of BC Issue;

c) registration of new Participants in the system;

d) coordination and information exchange between Participants;

e) production and testing of solutions and products from card equipment designers or suppliers on commercial terms;

f) issuing a conclusion based on the test results on the feasibility of using the card equipment and product;

g) maintaining the secrecy regime and ensuring the security of the PS operation;

h) minimizing the overhead costs of PS operation;

i) ensuring the operation, maintenance, and development of PS technical means;

j) development of the card system and card projects;

i) preparation of conditions for implementation of new card projects and technologies;

j) creation, support, improvement, and management of a unified PS database;

j) marketing research;

k) conducting seminars and courses on BC and correct operation of banking equipment.

7.7. The Operator is obliged to:

a) carry out its activities in accordance with the legislation of the Republic of Uzbekistan and the Operator's Charter;

b) ensure the ability to process Transactions using the BCs issued by Participants;

c) cease the processing of Transactions via BCs upon receipt of a written decision from the Issuer to prohibit servicing the BCs issued by it (to prohibit the execution of certain Transactions);

d) cease the processing of Transactions via the Issuer's BCs in the event of the revocation of the latter's banking license or the voluntary liquidation of the Participant;

e) ensure the complete storage of encryption cryptogram;

f) provide the necessary conditions for timely exchange of information between Participants;

g) maintain a register of BC Issuers and publish it on the Website;

h) ensure timely testing of the servicing system software of BC, ATM, POS terminal, and specialized card equipment provided by Participants for the proper protection of confidential information;

i) issue a conclusion based on the testing results on the feasibility of using the card equipment and product within the payment system;

j) not disclose information about Participants' Transactions, nor information constituting a banking secret.

k) take measures to restrict access to protected and proprietary information, ensure the protection of information on its network, and protect against unauthorized access to network software and information resources.

7.8. The Operator is entitled to:

a) subject to the acceptance of a Participant into the PS, grant permission and conduct Transactions using BCs for Participants;

b) suspend Transactions on the Issuer's BCs in case of the latter's failure to fulfill the terms of agreements with the Operator, as well as agreements with other Participants, in accordance with decisions of the Operator's management or upon written request of the Settlement Bank;

c) require Participants to comply with the terms of the relationship between Participants and the Operator;

d) receive the established remuneration for services rendered;

e) receive remuneration for additional services not included in its core functions, the amount and procedure of which are determined based on agreements between the Operator and Participants;

f) require Participants to comply with agreements in force in the system, as well as with settlement discipline;

g) in case of reasonable suspicion of illegality in Transactions with BC, or upon a request from authorized state bodies of the Republic of Uzbekistan, the Operator has the right to suspend Transactions with BC for up to 72 (seventy-two) hours to conduct an appropriate investigation. The Operator has the right to request from Participants documents and information necessary to evaluate such Transactions or actions, and Participants are obligated to provide the requested materials no later than 24 (twenty-four) hours from the receipt of the request. If a Participant fails to provide the requested data, the Operator has the right to extend the suspension of Transactions with BC until all requested information is received and reviewed.

h) adopt local regulations in the form of provisions, procedures, reference manuals, and other PS documents that define the conditions necessary for functioning of the PS;

i) exercise other rights provided for in the Rules and legislation.

7.9. Legal regulation of the issues related to performance of the tasks assigned to the PS is carried out in accordance with these Rules and

other regulatory legal acts of the Republic of Uzbekistan, as well as agreements concluded by PS participants.

7.10. The Operator carries out its activities in cooperation with other Participants, payment organizations, payment service providers, and other entities, as well as with the Central Bank of the Republic of Uzbekistan within the scope of its authority.

7.11. Interaction is carried out through exchange of information messages in the established format and in accordance with ISO standards. Information exchange between the Operator and Participants uses a banking telecommunications channel. Access to that channel is granted to the Participant after the conclusion of the agreements "for registration and connection of a new Participant" and "for services at the processing center."

8. TYPES AND CRITERIA OF PARTICIPATION, SUSPENSION OF PARTICIPATION IN THE PS

8.1. Procedure of accession of a Participant

8.1.1. The Rules provide for only direct participation in the PS, with the exception of cases stipulated by current legislation and the Rules.

8.1.2. Only commercial banks of the Republic of Uzbekistan may be Participants, provided they accede to these Rules in their entirety.

8.1.3. To join the PS, a commercial bank must submit an application addressed to the Operator's executive body, with attachment of the following documents:

a) certified copy of the bank's state registration certificate;

b) certified copy of the bank's license issued by the Central Bank of the Republic of Uzbekistan to carry out banking activities;

c) certified copy of the bank's Charter;

d) copy of the bank's state registration certificate with the tax authority as a taxpayer;

e) written information signed by an authorized bank official on the structure and members of the bank's governing bodies, including information on the chairman of the board and the chief accountant of the bank, with attached documents confirming their appointment;

f) annual business plan for introduction and development of BCs;

g) bank's annual reports for the previous two years, certified by an audit firm (if operating);

h) the Participant's internal control rules, policies, and/or procedures for AML/CFT/FPWMD and sanctions compliance.

8.1.4. If the review of the set of documents is positive, the Operator shall send the bank agreements “for registration and connection of a new Participant” and “for servicing in the processing center”. The Participant's activity in Issuing and Acquiring BCs within the PS is possible only after completing the necessary set of activities to set up the Participant's basic/initial configuration in the PS and paying the mandatory fees in accordance with the concluded agreements.

8.1.5. To participate in the PS, a Participant must meet the principles of general financial stability which is assessed both upon obtaining a license and on a regular basis, but at least annually or in accordance with the requirements of the legislation of the Republic of Uzbekistan. Financial stability is understood as the Participant's financial condition, which allows it to timely fulfill contractual obligations to other Participants, including the Settlement Bank, the Operator, and the PSP that are not Participants.

8.1.6. This assessment is conducted based on verification of the following documents:

- title documents (certificate of state registration as a legal entity, certificate of tax registration, memorandum of association and/or charter, and other corporate documents);
- financial statements certified by auditors and prepared in accordance with legal requirements;
- financial statements certified by auditors and prepared in accordance with international financial reporting standards;
- information on the corporate structure and ultimate owners and beneficiaries.

8.2. Suspension of participation in the PS by the initiative of the Operator

8.2.1. Participation may be suspended by the Operator in the following cases:

a) Participant's systematic violation of the Rules, as well as applicable laws governing the conduct of Transactions using the BC;

b) failure to fulfill its obligations to other Participants, the Settlement Bank, and the Operator;

c) detection of violations by the Participant of information security requirements;

d) revocation of the Participant's banking license;

e) Participant's insolvency, i.e., Participant's inability to pay debts as they fall due, the initiation of liquidation or bankruptcy proceedings (mandatory or voluntary), the appointment of a liquidator or receiver, or suspension or revocation for any reason of a permit, license, or consent of a government agency for the Participant to conduct current activities;

f) if Participant or its shareholders are included in the sanctions lists of the UN, US, EU, or UK, as part of the management of risks threatening the functioning of the entire PS, including the risk of secondary sanctions;

g) other cases stipulated by the Rules and the current legislation.

8.2.2. If the Operator decides to suspend participation in the PS, the Operator will send the Participant a notice of suspension, specifying the violation that caused the suspension and a time limit within which the violation must be corrected.

8.2.3. The Participant's activity in the PS will be resumed provided the violation specified by the Operator in the notice is corrected.

8.2.4. If the violation is not corrected within the specified time, the Operator has the right to initiate the procedure for terminating the Participant's participation in the PS.

8.3. Suspension of participation in the PS by the initiative of the Participant

8.3.1. The Participant has the right to initiate the suspension of his participation in the PS.

If the Participant decides to suspend participation in the PS, the Participant shall send the Operator a notice of suspension of its participation in the PS.

8.3.2. The Operator shall review the notice of suspension of the Participant's participation in the PS and send the Participant a notice of suspension of its participation in the PS, indicating the date of suspension. From the date of suspension of the Participant's participation in the PS, the Operator ceases providing all services to the Participant under the PS.

8.3.3. The Participant's participation in the PS is automatically resumed upon expiration of the suspension period. The Participant has the

right to resume participation before the expiration of the suspension period, provided that the Operator is notified of the resumption of the Participant's activities in the PS.

8.4. Suspension or termination of participation in the PS in the event of suspension or revocation of the bank's license to conduct banking operations

8.4.1. In the event of suspension or revocation of a Participant's banking license, the Operator, from the date the Operator becomes aware of the occurrence of the said grounds, suspends the Participant's participation in the PS or terminates the Participant's participation and provision of all services to the Participant within the PS. The Operator will inform the Participant of the decision made.

8.4.2. The Operator will take measures to cease processing PS Transactions through the BC and on the Participant's network of devices on the day of license suspension or revocation.

In this case, the PS Operator:

a) sends a notice to the Participant containing the reason and date for suspension or termination of its participation;

b) notifies the Settlement Bank in writing of the suspension or termination of the Participant's participation in the PS.

8.5. The procedure for resolving the insolvency of PS Participants

8.5.1. The following measures are implemented in the PS to determine and ensure the sufficiency of funds to execute Participants' orders.

8.5.2. The Operator regularly assesses the financial stability of Participants and the Settlement Bank. This assessment includes an analysis of financial solvency and the ability to conduct timely and full settlements.

8.5.3. In the event of a debit payment clearing position on a net basis, payment is made by debiting funds from the Participant's bank account. The Participant is obligated to ensure sufficient funds in its bank account to meet its settlement obligations.

8.5.4. The Participant must ensure the availability of sufficient funds in its bank account opened with the Settlement Bank.

8.5.5. The Settlement Bank, no later than the end of each day of register acceptance on a net basis, conducts:

- debiting funds as the recipient from the PS participants' bank accounts in the settlement bank based on the net position register;

- crediting funds as the payer to the PS participants' bank accounts in the settlement bank based on a payment order in the amount of the net credit positions specified in the net position register.

8.5.6. If the Settlement Bank has reason to believe that the Participant will not be able to provide sufficient funds in their bank account, the Settlement Bank will promptly notify the Operator. If an uncovered Participant position arises, the Settlement Bank and the Operator will act in accordance with the agreement made between the Settlement Bank and the Participant.

8.5.7. The Operator has the right to determine payment clearing positions on a net basis based on the difference between the total amount of Participants' orders to be executed, for which the Participant is the payer of financial obligations to the Participants, and the total amount of Participants' orders for which the Participant is the recipient of funds.

9. RESPONSIBILITY FOR FAILURE TO FULFILL THE PS RULES

9.1. Participants' liability for compliance with the Rules commences upon accepting the Rules.

9.2. The Operator shall be liable to Participants for failure to fulfill or improper fulfillment of its obligations.

9.3. Participants shall be liable to their clients (BC Holders/MSE) for their actions/inactions within the PS, as well as for the actions/inactions of third parties engaged by the Participant to conduct activities within the system (including fraudulent activities), including violations of the Rules that arise through the participant's fault.

9.4. Participants are liable for failure to fulfill or improper fulfillment of the terms of placement and use of the trademark, service mark, and logo of the PS, as established by the Rules.

9.5. In case of a Participant's violation of the Rules, the Operator has the right to suspend transactions through the BC or the Participant's network of devices. The determination of the appropriate enforcement action is recognized as the unconditional and sole right of the Operator.

9.6. When applying enforcement actions, the type and frequency of the violation, the nature of the damage (including material) suffered by the Participant's clients and the Participant's ability to rectify it, as well as the consequences of the violation for the security and uninterrupted operation of the PS, shall be taken into account.

9.7. When applying enforcement action to a Participant, the Operator sends a notice to the Participant.

9.8. The Operator routinely monitors compliance with the Rules through the use of internal reporting tools and by monitoring external complaints of non-compliance with the Rules from Participants or their clients.

9.9. The Operator may establish the fact of violation of the Rules as follows:

- based on the Participant's response to the notice of an investigation into the violation, as well as other available information;
- if the Participant fails to respond to the notice of an investigation into the violation and fails to provide the requested information.

9.10. The Operator must notify the Participant that the Participant has violated or continues to violate the Rules and set exact timeframe for rectifying the violation. The notice must contain the following information:

- description of the violation;
- a notice stating that the Participant has the right to appeal the violation and/or the amount of the fine. The Operator may require the Participant to provide a plan for resolving the violation of established requirements.

9.11. Participant may submit complaints regarding violations of the Rules to the Operator. The Operator reserves the right to conduct investigations into alleged violations of the Rules.

The Participant is obligated to respond to the notice regarding the investigation of violation and, upon request, to provide the Operator with information regarding the violation of the Rules under which the investigation is being conducted. The Participant is obligated to respond to the Operator and provide any requested information within the specified timeframe by mail, courier delivery service, fax, in person, email, or other electronic means of communication. A response to the notice shall be considered valid if it is sent or transmitted to the Operator by the Participant.

10. REGISTRATION OF PARTICIPANTS, THEIR AFFILIATES AND BRANCHES. ASSIGNING BIN

10.1. All Participants shall be registered in the PS as financial institutions. Registration of a Participant and its branch network is completed through the user interface.

10.2. Participants register in the PS with the following parameters:

- Participant’s unique four-digit identifier in the PS;
- Participant's BIN.
- Participant's name;
- Participant's address;
- primary contact telephone number;
- Participant's primary contact;
- Participant's secondary contact;
- fax number;
- Email address.

The following parameters are defined for a Participant:

- Participant's branches;
- Participant's cryptographic keys;
- currencies in which the Participant's clients can open BCs. Currencies assigned to Participants also apply to all of the Participant's branches. Therefore, there is no need to assign currencies to agents separately.

10.3. BIN can only be assigned to a Participant after joining the PS.

10.4. BIN is unique and cannot be used by other Participants.

10.5. Participant may not transfer the right to use the BIN assigned to them by the Operator to other financial institutions.

11. ISSUE

11.1. Issuer in the PS performs the following functions:

11.1.1. issues BCs in accordance with the requirements determined by the Rules;

11.1.2. ensures settlement of accounts with its clients based on OBI files containing Transactions received from the Operator;

11.1.3. ensures settlement of accounts with Acquirers for Transactions conducted using the Issuer's BCs in the Acquirers' network of devices;

11.1.4. ensures the security of issue of BCs and authorization processes;

11.1.5. participates in the resolution of disputes regarding Transactions conducted using the Issuer's BCs in the Acquirers' network of devices.

11.2. Issuer is obliged to:

11.2.1. conduct the activities in accordance with the requirements of the Rules;

11.2.2. use only BINs provided to the Participant by the Operator for the Issue;

11.2.3. engage third-party organizations approved by the Operator to personalize the BCs, or, if the Issuer personalizes the BC independently, ensure that the personalization procedures and the Issuer's personalization center comply with the requirements of the Rules;

11.2.4. coordinate the BC design with the Operator;

11.2.5. comply with the security requirements of the PS and applicable legislation for the storage, movement, and destruction of BCs;

11.2.6. employ personnel directly responsible for all aspects of BC security, including:

- monitor transactions using BC to identify instances of their illegal use;
- investigate instances of illegal use of BC;
- plan personalization, coding, printing, and other procedures related to the Issuance of BCs.

11.2.7. approve the list of officials responsible for the storage and movement of BC;

11.2.8. ensure the storage of BC and PIN envelopes in a special storage facility equivalent in security to a cash vault;

11.2.9. ensure control and records of the movement of BCs and PIN envelopes, and conduct inventory procedures upon receipt/shipment of BC;

11.2.10. plan and monitor the personalization and destruction of BC using double-checking methods;

11.2.11. develop a procedure for destruction of BCs and record the destruction procedure in reports;

11.2.12. conduct an inventory of the BC storage facility at least once a year;

11.2.13. ensure the provision of virtual card details to the BC holder in a secure manner.

11.2.14. promptly notify the PS Operator of all identified cases of damage, packaging tampering, or absence/loss of BC upon receipt/shipment of a batch of BC in order to jointly determine the course of further action.

11.2.15. comply with the requirements of the international PCI DSS security standard;

11.2.16. provide the Acquirer with reimbursement for Transactions with the Issuer's BCs;

11.2.17. provide BC holders with full information on the BC service rules and provide advice on the Issuer's BC usage rules;

11.2.18. organize 24/7 support for BC holders to assist them in using the BCs.

11.2.19. conduct client identification and authentication in accordance with legal requirements and AML (Anti-Money Laundering) compliance.

11.2.20. verify the accuracy and relevance of the data provided by the BC holder and the data transmitted in the BTRT application.

11.2.21. if the BC holder's data changes, promptly update it in its system and in the Operator's system.

11.2.22. the Issuer bears responsibility for any instances of BC holders registering using false or fictitious data.

11.2.23. respond promptly to suspicious transactions related to the initial registration and activation of the BC.

11.2.24. ensure the correct display of the available balance on the BC, taking into account all authorization and settlement transactions.

11.2.25. if the funds in BC in the ABS are insufficient to successfully process OBI files, inform BC holder of the outstanding debt and take measures to resolve it in accordance with the agreement concluded with BC holder.

11.2.26. specify the terms and conditions for debt repayment in the agreement with BC holder.

11.2.27. generate and present to BC holder, prior to the conclusion of the relevant agreement and throughout its entire term, the information document containing information about BC, its validity period, functional capabilities, limitations, tariffs, and terms of use, and inform BC holder in advance of any changes.

11.3. Issuer is entitled to:

11.3.1. issue BCs with the trademarks and logos of the PS of its own design, approved by the Operator for BINs provided by the Operator to the Issuer;

11.3.2. issue, in accordance with the requirements established in the Rules, co-branded BCs, including those for BINs provided to the Issuer as part of its participation in another PS;

11.3.3. Independently determine financial relationships with clients related to the provision of BCs to client and the execution of Transactions using BCs in the PS.

11.4. Requirements to Agreement signed by the Participant with Client

11.4.1. The Participant-Client Agreement defines the relationship between the Participant and its client in connection with the provision of BC to client.

11.4.2. The Issuer-Client Agreement must include the following provisions:

- the procedure for certifying the right to manage funds in the BC account, using signatures, codes, passwords, and other means confirming that the order was given by an authorized person;
- BC must not be used for any illegal purposes, including the purchase of goods (works, services) prohibited by the laws of the Republic of Uzbekistan;
- the client's liability to the Issuer for the reimbursement of the amount of a Transaction completed using the BC;
- the procedure for direct debiting of funds from a BC;
- the procedure for changing the Acquirer's fees for cash withdrawal Transactions;
- the obligation to ensure the timely execution and accuracy of settlements for transactions carried out by MSEs using BC;
- the obligation to provide retail and service entities with the equipment and information necessary to service BCs under the terms established by the agreement made;
- ensure the timely execution and accuracy of mutual settlements with MSEs for transactions carried out using the BCs;
- requirements for the procedure and timeframes for informing the Issuer by BC holder of any unauthorized use of BC that becomes known to them, as well as in the event of loss of BC;
- the procedure for notifying BC holder about Transactions using BC, the methods and frequency of sending such notices, as well as the

amount and procedure for charging the Issuer's fee for notifying BC holder of Transactions using BC;

- the Issuer's right to transfer the rights to notify BC holder of Transactions using BC to the Operator for notifying BC holder of Transactions using BC. The amount and procedure for charging the fee for notifying BC holder of Transactions using BC shall be determined by the relevant content provider and mobile operator;
- inclusion of the conditions for obtaining the client's consent to the Processing of RCI as a part of PD in accordance with Section 30 of the Rules.

11.4.3. The Operator shall not consider claims from the Issuer's clients regarding the Issuer's unfair fulfillment of the terms of contracts with clients, but the existence of such claims may become the reason for initiating an audit of the Participant's compliance with the requirements of the Rules.

12. INFORMING AND AUTHENTICATION IN THE FRAMEWORK OF PS

12.1. The Operator provides the ability to inform BC holders about the Transactions performed and ensures the application, both by the Participant and independently, of multi-factor authentication procedures for the Transactions performed using various communication channels, including, but not limited to:

- SMS notices;
- E-mail.

12.2. Notification is provided to reduce the risk of fraudulent activity and curb the growth of fraudulent transactions involving theft of BC holder funds when sending orders to execute Transactions via communication channels. These include multi-factor authentication procedures for BC holders, as well as prompt notification of BC holders about completed payments, transfers, deposits, refunds, commission charges, and other transactions related to the use of the BC.

12.3. Notification may be either mandatory or voluntary, depending on the type of transaction, legal requirements, the PS Rules, and international payment card industry data security standards.

12.4. To ensure timely and reliable notification, the Operator reserves the right to engage third parties, including content providers and

mobile operators who provide relevant services. When sending notices, the Operator reserves the right to transfer BC holders' RCI to third parties solely as part of the provision of services to inform BC holders about Transactions, subject to compliance with legal requirements regarding the protection of RCI and imposition of similar requirements on third parties.

12.5. Mandatory notification is provided at the expense of Participants and/or the Operator.

12.6. Optional notification supported (administered) by third parties may be provided to the BC Holder for a fee, in accordance with the rates of such third parties (content providers, mobile operators).

12.7. The Operator provides optional notification free of charge by sending email notices in the manner described on the Website.

12.8. BC Holders can change notice settings, including enabling or disabling them.

12.9. The Operator is under no circumstances liable for failure to receive notices or for the late receipt of notices by BC Holders.

12.10. The relationship between BC Holder and third parties, including the scope of liability and other terms, is determined in accordance with the contractual legal relationships established between them.

12.11. BC Holder is responsible for ensuring that the contact information provided (phone number and email address) is up-to-date.

13. TYPES OF BC

13.1. Depending on the card account holder, operating procedure, and form factor, BC are divided into the following types:

a) by subjects:

- personal BC – a BC that allows for management of funds in the Card Account(s) of BC Holder (except for sole entrepreneur) identified by the Issuer prior to the issuance of Personal BC and that contains all required details;
- pre-issued BC – a BC issued in advance without inclusion of such required details as the BC Holder's surname and first name. Transactions using such a BC become possible after the Issuer has completed mandatory identification of Holder of the pre-issued BC in accordance with the procedure established by law and has entered the last name and first name electronically;

- corporate BC – a BC that allows an authorized employee of a legal entity to manage funds in the card account;
- business BC – a BC that allows a sole entrepreneur or self-employed person to manage funds in their card account;
- social BC – a BC that allows you to manage funds deposited into the card account through social and other payments;
- children BC – a BC that allows minor children to manage funds in their card account;

b) by functioning procedure:

- debit BC allows to use funds within the balance of the corresponding card account to perform payment transactions and/or receive cash (excluding corporate bank cards);
- credit BC allows to perform transactions in excess of the balance of the corresponding card account to perform payment transactions and/or receive cash (excluding corporate bank cards).

c) by holder:

- physical BC is a BC that has a physical medium in the form of a plastic card or other tangible medium (bracelet, ring, keychain, etc.), on which the mandatory BC details are applied or provided upon issuance;
- virtual BC is a BC that does not have a physical medium, the mandatory BC details of which are generated and stored exclusively in electronic form and are used to conduct Transactions;

d) by issuers:

- co-badging BC are BC operating in two or more payment systems, with their logos displayed on them;
- co-branded BC are BC issued under two or more trademarks.

13.2. A single BC may simultaneously belong to several types based on various characteristics (for example, it may be a personal, debit, and co-branded BC).

13.3. BC are issued in accordance with the Operator's requirements for the parameters of a particular BC type, as per the UZCARD GUIDEBOOK published on the Website.

13.4. Virtual BC

13.4.1. Virtual BC is a BC in electronic form, linked to a BC account, which serves as a payment instrument containing the required BC details required for making payments.

13.4.2. Virtual BC details may include:

- first name and surname of BC holder (for personal BC);
- corporate (official) name of legal entity that owns the card account and/or its payment system identification number (for corporate cards);
- The official name of BC issuer;
- BC number and expiration date.

13.4.3. In terms of functionality and application, Virtual BCs are similar to physical BC and allow for a full range of payment Transactions: incoming and outgoing transactions, and transactions related to managing Virtual BC.

13.4.4. Receipt transactions available through Virtual BC include:

- topping up the Virtual BC from your own BC linked to the Issuer's app;
- topping up the Virtual BC using the Virtual BC details by transferring funds from another BC or a virtual BC;
- topping up the Virtual BC using a QR code by transferring funds from another BC, a Virtual BC, or an e-wallet, performed by scanning the QR code generated to receive the transfer;
- accruing cashback for using services, which implies a percentage refund of the amount spent on the service;
- other transactions carried out within the PS.

13.4.5. Expense transactions available through Virtual BC include:

- payment for online services;
- payment for online purchases;
- subscriptions to services that require Virtual BC details for monthly subscription charge-off;
- payment for offline services and goods through Issuer/PSP mobile apps with contactless and QR payment functions;
- card-to-card transfers;
- Cash withdrawals from Virtual BC at ATMs that support contactless payment;
- other transactions carried out within the PS.

13.4.6. Non-financial transactions available in virtual BC, including:

- obtaining Virtual BC details;
- monitoring payments made through the Virtual BC;
- card management, i.e., designating the Virtual BC as the primary BC in the Issuer's app;

- blocking Virtual BC;
- removing a Virtual BC from the list of BC in the Issuer's mobile app;
- configuring the display of the Virtual BC in the Issuer's mobile app;
- other operations performed within the PS.

13.4.7. The functionality of incoming and outgoing payment transactions for Virtual BCs depends on the capabilities of the Issuer's mobile app.

13.4.8. To issue Virtual BCs, PS Participants must review the document "Requirements for connecting systems to the BO-Gate virtual gateway in accordance with information security requirements 1.0" posted on the www.uzcard.uz website and submit the completed "Form for organizing network access to BO-Gate" to the PS Operator.

13.5. Children BC

13.5.1. Children BC is a bank card issued in the name of a minor individual aged 6 (six) to 18 (eighteen) years in accordance with the laws of the Republic of Uzbekistan, the PS Rules, and the Issuer's internal regulations.

13.5.2. Children BC is issued and served:

13.5.2.1. For a minor under fourteen (14) years of age (minor) – with the written consent of one of the parents, adoptive parents, or guardians, by making an agreement on behalf of minor with the said persons based on their written application or by accepting an offer, subject to mandatory identification by the Issuer of minor and said person in accordance with the procedure established by the law. The Issuer is obliged to verify the existence of a first-degree kinship relationship between the minor and the parent (adoptive parent) or guardian. Liability for the issuance of a Children's BC that does not comply with the terms of this clause rests with the Issuer;

13.5.2.2. For a minor between fourteen (14) and eighteen (18) years of age – by making an agreement based on the minor's application or by accepting an offer, subject to mandatory identification by the Issuer of the minor in accordance with the procedure established by law.

13.5.3. Children's BC allow for a full range of payment transactions: incoming and outgoing transactions, and transactions related to

managing the Children's BC, subject to established restrictions and functionality provided by the Issuer.

13.5.4. Children BC may have additional conveniences, features, functions, and restrictions determined by the Issuer, which make it safe and convenient for use by minors. Additional features, functions, and restrictions may also be determined by the Operator.

13.5.5. Additional conveniences and capabilities of Children's BCs are necessarily published on the Operator's (as part of the loyalty program) and Issuer's websites.

13.5.6. Issuers may use additional conveniences and abilities of Children's BCs provided by the Operator no earlier than 15 (fifteen) calendar days from the date of publication on the Website, if such conveniences require additional settings on the Issuer's part.

13.5.7. The following are the details of Children's BC:

- first name and surname of Children BC Holder (minor);
- Children BC number and expiration date;
- other required BC details.

13.5.8. The rules for servicing Children's BCs are determined by the Issuer based on the Issuer's internal regulations and the requirements of current legislation.

13.5.9. The validity period of a Children's BC does not exceed five (5) years from the date of issue, but terminates in any event when Children BC Holder reaches eighteen (18) years of age.

13.5.10. The Issuer is responsible for ensuring termination of Children's BC upon BC Holder reaching eighteen (18) years of age.

13.5.11. The Issuer is responsible for all Transactions using Children's BC after receiving application from one of the parents (adoptive parents), guardians, or trustees of Children BC Holder regarding its loss or unauthorized use, as well as after the Children BC Holder reaches fourteen (14) years of age.

13.5.12. Transactions with Children's BC are carried out by Children BC Holder within the established limit determined by the parent (adoptive parent), guardian, or trustee via the Issuer's mobile app or branches.

13.5.13. The Issuer provides the parent (adoptive parent), guardian, or trustee of Children BC Holder with access to monitoring of Transactions in the Issuer's mobile app and/or the PSP.

13.5.14. Notifications of completed Transactions are sent by phone to both Children BC Holder and the parent (adoptive parent) or guardian when BC is enabled for notification in accordance with the PS Rules.

13.5.15. PIN for Children's BC is set by BC Holder and/or the parent (adoptive parent) or guardian in person via the mobile app, ATMs, and/or at the Issuer's branches.

13.5.16. Children BC is intended solely for use by Children BC holder for the purpose of improving financial literacy, conducting Transactions, and other actions within the functionality of Children BC, as provided for by the Rules and applicable law.

13.5.17. If a minor violates the terms of the agreement with the Issuer, or commits illegal actions, liability lies with the Issuer unless the terms of this section of the PS Rules were included in the agreement with the minor.

13.6. Premium BC

13.6.1. Premium BC is a BC with premium service and unique options provided by the Operator's loyalty program.

13.6.2. The rules for issuing and servicing Premium BC are determined by the Operator and the Issuer based on the Issuer's Rules and local regulations. Premium BC allow for a full range of payment transactions: incoming and outgoing transactions, and transactions related to managing the Premium BC, subject to established restrictions and the functionality provided by the Issuer.

13.6.3. The Operator provides additional conveniences and opportunities to Premium BC holders when using Premium BC in accordance with the Rules and offers published on the Website. The Issuer reserves the right to provide Premium BC holders with additional conveniences and opportunities within the framework of its own loyalty program, subject to the terms and conditions determined by the Issuer.

13.6.4. Privileges, including discounts, bonus accruals and access to exclusive offers and services provided by merchants to Premium BC holders, are provided in accordance with the Operator's current loyalty program based on the terms of separate agreements concluded with merchants and merchant offers addressed to Premium BC holders.

13.6.5. Additional conveniences and features are provided during a specific period established by the Operator.

13.6.6. The Operator must publish the additional conveniences and features provided by the Premium BC on the Website.

13.6.7. The Operator charges a fee for issuing Premium BCs in accordance with the Tariffs.

13.6.8. The fee for issuing Premium BCs is waived in the event of loss, expiration, or early closure of Premium BC card account.

13.6.9. Participants may use the additional conveniences and features provided by the Premium BC no earlier than fifteen (15) calendar days from the date of publication on the Website by the Operator, in cases where the use of such amenities requires additional settings on the Participant's part.

13.6.10. Access to the additional conveniences and features by Premium BC holders constitutes acceptance of the terms of the Offer "On joining the UZCARD Payment System's Loyalty Program."

13.7. Business BC

13.7.1. Business BC is a bank card designed for sole entrepreneurs (individuals engaged in entrepreneurial activity without forming a legal entity) and/or self-employed individuals. Business BC allows its Holder to perform Transactions related to production activities, trade, maintenance and performance of works, as well as to cover other expenses stipulated by the laws, including cash withdrawals.

13.7.2. Business BC may have additional conveniences, features, functions and restrictions determined by the Issuer, which make it secure and convenient to use. Additional features, functions and restrictions may also be determined by the Operator.

13.7.3. Additional conveniences and capabilities of Business BC are necessarily published on the websites of the Operator (as part of the loyalty program) and the Issuer.

13.7.4. Issuers may use additional conveniences and capabilities of Business BC provided by the Operator no earlier than 15 (fifteen) calendar days from the date of publication on the Website, if such convenience requires additional settings on the part of the Issuer.

13.7.5. Business BC service rules are determined by the Issuer based on the Issuer's internal regulatory documents and applicable legislation. Business BC allow for a full range of payment

transactions: incoming and outgoing transactions, and transactions related to the management of Business BC, subject to established restrictions and the functionality provided by the Issuer.

13.7.6. Receipt Transactions available within the Business BC include:

- receipt of funds into a Business BC card account as a result of business activities, in accordance with the Issuer's requirements, the PS Rules, and current legislation;
- topping up a Business BC card account through Participants' remote banking service (RBS) systems by means of an electronic payment order from other accounts of the Business BC Holder who opened the card account;
- other transactions not prohibited by law.

13.7.7. Expense Transactions available within the Business BC, including:

- payments related to production activities, trade, maintenance and performance of works; payments for goods within the Republic of Uzbekistan, including payments of state duties and fees, and utility bills;
- cash withdrawals from ATMs and/or cash desks of the Issuer and/or Acquirers;
- other transactions not prohibited by law, with the exception of funds transfers from one BC to another, including transfers between Business BCs.

13.7.8. Non-financial Transactions available with Business BC, including:

- adding a Business BC to the Issuer/PSP mobile app;
- obtaining Business BC details;
- managing a Business BC, i.e., designating a Business BC as the primary BC in the Issuer/PSP mobile app;
- monitoring payments made using a Business BC;
- blocking a Business BC;
- removing a Business BC from the list of Business BCs in the Participant/PSP mobile app;
- other Transactions carried out within the PS.

13.7.9. The Issuer reserves the right to impose additional restrictions and/or limits on the above-mentioned Transactions I the framework of Business BC.

13.7.10. Business BC Holder is obligated to comply with the requirements of the legislation of the Republic of Uzbekistan, the

regulatory legal acts of the Republic of Uzbekistan, and the PS Rules.

13.8. Credit BC

13.8.1. Credit BC is a bank card that allows for payment transactions and/or cash withdrawals, as well as other transactions, within the credit and/or loan provided to Credit BC Holder in the form of a revolving credit line within the credit limit established by the Issuer (hereinafter referred to as credit funds).

13.8.2. The functionality and restrictions of Credit BC are configured by the Operator based on the Credit BC Passport provided by the Issuer. Credit BC Passport is approved by the Issuer and must contain information required by the legislation of the Republic of Uzbekistan and necessary for the configuration and operation of Credit BC in the PS.

13.8.3. Credit BC may, and in cases stipulated by current legislation, must, comply with the following key characteristics:

- no fixed repayment schedule;
- grace period during which interest on term debt is not charged, provided such debt is repaid in full within the specified timeframe. The grace period may not be less than 45 (forty-five) calendar days from the date of the relevant Transaction;
- additional commission may be charged for funds transferred from Credit BC to other Credit BCs, bank accounts, and e-wallets, as well as for cash withdrawals using credit funds;
- suspension of the grace period for credit funds withdrawn in cash;
- minimum mandatory monthly payment must be made by the Credit BC Holder in the manner and within the timeframes established by the Issuer;
- other requirements established by the current legislation of the Republic of Uzbekistan.

13.8.4. Transactions under Credit BC are carried out within the limits not prohibited by the legislation of the Republic of Uzbekistan. The Issuer has the right, and in cases stipulated by law, the obligation, to impose additional restrictions and limits on Credit BC, provided they comply with the requirements of these Rules and current legislation.

13.8.5. When issuing a Credit BC, the Issuer ensures that the Credit BC Holder receives complete, accurate, and understandable information regarding the terms of its use, including key lending parameters, servicing procedures, consequences of default, and the Holder's rights and obligations. This information is communicated to the Holder prior to the conclusion of the banking services agreement under the Credit BC.

13.8.6. Credit BC Holder is obligated to comply with the requirements of the legislation of the Republic of Uzbekistan and the PS Rules.

13.9. The issue of BCs not described in this section of the Rules (including corporate BCs, co-branded BCs, and other types of BCs) is carried out by the Issuer in accordance with these PS Rules and legislative requirements, using certified software and hardware, based on BC passport approved by the Issuer.

13.10. If the Operator disagrees with the terms of the approved BC passport contradicting the requirements of current legislation and/or violate the rights and legitimate interests of the Operator, such terms shall not apply to the extent of the relevant contradiction, and BC passport shall be amended by the Issuer in this respect within 30 (thirty) calendar days from the date of receipt of the Operator's reasoned objections. The updated BC passport shall be sent to the Operator within the specified timeframe. Failure by the Issuer to comply with these requirements shall be classified as abuse.

14. ACQUIRING

14.1. General Requirements to MSE

14.1.1. Before entering into an agreement with a MSE, the Acquirer must establish that it is capable of bearing financial responsibility and is obliged to ensure that MSE complies with the Rules, as well as the current legislation of the Republic of Uzbekistan.

14.2. Acquirer functions

14.2.1. Acquirer performs the following functions in the PS:

- maintains and manages devices in its terminal infrastructure designed for executing Transactions using BCs;
- conducts Transactions determined in the Rules on the Acquirer's device network;

- participates in settlement of disputes regarding Transactions performed on devices;
- ensures the secure operation of devices on its infrastructure;
- ensures uninterrupted service for all Participants' BCs on the Acquirer's devices;
- uses devices that comply with PCI DSS security standards;
- inspects and tests all equipment and software purchased from the Operator for servicing BC holders for proper protection of confidential information;
- when servicing BC uses devices, equipment, and software successfully tested by the Operator;
- ensures the safety and security of BC Transactions on its infrastructure in accordance with the Rules and the legislation of the Republic of Uzbekistan;
- marks the PS logo on devices designed for executing Transactions using the BC and the merchant;
- provides BC holders with information on the terms of servicing the BC on its infrastructure;
- exercises control over the activities of MSE in order to monitor and prevent fraudulent activities.

14.3. Obligations for updating BIN list

14.3.1. To ensure correct routing of Transactions, stable acceptance of BC, and compliance with the Operator's information security requirements, Acquirers are required to regularly update their BIN lists.

14.3.2. BIN list must be updated at least once a week in accordance with the Operator's process instructions.

14.3.3. The Acquirer is obligated to ensure the completeness and timeliness of BIN list updates, including the implementation of an appropriate automated mechanism or routine update control process.

14.3.4. In the event of a violation stipulated by the clause 14.3 of the BIN List Updating Rules, the Operator has the right to apply enforcement measures against the Acquirer in the manner, amounts, and timeframes stipulated in Section 31 of these Rules.

14.4. Interaction of Acquirer with MSE

14.4.1. The relationship between the Acquirer and MSE is established in accordance with a separate agreement.

14.4.2. The Acquirer is responsible for ensuring that the Rules, to the extent sufficient and necessary for the conduct of servicing the BC, are communicated to and complied with by MSE. To this end, the Acquirer must conduct training for MSE employees, including on the implementation of necessary security procedures and the operation of Terminals during the transaction day. The Acquirer is obligated to guarantee to MSE timely settlements and reimbursement for Transactions conducted at MSE using the BC. The Acquirer must represent MSE interests in dispute resolution proceedings related to Transactions conducted at MSE using the BC.

14.5. Design requirements for MSEs accepting BCs

14.5.1. The Acquirer is obliged to place an image of the trademark and logo of the PS to visually inform holders of the BC about the possibility of accepting BC for servicing at the cash desks, display cases and entrance doors of the branches of the Acquirer and MSE with which the Acquirer has entered into an agreement for servicing BC, on ATMs, websites, in mobile/web applications and other devices intended for servicing BC holders.

14.6. Inspections

14.6.1. The acquirer is required to inspect the premises of MSEs with whom it plans to enter into an agreement. When entering into an agreement with a MSE selling goods via e-commerce, the Acquirer must have a detailed description of their operations.

14.7. Audits of activities of MSEs

14.7.1. To conduct audits of the activities of MSE branches/offices, the Operator may directly contact any branch/office of MSE at any time and conduct an on-site audit of the suspected violation. If MSE fails to rectify the violations identified by the Operator, the Operator has the right to establish conditions for participation or prohibit/restrict participation in the PS for the Acquirer who has entered into an agreement with MSE.

14.8. Requirements to entering into agreement with MSE

14.8.1. Acquirer is obliged to:

- enter into an agreement with each MSE;
- include in such agreement clauses obligating MSE to fulfill the obligations stipulated by the agreement and applicable law;
- inform MSE about the relevant provisions of the Rules applicable to MSE activities;

- Ensure that the provisions of the Rules are complied with by MSE;
- Ensure that the relevant provisions on payment acceptance are included in the agreement with MSE;
- Accept for further processing Transactions only from those organizations or individuals with whom it has valid agreements with MSE.

14.9. Right to terminate agreement with MSE

14.9.1. The acquirer shall have the right to limit or terminate the agreement with MSE at the request of the Operator.

14.10. Information of MSE

14.10.1. The acquirer is required to maintain a file containing full information about MSE, including any information about any investigations conducted in relation to it, for at least two years after termination of the agreement with MSE.

14.11. Right to provide information about MSE

14.11.1. The Acquirer is responsible for ensuring that the information it provides to the Operator about MSE does not contradict current legislation.

14.12. Illegal transactions

14.12.1. The agreement with MSE must specify that MSE has no right to knowingly conduct any illegal Transaction if it knew or should have known of its illegality, and the Acquirer has no right to knowingly accept such a Transaction from MSE for further processing.

14.13. Restrictions on provision of data on individual clients and completed transactions

14.13.1. The Acquirer is obliged to ensure that its staff:

- do not disclose the data received to third parties;
- treat the data received as strictly confidential;
- comply with all requirements of the current legislation of the Republic of Uzbekistan with respect to this data.

14.13.2. The Acquirer or MSE have the right to transfer data on Transactions to third parties agreed with the Operator only for the purposes of:

- loyalty program support;
- as part of fraudulent Transaction monitoring.

14.14. Prohibition on disclosure of data about clients and completed Transactions

14.14.1. MSE has no right to provide the client's RCI or details of completed Transactions to any third parties.

14.14.2. Any disclosure of such data may only be made in cases where it:

- required to conduct a MSE Transaction;
- as provided for by the legislation of the Republic of Uzbekistan.

14.15. Providing information by MSE

14.15.1. The acquirer is obliged to ensure that its MSE clearly indicate all of the following information when providing goods or services:

- the terms of the promotion (if any);
- duration of the trial period (if offered), including a clear and understandable notice that a payment will be effected on client account unless client explicitly declines payment;
- the start date for any charges and fees;
- the procedure for canceling Transactions, including clear and detailed instructions for customers on how to cancel a Transaction before the end of the trial period.

14.16. Permissible types of Transactions in the PS

14.16.1. The PS allows for operations carried out in real time at Terminals in MSE, at CDPs, at ATMs, self-service devices, administrative functions for MSE and CDP, Internet banking, and the ABS.

14.17. Methods of performing Transactions

14.17.1. The following methods of performing Transactions are provided in the PS:

a) with presentation of BC – BC holder is present during the execution of Transaction in the presence of MSE staff. In order to reduce the risk of unauthorized Transactions, Acquirers are recommended to ensure that Transactions are executed with presentation of BC in the acquiring network using the BC microprocessor. If a Transaction is executed using a magnetic stripe or with manual entry of the BC details and the Transaction is subsequently recognized as unauthorized, responsibility for the risks associated with the execution of this unauthorized Transaction rests with the Acquirer;

b) without presentation of BC

- BC holder is absent when the Transaction is performed (MSE or acquirer employee does not have physical access to BC).
- BC holder is present when the Transaction is performed (MSE or acquirer employee does not have physical access to BC).

15. OPERATOR SERVICES PRICE AND SETTLEMENT OF ACCOUNTS

15.1. The Operator's service fees exclude VAT and are determined in accordance with the Rate approved by the Operator, effective on the payment date. Rate is posted on the Website and is an integral part of the Rules. The Rates determine the price of the Operator's services, the frequency and terms of payment, as well as the interbank fees, which are not the Operator's income and are paid by the Acquirer to the Issuer. All the taxes and fees that are or may be levied on services in the future are payable in addition to Rate by the Participant, unless otherwise provided by the legislation of the Republic of Uzbekistan.

15.2. The Operator reserves the right to change the Rate unilaterally. Information about the Operator's Rates and all changes to Rates will be published on the Website within three (3) business days of their approval by the Operator.

15.3. Changes to the Rates will take effect and be applied by the Operator no earlier than 15 (fifteen) calendar days from the date of their publication on the Website or from the date the Participant receives written notice from the Operator, whichever occurs first.

15.4. Following the relevant reporting period, within three (3) business days, the Operator will generate a report on services rendered, specifically, the quantity and amount of funds debited from BC, and other necessary information on the service rendered. Based on the confirmed report, the Operator will send Participants a Certificate of Services Rendered and an electronic invoice by 10th (tenth) day of the month following the reporting month, in accordance with the current legislation of the Republic of Uzbekistan.

15.5. Participants are required to accept the Certificate of Services Rendered and the invoice within five (5) banking days from the date the Operator issues the Certificate of Services Rendered and the invoice on the my.soliq.uz online platform, provided by the State Tax Committee of the Republic of Uzbekistan, or provide a reasoned refusal to accept them.

15.6. Payment for the Operator's services rendered during the Reporting Period is made within five (5) banking days from the date the Certificate of Services Rendered and the invoice are signed.

15.7. If a Participant gives a reasoned refusal to sign the Certificate of Services Rendered and the invoice, the Parties shall, within two (2) business days, prepare a Certificate listing the necessary modifications and the deadlines for their completion. After the modifications are completed, but no later than the next business day, the Parties shall sign the Certificate of Services Rendered and the invoice. The executed documents shall serve as the basis for settlement. The Participant's refusal to sign the Certificate of Services Rendered and the invoice for reasons not previously specified in the reasoned refusal is not permitted.

15.8. If the Participant fails to comply with the terms of the clause 17.7 of these Rules, the service is considered rendered by the Operator in full and of proper quality, and the submitted Certificate of Services Rendered is accepted by the Participant as amended by the Operator, and is subject to payment in accordance with the terms of these Rules.

16. INTERSYSTEM INTERACTION OF PS AND PPS

16.1. The Operator is actively developing its Payment System to improve efficiency, ensure uninterrupted operation, reduce costs, and increase the availability of payment services to a wider range of payers, including by expanding the payment space and establishing partnerships with PPS.

16.2. The main integration vector for the intersystem interaction between the PS and PPS is the expansion of acquiring networks.

Intersystem payment transactions carried out in the ATM network of the payment infrastructure of PPS are carried out in compliance with all information security requirements, requirements for the uninterrupted operation of PPS, and also taking into account all the requirements of the risk management system, including the financial risks specified in the Rules of both PS.

16.3. In accordance with legal requirements, payment system operators are obligated to ensure the confidentiality of information, including personal data, and the security of data transmission. They must comply with security and integrity requirements, as well as the means and methods for ensuring these, along with the obligation to store such information for five (5) years from the date of registration of the information in the payment system.

16.4. Interaction between the PS and other partner payment systems (PPS) is carried out on the basis of agreements concluded between the Operator and the operator of the relevant PPS.

16.5. The Operator has the right to enter into agreements with PPS operators on the interaction of payment systems for the purpose of executing intersystem transactions – Transactions using the Participant's BC in the PPS Participants' Network of Devices or using the PPS's BC in the Participants' Network of Devices. A Transaction is also considered intersystem if the Participant and PPS participant are the same person.

16.6. Payment clearing and settlements between the PS and PPSs are carried out in accordance with the procedure stipulated by the agreement concluded between the Operator and the operator of the relevant PPS, including:

16.6.1. The Operator performs payment clearing and generates settlement data for Participants for all intersystem Transactions processed within the framework of intersystem interaction;

16.6.2. payment clearing and settlement services for Participants for intersystem Transactions are provided by the PS in accordance with the Rules, Tariffs, and Standards;

16.6.3. payment clearing and settlement services for PPS participants for intersystem transactions are provided by PPS in accordance with the rules, tariffs, and standards of PPS.

16.7. Services provided PPS' BC by Participants to the Participants' devices network, as well as by BC of the Participants within PPS Participants' devices network (intersystem transactions), are carried out in the manner established by the terms of the concluded agreements, unless otherwise provided by the rules, rates and standards of the PS and/or devices network.

16.8. The set of devices (ATMs, electronic terminals, self-service terminals, and other devices) through which intersystem Transactions can be performed are determined by the terms of the agreements on interaction between the payment systems.

17. PROCEDURE OF IMPLEMENTING OPERATIONS IN PS

17.1. When a transaction is performed in the PS, the request is processed in the PS authorization module. The PS provides for online authorization, where authorization is requested from the PS:

- checks are performed on BC and account in accordance with the BC's BIN authorization scheme;
- BC issue limits are verified;
- the terminal device's acquiring limits are verified;
- if all Transactions are successfully completed, a record of the payment's success is made in the database and transmitted to Participants as OBI files during the Transaction Day.

After processing a request, the PS generates and sends either a confirmation or a refusal to execute the Transaction to the terminal device.

Therefore, a Transaction through the BC within the PS is carried out by simultaneously reducing the payer's electronic money balance in its servicing Participant and increasing the recipient's electronic money balance in its servicing Participant. The Participant's payment clearing position is calculated by including the equivalent of the electronic money transfer amount in the Participants' payment clearing positions, determined on a net basis. Settlements for Transactions are made in the general manner in accordance with the Rules.

When executing Transactions, authorization, identification, and authentication may be performed in compliance with the requirements of the legislation of the Republic of Uzbekistan and the Rules.

18. ONLINE INTERFACE WITH ABS OF PARTICIPANTS, INTERFACES BETWEEN PS AND ABS OF PARTICIPANTS

18.1. In the PS, Participant interaction occurs via an online interface between the Participant's ABS and the Operator's front-end system.

18.2. Participants' ABS systems must send authorization requests to the Operator's front-end system in real time whenever a Transaction (debit, credit, block, unblock, etc.) is required. The request format must be implemented according to the specifications provided by the Operator.

19. STATEMENT UPLOADING FORMAT

19.1. The Participant's ABS must send issuing and acquiring statements to the Operator's Back End System for registration of issue and acquiring entities in the PS, as well as changes to their data. Statements are uploaded in the BTRT file format. Statement files can be uploaded to the Operator's Back Office System multiple times during a Transaction Day, depending on the Participant's needs.

19.2. The Operator's Back Office System generates OAR files (BTRT statement processing results) for Participants. The fields in the OAR files must correspond to the values generated in the Operator's Back Office System.

19.3. Uploading changes to BC account balances:

19.3.1. The Participant's ABS must upload IBI files containing changes in the Participant's BC balances to the Operator's back-end system.

19.3.2. The Operator's back-end system uploads OBI files containing information on Transactions executed through the Participant's BC and devices to the Participant's ABS.

19.4. Uploading payment register:

19.4.1. The Operator's back-end system uploads a file-registry of Operations performed on the Participant's devices to the Participant's ABS.

19.5. Uploading BC status changes

19.5.1. The Operator's back-end system uploads to the Participant's ABS a file with data on the Participant's BC, the status of which has been changed in the PS.

20. COMMISSION

20.1. Participants have the right to charge a commission directly from BC holder for the following types of Transactions:

a) "Cash withdrawal from ATMs";

b) "Cash withdrawal in national currency and foreign currency in CDPs";

c) "BC-to-BC Transfer";

d) Transactions stipulated by the current legislation of the Republic of Uzbekistan.

20.2. If the Participant charges a commission, the Participant is obligated to inform BC holder of the amount of commission charged to BC holder for the Transaction prior to the Transaction. This must be

done in an agreement concluded with BC holder, or in an offer for the issuance and servicing of BC posted on the Participant's official website in other procedure, confirming BC holder's consent and knowledge of the procedure and amount of the commission charged.

20.3. Acquirer that applies or plans to apply ATM access commission for domestic Transactions, cross-border Transactions, or both must comply with all of the following requirements:

a) At the time of each Transaction for which an ATM access fee is charged, the Acquirer of that Transaction is obligated to transmit/display the amount of the fee in a separate field, separate from the amount of cash dispensed under that Transaction;

b) Acquirer may not charge an ATM access fee in an amount exceeding the fee charged by it for Transactions of other payment networks (systems), including international ones, accepted at that ATM.

21. MSE CANCEL AND REFUND TRANSACTIONS

21.1. The "Cancel" transaction is performed at MSE when a BC holder returns a full or partial refund of goods (or refuses work or services) purchased at that MSE and paid for using the BC/BC details. This "Cancel" transaction is possible before the close of business.

21.2. The "Return" transaction is performed at MSE when a BC holder returns a full or partial refund of goods (or refuses works or services) purchased at that MSE and paid for using the BC/BC details. This "Refund (Partial Refund)" transaction is possible after the close of business for 90 (ninety) calendar days from the date of purchase.

21.3. After the expiration of the above periods, a full or partial refund to the BC holder is only provided by MSE through the servicing bank in accordance with the established procedure.

21.4. The "Cancel" or "Refund" transaction, at MSE discretion, must be performed using the BC used to pay for the returned goods (work, services) or part thereof at MSE. When performing a "Cancel" transaction, the full amount of the previously completed transaction is refunded to the BC. When performing a "Refund" transaction, either the full or partial amount of the previously completed payment for the goods (work, services) can be refunded to the BC.

21.5. After a "Cancel" or "Refund" transaction, the BC balance in the Front-End System is increased by the amount of the "Cancel" or "Refund" transaction.

22. PROCESSING OF AUTHORIZED TRANSACTIONS IN PS

22.1. During Transaction Day, the Operator's system records authorizations for financial Transactions. These authorizations are uploaded to a posting file, which is then sent to the Operator's back-end system for further processing.

22.2. The Operator's back-end system downloads and processes the received posting file, which then creates a register of all successfully processed financial Transactions.

22.3. After processing the data, the Operator's back-office system creates the following files for transmission to external systems:

- for ABS of each Participant:

a) Registry of Operations – OBI files for all operations performed through Participants' devices and through the BC.

- for Settlement Bank:

a) registers of interbank transactions containing data on transactions carried out between different Participants.

- for PPS:

a) clearing files.

23. GENERATING AND SENDING NET POSITIONS TO SETTLEMENT BANK

23.1. The Operator generates and sends to the Settlement Bank a register of net positions for settlements based on the results of payment clearing based on the PS Regulations “Uploading files with transactions in the UZCARD payment system” (Appendix No. 1).

24. INTER-BANK SETTLEMENT PROCESS. ORGANIZATION OF INTERACTION OF SETTLEMENT BANK WITH PS

24.1. The Settlement Bank generates instructions based on the net position register received from the PS on the day the net position register is received.

24.2. By joining to the Rules, the Participant undertakes to grant the Settlement Bank the right to debit funds from the Participant's

account without further instruction from the Participant, based on instructions generated by the PS based on the net position register.

24.3. Interaction between the Settlement Bank and the PS is automatic and consists of the following sequential steps:

a) The Operator sends files to the Settlement Bank, formatted in accordance with established requirements;

b) The Settlement Bank, having received the files from the Operator, processes them;

c) archived files undergo a file extraction procedure;

d) database of Participants' claims and obligations is created based on the contents of the extracted files.

25. TIME AND PROCEDURE OF SENDING FILES FROM PS

25.1. The Operator generates and sends files in the manner and within the timeframes established in the PS Regulations for "Uploading Files with Transactions in the UZCARD Payment System" (Appendix No. 1).

25.2. Depending on the volume of Transactions received by the PS, deviations from the File Upload Regulations are permitted.

26. REQUIREMENTS TO SETTLEMENT BANK

26.1. To implement interaction, the Settlement Bank must meet the following requirements:

a) connection of the Settlement Bank to the banking telecommunications network;

b) availability of means and methods for receiving and processing files sent by the Operator;

c) availability of appropriate accounts for each Participant to record claims and liabilities.

27. TRANSACTION DAY. CLOSE OF TRANSACTION DAY

27.1. Transaction Day in the PS is set from 4:00 PM (inclusive) of the current day to 4:00 PM (not inclusive) of the following day.

27.2. The closing of the Transaction Day in the Operator's Back-End System is divided into two phases. Each phase consists of processes responsible for specific system functions.

27.3. The first phase of the Transaction Day closing may include processes that can be launched multiple times during a single Transaction Day. The number of times the first phase of the Transaction Day closing can be launched is unlimited.

27.4. The second phase of the Transaction Day Closing includes processes that must be launched no more than once per Transaction Day. Accordingly, the second phase of the Transaction Day closing can be launched no more than once per Transaction Day. The procedure for uploading files to the Participants' ABS during the Transaction Day is provided in Appendix No. 1 to the Rules.

28. CLOSING AND OPENING OF FISCAL YEAR

28.1. The closing and opening of the corresponding fiscal year in the PS is carried out in accordance with the decision of the technical director of the Operator.

29. COLLECTION OF INFORMATION ABOUT FRAUDULENCE WITH BC

29.1. To prevent fraudulent transactions with BC/BC details or data compromise, each Participant is obligated to report all fraudulent transactions with BC to the PS Operator.

29.2. The PS Operator has the right to initiate a compliance review of Participants involved in identified cases of fraudulent transactions with BC/BC details.

30. ENSURING SECURITY AND INFORMATION PROTECTION

30.1. Participants are obligated to obtain consent of BC holders for Processing of RCI (PD), including automated processing, to the extent and in the manner established by the laws of the Republic of Uzbekistan, including consent to transfer of RCI (PD) to the Operator and third-party tokenization service providers for the purposes of operating the UZCARD PS and providing related services, as well as automated Processing of RCI (PD).

30.2. The consent of a BC holder for Processing of RCI (PD) must include consent to Processing of RCI (PD) by the Operator and Participants for historical, statistical, sociological, and scientific research. When

using RCI (PD) for the above purposes, the Operator and Participant ensure their anonymization.

30.3. Participants are obligated to ensure that the consent of a BC holder includes provisions regarding the possibility of transferring RCI (PD) to the Operator and the Processing of RCI (PD) by the Operator for the following legal purposes:

30.3.1. Identification, authentication and verification of BC holder:

- identification, authentication, and verification of personality of BC holder;
- carrying out identification, authentication, and verification procedures as required by the law;
- confirming the legality of using the PS services;
- preventing fraudulent activities and other illegal transactions.

30.3.2. Tokenization and processing of Transactions using tokens:

- tokenization of BC details and other BC holder data;
- transfer of personal data and payment details to third-party tokenization service providers for generation, storage, management and use of payment tokens;
- processing of Transactions using tokens, including their authorization, routing, clearing, and settlements;
- ensuring the security of payment Transactions, including mitigating the risk of payment data compromise;
- ensuring functioning of PS services based on the use of tokens, including interactions with foreign payment systems, banks, and other payment infrastructure participants.

30.3.3. Provision of services to Participants, PSP for the provision of payment services to BC holder and ensuring their correct functioning:

- creating and maintaining of BC holder account;
- conducting, executing, recording and processing payment Transactions;
- ensuring the exchange of information and Transactions between Participants and PSP;
- conducting transactions stipulated by the laws and the PS Rules.
- displaying payment history;
- performing BC holder scoring by the Participant;
- ensuring the technical capability to process transactions in the framework of PS.

30.3.4. Ensuring the security of the PS and protecting the rights of BC holders:

- preventing unauthorized actions, cyberattacks and fraud;
- monitoring, identifying and investigating suspicious Transactions;
- risk management and ensuring information security in accordance with legislation and the PS's internal procedures.

30.3.5. Compliance with the requirements of the laws of the Republic of Uzbekistan

- fulfillment of obligations stipulated by the law, including the requirements of government authorities;
- fulfillment of obligations under AML/CFT/FPWMD legislation;
- maintaining accounting and tax records to the extent required by the law.

30.3.6. Communication with BC holder

- sending notifications about Transactions, changes, and service updates;
- processing requests, inquiries and complaints from BC holders;
- providing reference and other information.

30.3.7. Improving the quality of services and development of PS functions

- analysis of the use of PS services;
- conducting statistical, analytical, and other research aimed at developing and improving PS services;
- testing and improving the user experience.

30.3.8. Carrying out activities in accordance with Laws, Rules and annexes thereto, Standards, Regulations:

- ensuring uninterrupted, efficient and accessible provision of money transfer services;
- organizational and legal measures for adherence to the Rules, as well as providing support on organizational and operational issues to Participants, PSPs, and counterparties;
- processing letters, requests, and other correspondence from Participants, other persons, and BC Holders;
- interacting with Participants, other persons, and BC Holders in the implementation of the Rules and Standards;
- resolving disputes, non-standard, and emergency situations, including cases of system and technological failures, resolving disputes between Participants and other persons, including

disputes related to the execution (refusal to execute) of Transactions, including situations of unauthorized use of the BC arising both between Participants and between the parties involved in the Transaction;

- verification and comparison of personal data to confirm its accuracy and verification by third parties in cases stipulated by the legislation of the Republic of Uzbekistan;
- preventing unauthorized, illegal Transactions and other abuses, as well as investigating such cases;
- providing services to Participants to securely authenticate BC holders and make decisions when executing Transactions in the Internet;
- providing mobile payment service;
- providing services to Participants to identify risks associated with transferring funds without the consent of BC holders and other risks during MSE inspection.

30.4. Cross-border transfer of RCI (PD) of BC holders is carried out by the Operator and Participants in cases where Transactions are conducted outside the Republic of Uzbekistan, as well as when interacting with foreign payment systems, foreign banks, and other organizations involved in facilitating such transactions.

30.5. Transfer of RCI (PD) outwards the Republic of Uzbekistan is carried out:

- to the extent necessary for authorization, execution, and settlement of transactions;
- in accordance with the requirements of the legislation of the Republic of Uzbekistan, including requirements for the cross-border transfer of personal data;
- exclusively to organizations, foreign banks, and payment systems participating in the execution of the BC holder Transactions and having contractual relations with the Operator.

30.6. Participants are obligated to inform BC holders of the possibility of cross-border transfer of their personal data and ensure that appropriate consent is obtained in accordance with the legislation of the Republic of Uzbekistan.

30.7. Security and information protection in the PS encompasses the entire technological cycle of the system's operation, including:

a) Operator;

b) Settlement Bank;

c) Issuers and Acquirers;

d) BC holders;

e) MSE;

e) communication systems and facilities.

30.8. Participants ensure the use of BC having internal security features that prevent counterfeiting and meet the security requirements of the underlying technology. Participants ensure the use of an encryption algorithm by the specific technological platform of the system.

30.9. Participants are required to take measures to ensure data protection during card issuance to prevent its compromise.

30.10. All Participants must ensure that sensitive information is not accessible in clear text and cannot be accessed by the computer's RAM. The key system must be managed in accordance with all information system security requirements.

30.11. BC are equipped with built-in security features that ensure the system is hack-resistant. PIN code is used when working with a BC.

30.12. To enhance the security of BC holder data and facilitate the widespread implementation of uniform measures to protect BC holder data, the infrastructure of the Acquirer's mobile/web application must comply with the security requirements for the use of services implemented in accordance with the PS Standard "Information Security Requirements in the UZCARD Payment System" (Appendix No. 2 to the Rules).

30.13. Activation of terminal in the PS is to be done from the day of initial registration of the terminal by the Acquirer in MSE by receiving a configuration file for the terminal:

a) POS models operating under the ISO8583 protocol, compliant with the current PCI DSS standard, and supporting EMV-compliant POS terminals;

b) a terminal service agreement with a service provider authorized by the manufacturer;

c) a letter of guarantee from the manufacturer regarding support for the terminal model range;

d) POS terminals have been tested for compliance with PCI DSS security standards at authorized service centers for 5 years from the date of initial registration with MSE;

e) an information letter from the Operator confirming certification and testing;

f) installation of software that complies with the requirements of the POS.

31. PROCEDURE OF IDENTIFYING ABUSE AND APPLYING ENFORCEMENT ACTIONS

31.1. Abuse by Participants includes any actions and/or inactions aimed at disrupting the normal operation of the PS, obtaining unjustified advantages, and/or causing damage to other Participants and/or the Operator, including violating the rights and legitimate interests of the Operator and Participants.

31.1.1. Abuse is defined as actions and/or inactions that include, but are not limited to, actions aimed at non-compliance with or circumvention of Transaction processing procedures (incorrect indication of MSE's MCC codes, untimely updating of BIN lists, violation of authorization, clearing, and settlement rules, manipulation of Transaction parameters, changes to Transaction types in terminals, inconsistency between Transaction service types and actual data, as well as any other actions that result in distortion of transaction activity data, financial damage, or violation of regulatory requirements).

31.1.2. To identify abuse, the Operator reserves the right to monitor and verify potential cases.

31.2. Mechanisms for monitoring and identifying abuses

31.2.1. Monitoring of Transactions:

- Regular audits of ongoing Transactions and terminal settings by a specialized division of the Operator;
- audits include compliance analysis and identification of discrepancies in Operation types, MCC codes, service type validity, and other parameters, as well as the identification of potential abuses, followed by data adjustments and recalculations.

31.2.2. Audit of abuse cases:

- conducting scheduled and unscheduled audits of Participants.

31.2.3. Processing appeals and prescriptions:

- Receiving and reviewing appeals from Participants, TSPs, and other PPUs;

- Reviewing and implementing prescriptions from the Central Bank of the Republic of Uzbekistan.

31.3. Monitoring procedure

31.3.1. Monitoring of Participants' Transactions is carried out on the basis of a local regulatory act of the Operator approved in the established manner.

31.4. Audit procedure

31.4.1. Preparatory stage:

31.4.1.1. Definition of the audit purpose:

- The purpose of the audit is to identify and analyze cases of abuse, assess the effectiveness of existing procedures for monitoring, controlling and preventing abuse, as well as their compliance with the requirements of the PS and internal regulations.

31.4.1.2. Preparation of audit program:

- determining the scope of the audit, including a list of audited Operations, processes, and time periods;
- formation of the audit team;
- preparing documents (checklists, evaluation criteria, regulations).

31.4.1.3. Notice to Participant about audit:

- sending a notice of audit, including the objectives, deadlines, and list of required documents and data.

31.4.1.4. Collection of information:

- request for documents related to procedures for identifying and preventing abuse (security policies, monitoring regulations, reports on suspicious transactions, information on the actual purpose of the terminals and their compliance with the declared types of activities, etc.).

31.4.2. Stages of audit:

31.4.2.1. Analysis of existence of respective procedures:

- verification of the presence and implementation of local regulations to prevent abuse by Participants.

31.4.2.2. Check of randomly selected terminals and Transactions on them:

- analyzing Transactions for compliance with established limits, standards, and rules;
- checking the correctness of service Transaction types, terminal parameters, and other criteria reflecting the actual purpose of the terminals;

- checking the response to identified suspicious Transactions.

31.4.2.3. Assessment of information systems:

- analysis of the E-POS terminal registration process, including the procedure for integrating them into payment products, setting up service types and Transaction parameters;
- verification of system compliance with data security requirements.

31.4.2.4. Interview with Participant's staff:

- conducting interviews with responsible persons to determine the level of awareness and compliance with procedures.

31.4.3. Analysis and finding stage

31.4.3.1. Generalization of data:

- comparison of actual results with the requirements of regulatory documents and Payment System standards.
- identification of violations and deviations:
- classification of violations (critical, significant, minor);
- determining the causes of identified cases of abuse (weaknesses in processes, deficiencies in staff training, technical vulnerabilities).

31.4.3.2. Development of recommendations:

- preparing recommendations to address identified deficiencies;
- developing proposals to improve control procedures, prevent and address abuse.

31.4.4. Final stage

31.4.4.1. Preparing the report including:

- brief description of the audit;
- list of identified violations;
- recommendations for correcting deficiencies;
- timeframe for implementing the recommendations/requirements.

31.4.4.2. Control of fulfillment of recommendations/requirements:

- establishing deadlines for correcting violations;
- organizing follow-up monitoring or additional audit (if necessary).

31.4.5. In case of confirmation of abuse, all documentary costs for conducting the inspection will be reimbursed by the Participant who committed the abuse.

31.5. Actions applied in case of confirmation of abuse

31.5.1. In case of confirmation of the fact of abuse by the Operator, the following measures may be applied to the Participant:

- a written warning regarding the need to address identified deficiencies and implement recommendations during the implementation of monitoring and verification mechanisms;
- decision to impose penalties in accordance with this section of the Rules;
- decision to temporarily or completely restrict certain functions of the Participant in the PS.

31.6. Penalties

31.6.1. Penalties are imposed by the Operator if Participants violate the established rules, deadlines, or obligations stipulated by these Rules.

31.6.2. The purpose of imposing penalties is to ensure the proper fulfillment of obligations by all Participants and to maintain the stability and reliability of the payment system.

31.6.3. The amount of penalties and payment deadlines are determined by these Rules.

31.6.4. The basis for imposing penalties is a decision made by the Operator.

31.6.5. The Operator's decision to impose penalties shall specify:

- name of the Operator;
- number, date, and place of decision;
- name of the Participant who committed the abuse;
- subject of the abuse;
- brief summary of the content of the decision;
- the basis for the decision, the evidence on which the decision is based;
- conclusions based on the investigation of the abuse.

31.7. Amounts and procedure of payment of penalties

31.7.1. Fines are set at a fixed amount, depending on the type of abuse.

31.7.2. Types of abuse and fine amounts:

31.7.2.1. Incorrect classification of trading operations (MCC codes) or untimely updating of BIN lists:

- providing incorrect MSE category codes to reduce fees or circumvent restrictions, as well as failing to update BIN lists in a timely manner;

- financial penalty in the amount of, under the following conditions:

  a) for the first recorded incident, 35 reference calculation values (RCV) on the date of decision;

  b) for the second recorded incident, 70 RCVs on the date of decision;

  c) for the third recorded incident, 100 RCVs on the date of decision;

  d) for the fourth recorded incident, 1,000 RCVs on the date of decision.

  for each subsequent recorded incident after the fourth instance, a financial penalty of 1,000 RCVs on the date of decision will be applied.
- incorrect registration of devices, resulting in the inability to process Operations.

31.7.2.2. Violation of the rules of Transactions authorization and processing:

- conducting Transactions without proper authorization or in violation of established procedures;
- financial penalty of 35 to 50 RCVs on the date of the decision.

31.7.2.3. Using E-POS terminals for other purposes or to circumvent established limits and rules (unauthorized changes to the parameters of Operations, including the type of service Operations, the category of Operations (Trans Type), the payment processing method):

- financial penalty in the amount of 10% of the total amount of all Transactions carried out for other than their intended purpose or for the purpose of circumventing established limits and rules for the last twelve-month period preceding the date of the decision.

31.7.2.4. Any other violations not specified in the above clauses, including actions (or inactions) by the Participant that violate the requirements of these Rules, will result in a financial penalty in the amount of 10 (ten) reference calculation values (RCV).

31.7.2.5. Penalties are payable by the Participant within 10 (ten) business days of the Participant's receipt of the decision to impose the penalty.

31.7.2.6. In the event of an overpayment by the Participant due to incorrectly specifying the Transaction parameters in E-POS terminals, the overpayment is non-refundable unless the overpayment amount for the reporting month exceeds 500 RCVs.

31.7.3. Payment of penalties does not relieve the Participant of the obligation to properly fulfill its obligations to other Participants and/or the Operator.

31.8. Temporary restriction of certain functions of Participant in the PS.

31.8.1. In case of a repeated violation by the Participant of a similar abuse for which a decision was previously made to impose penalties, and/or failure to correct such abuse within 1 (one) month from the date of the relevant decision, as well as failure to provide the Operator with written notice of the correction of the identified abuse and failure to pay the imposed penalties, the Operator has the right to apply measures to the Participant to temporarily restrict the functionality of the PS.

31.9. The procedure for introducing and implementing temporary restrictions on certain functions of a Participant in the PS.

31.9.1. Restrictions are imposed by the Operator based on a decision to temporarily limit certain functionality of the Participant in the PS.

31.9.2. The Operator imposes restrictions at its sole discretion, including with respect to services or functions unrelated to identified cases of abuse.

31.9.3. The restrictions remain in effect until the Participant eliminates the identified abuses, pays the imposed penalties, and confirms the fact of their elimination based on a written notice sent by the Participant to the Operator.

31.10. Appealing against decisions

31.10.1. Participant has the right to appeal against the Operator's decision within the time and according to the procedure established in this section.

31.10.2. Procedure for appealing against the Operator's decision:

31.10.2.1. The time for appealing the Operator's decision is 5 (five) business days from the date the Participant receives it.

31.10.2.2. When appealing against the Operator's decision, the Participant must provide:

- a brief description of the disagreement;
- arguments and evidence supporting the position;
- contact information for feedback.

31.10.2.3. Objection is sent via the official communication channel.

31.10.3. The Operator is obligated to review submitted objections within 5 (five) business days from the date of their receipt.

31.10.4. The Operator has the right, if necessary:

31.10.4.1. request additional documents or information from the Participant;

31.10.4.2. extend the period for reviewing the objection, which may not exceed 7 (seven) business days from the expiration date of the initial period.

31.10.5. After the review, the Operator is entitled to:

31.10.5.1. leave the decision unchanged and dismiss the objection;

31.10.5.2. change or revoke the decision;

31.10.5.3. revoke the decision and conduct a retrial.

31.10.6. A reasoned decision shall be sent to the Participant no later than 5 (five) working days from the date of its issuance.

32. SETTLEMENT OF DISPUTES BETWEEN THE PARTICIPANTS OF PS

32.1. Documents confirming the Operations carried out in the network of devices are:

a) ATM printer tape (either hard copy or electronic);

b) a copy of the POS terminal receipt;

c) a statement of funds flow in the Participants' BC accounts;

d) all electronic files and electronic authorization log files (registers) maintained by the payment system, as well as printouts of such files and logs, are recognized as adequate evidence in resolving disputes and mutual claims;

e) documents regulating the terms and conditions of work performed by Participants – contracts, agreements made between BC holders/MSE, work acceptance certificates, and other documents confirming the completion of such work;

f) all documents and information exchanged between BC holders/MSE, prepared in electronic form.

32.2. Participants are obliged to inform the Operator about events that have given rise to controversial, non-standard and emergency situations, including the cases of system and operational failures, as well as other events related to the information security of the PS infrastructure, no later than 8 (eight) business hours from the moment the relevant fact is identified, and also to provide information on the results of investigation of the said events, an

analysis of their causes and consequences, as well as on the corrective actions taken.

32.3. Participants are also obligated to ensure continuous, regular, systematic and documented monitoring and analysis of BC Transactions, as well as any operational incidents affecting or potentially affecting the security of BC Transactions and BC Holder data within one calendar month (hereinafter referred to as the "reporting period"). Monitoring within each reporting period must include, but is not limited to:

- unauthorized, erroneous and otherwise incorrect Transactions;
- suspicious Transactions, anomalies, and deviations from the normal activity profile.

32.4. At the end of each reporting period, Participants are required, no later than 5 (five) calendar days from the date of its end, to send the Operator a report on all identified incidents specified in the clause 32.3 of the Rules, which must include:

- detailed description of the incidents;
- investigation results and root cause analysis;
- assessment of actual and potential consequences;
- a list of implemented and planned corrective and preventive measures, as well as their implementation deadlines and the persons responsible.

32.5. Upon receipt of a notice of an event and/or following the results of the reporting period of incidents that have occurred, the Operator shall immediately initiate procedures for responding to and managing the relevant event/incident together with the Participant, including:

- determines the level of criticality and response priority;
- approves and implements a plan for response, recovery, and mitigation of the consequences of an event/incident;
- takes measures aimed at preventing the recurrence of a similar event/incident, in strict compliance with the requirements of the legislation of the Republic of Uzbekistan, ISO/IEC 27001, ISO/IEC 27002, PCI DSS, and the internal regulatory documents of the PS.

32.6. Failure to provide the specified information, provision of incomplete or inaccurate information, lack of proper monitoring, failure to document its implementation, as well as failure to promptly identify events and/or incidents, are considered improper performance by

the Participant of the monitoring obligations stipulated by these Rules.

32.7. All disputes and disagreements arising in connection with the use of the PS are resolved primarily through pre-trial resolution. The Operator and Participants are obligated to establish and maintain a mechanism for resolving disputes at an early stage in order to minimize litigation and preserve business relations between the parties.

32.8. Pre-trial dispute resolution is mandatory, and only after all avenues for amicable resolution have been exhausted may the parties appeal to court.

32.9. If agreement is not reached, a dispute involving the Operator shall be referred to the Tashkent Inter-district Economic Court for examination in accordance with the legislation of the Republic of Uzbekistan.

32.10. The results of examination of disputes between Participants by judicial bodies shall be communicated by the Participant to the Operator in writing within 30 (thirty) calendar days from the date of the issuance of the judicial decision by the relevant authority.

33. REQUIREMENTS TO PARTICIPANTS' COMPLIANCE WITH THE AML/CFT/FPWMD LAWS

33.1. Participants are required to comply with all applicable laws and regulations of the Republic of Uzbekistan in the field of combating the legalization (money laundering) of proceeds from crime (AML), combating the financing of terrorism (CFT) and the financing of the proliferation of weapons of mass destruction (FPWMD) and compliance with sanctions regimes, including:

- sanctions regimes established by the United Nations (UN);
- sanctions regimes established by the Office of Foreign Assets Control of the U.S. Department of the Treasury (OFAC);
- EU Restrictive Measures;
- UK Sanctions Regime;
- other mandatory international and national requirements.

33.2. If UN, US, EU, or UK sanctions are imposed on a Participant (including indirect sanctions based on ownership or control), the Participant is required to notify the Operator by sending an email to info@uzcard.uz no later than one (1) business day from the date the Participant becomes aware of the sanction.

33.3. Participants are required to provide the Operator with information regarding AML/CFT/ FPWMD compliance within five (5) business days of receipt, including:

- results of inspections by regulatory authorities (reports and orders on AML/CFT/ FPWMD issues);
- reports and opinions from other supervisory and audit organizations, if they contain an assessment of the effectiveness of AML/CFT/FPWMD procedures and compliance with sanctions regimes;
- information on identified violations and the actions taken to correct them, if these violations are related to non-compliance with AML/CFT/FPWMD requirements or sanctions regimes.

33.4. Participants are required to submit quarterly reports to the Operator on high-risk clients to whom the BCs were issued:

- persons registered in countries not participating in the international cooperation on AML/CFT;
- non-residents of the Republic of Uzbekistan;
- politically exposed persons, their family members and persons close to public officials.
- persons with card accounts linked to 20 or more BCs (regardless of the payment system they are served with).

33.5. Mandatory requirements for all the Participants:

- availability of customer identification procedures;
- availability of a customer due diligence (KYC) procedure, including:
  identification of beneficial owners;
  determination of publicly exposed persons (PEPs);
- the existence of AML/CFT risk assessment system and appropriate control measures proportionate to the risk level;
- the existence of a transaction screening system for sanctions elements;
- customer and transaction verification for compliance with international and national Lists;
- BC must be registered under the PINFL of a person the Participant reasonably believes will use a BC.
- if the Participant determines that a cardholder or MSE is on the UN sanctions list or other applicable sanctions list, or that MSE is subject to UN sanctions or other applicable sanctions regimes based on ownership or control, the Participant is obligated to:

take appropriate and timely measures to suspend the cardholder's or MSE use of the PS services and products until the PS recommendations are received;

provide the PS with detailed information on all matches and the measures taken by the Participant with respect to each cardholder or MSE after such matches are identified at least once per quarter.

33.6. Participants are required to annually, no later than the end of the first quarter, provide the Operator with a declaration of compliance with the sanctions regimes listed in this section of the Rules. The declaration must confirm that the Participant:

- complies with the requirements of the UN sanctions regimes, the US OFAC, the EU Restrictive Measures, the UK Sanctions Regime, and other applicable sanctions regimes;
- does not conduct Transactions with sanctioned persons or entities;
- applies internal procedures to monitor compliance with sanctions regimes.

33.7. Failure to comply with the above requirements may result in the Operator taking measures, including suspension or termination of participation in the PS.

34. ANTI-CORRUPTION REQUIREMENTS TO PS PARTICIPANTS

34.1. The Participant is obligated to comply with the anti-corruption legislation of the Republic of Uzbekistan, as well as other applicable international requirements.

34.2. The Participant formally establishes the principle of zero tolerance for corruption in internal documents and public statements.

34.3. The Participant does not tolerate any form of bribery, commercial bribery, abuse of office, extortion, or other corrupt practices when interacting with the PS, its representatives, employees, and agents.

34.4. The Participant is obligated to prevent the use of the Operator's services for the transfer of illegal remuneration to government officials or other persons.

34.5. Violation of the Operator's anti-corruption requirements by Participants may constitute grounds for application of measures by the payment system, including restrictions, suspension of Transactions, or termination of participation agreement/exclusion from the PS.

34.6. The Participant acknowledges the Operator's right to evaluate the Participant's anti-corruption system and demand corrective measures if significant deficiencies are found.

35. ANTI-FRAUD REQUIREMENTS TO PARTICIPANTS

35.1. This section sets out the minimum requirements for Participants to identify and prevent fraudulent transactions using BC and terminals when carrying out transactions through the PS.

35.2. Participant should:

- have documented policies and procedures for identifying and preventing fraudulent transactions using BC and devices, taking into account a risk-based approach;
- ensure monitoring of BC and device transactions to identify abnormal and suspicious activity;
- implement immediate measures to mitigate the risk of fraud, including temporarily restricting transactions using BC or device, requesting supporting documents from BC Holder or MSE, and forwarding information to the Operator, specifying available information on suspicious transactions and the response measures taken;
- designate a responsible unit or employee for fraud prevention and promptly provide the Operator with a document confirming such appointment, and ensure that this unit or employee interacts with the Operator.

35.3. The PS is entitled to:

- initiate investigations of transactions and BC Holders if there are signs of fraud or an increased risk of fraud;
- establish temporary restrictions on individual transactions of BC, MSE, or certain PS products and services, as well as initiate temporary blocking of a BC or device in the PS until the investigation is completed;
- provide the Participant with mandatory instructions aimed at preventing and limiting fraudulent transactions.

35.4. Participant is obliged to:

- provide, upon the Operator's request, complete and accurate information and documents necessary to analyze transactions and check for signs of fraud, including, if necessary, data on BC transactions or devices, KYC and due diligence results for BC

Holders and MSEs, the results of internal audits, and other relevant information;

- ensure the safety and accessibility of transaction information, documents, and event logs within the timeframes established by law, and provide such information upon the Operator's request within the agreed-upon timeframes and in the required format;
- based on the results of the Operator's audits, implement corrective measures, including strengthening monitoring settings, changing transaction limits, terminating service to certain MSEs, and other fraud risk mitigation measures, and inform the Operator of the implementation of such measures upon its request.

35.5. Failure by the Participant to comply with the requirements of this section, as well as failure to comply or untimely compliance with the Operator’s requirements, shall be considered a violation of the requirements of these Rules and may entail the application of measures, up to and including suspension of participation in the PS.

36. SETTLEMENT OF DISPUTABLE SITUATIONS

36.1. When resolving disputes and disagreements, the party whose rights have been violated may demand full compensation for actual damages from the guilty party.

36.2. Disputes between Participants are resolved through pre-trial dispute resolution in accordance with these Rules.

36.3. The Parties will take all measures to resolve disputes and disagreements arising during interactions between Participants through negotiations.

36.4. If agreement is not reached, the dispute will be referred to the court at the location of the defendant, in accordance with the legislation of the Republic of Uzbekistan.

36.5. The results of judicial consideration of disputes between Participants will be communicated to the Operator in writing.

37. RISK MANAGEMENT SYSTEM IN PS

37.1. The PS has the organized risk management system. This system identifies, monitors, and manages risks arising within the system.

37.2. The risk management unit (an authorized structural unit of the Operator) manages the risk management system, monitoring, and overseeing potential risks associated with the operation of the PS.

37.3. The unit has the authority to take prompt measures to prevent risk threats and coordinate the actions of all system participants to ensure the stability of the PS.

37.4. The main objectives of the risk management system are:

a) ensuring the uninterrupted operation of the PS;

b) reducing the impact of adverse factors on the uninterrupted operation of the PS;

c) developing and maintaining an effective mechanism for the timely identification, assessment, and prevention of potential adverse events;

d) developing measures to mitigate the consequences of realized risks;

e) ensuring the implementation of the system development strategy;

f) timely identification of information security risks;

g) developing and implementing information security measures and tools aimed at mitigating identified information security risks;

h) regulating the methodology for assessing information security risks and the procedure for documenting the results.

37.5. All the above points are implemented in accordance with the local regulations of the Operator.

38. LIMITATION OF LIABILITY OF PS

38.1. The Operator undertakes to take measures to prevent, minimize, and eliminate the consequences of events/incidents related to the operation of the PS, but does not guarantee their complete elimination.

38.2. The Operator shall not be liable to Participants for any consequences associated with Participants' use of the payment infrastructure, services, software products, interfaces, APIs, technical documentation, information resources, and other components of the UZCARD PS or the UZCARD PS Processing Center, regardless of the causes of such consequences, the nature of the claims, and the legal status of such claims. Participants acknowledge and agree that use of the services, infrastructure, and functionality of the UZCARD PS is at their own risk.

38.3. The Operator shall not be liable for any losses incurred by Participants, including direct, indirect, consequential or derivative

damages, lost profits, lost income, data loss, damage to business reputation, regulatory consequences, fines, sanctions, penalties, fines, legal costs, or any other property or non-property losses, even if the Operator has been advised of the possibility of such consequences.

38.4. The Operator's exemption from liability applies regardless of the form and degree of fault, including negligence, gross negligence, technical errors, software failures, actions or omissions of the Operator's employees, automated decisions of information systems, integration errors, and other circumstances, to the maximum extent permitted by applicable law.

38.5. The Operator's disclaimer of liability extends to contractual and non-contractual (tort) liability, liability for damages, liability for unjust enrichment, information loss, as well as claims based on recourse, subrogation, compensation, retention, and setoff.

38.6. The Operator is not responsible for the execution, refusal, delay, rejection, cancellation, or other results of payment transactions, nor for the financial consequences of such transactions or the accuracy of settlements between UZCARD PS Participants. The Participant assumes all risks associated with the results of payment transactions.

38.7. The Participant waives any claims for compensation, damages, recourse, withholding, setoff, or other property claims against the Operator related to the implementation of these Rules.

38.8. The Operator shall not bear joint, several, subsidiary, or other joint liability with Participant of the UZCARD PS.

38.9. The provisions of this section shall apply to the maximum extent permitted by applicable law and shall not limit the Operator's liability solely in cases where such limitation is expressly prohibited by mandatory provisions of law.

38.10. The Operator shall not be liable to BC Holder for illegal, unfair, or unintentional actions of the Participant and/or its staff.