APPROVED
Solution of
UNIUNI PAYMENTS TECHNOLOGIES - FZCO

RULES
Payment system of money transfers "UNIUNI PAYMENTS TECHNOLOGIES - FZCO"

United Arab Emirates, 2025

CONTENT

1. Status of the Rules

1. These Rules of the payment system of money transfers "UNIUNI PAYMENTS TECHNOLOGIES - FZCO" (hereinafter referred to as The Rules hereinafter referred to as the System Operator) have been developed by UNIUNI PAYMENTS TECHNOLOGIES - FZCO (hereinafter referred to as the System Operator) based on the requirements of the legislation of the United Arab Emirates in order to determine the conditions under which the System Operator cooperates with legal entities in carrying out money transfers, including cross-border money transfers, within the framework of the UNIUNI PAYMENTS TECHNOLOGIES - FZCO Money Transfer Payment System (hereinafter referred to as the System/UniUni.Market System).

These Rules shall be deemed accepted by potential Participants from the moment of signing the Agreement on participation in the Payment System of Money Transfers “UNIUNI PAYMENTS TECHNOLOGIES - FZCO”.

These Rules shall be deemed accepted by potential Partners from the moment of signing the relevant cooperation agreement between the parties.

The System Operator develops and implements the System Rules. Regulation of organizational and technological interactions between payment system participants, establishment of security standards, and risk management are the exclusive prerogative of the payment system operator. Requirements in these areas are the same for all payment system participants.

1.1. The rules establish:

- principles of organization and functioning of the System;
- procedure for participation in the System;
- procedure for servicing the System's clients;
- the grounds for the emergence and procedure for fulfilling the obligations of the Parties in relation to each other and to clients;
- payment procedure;
- other requirements necessary for the proper functioning of the System.

These Rules constitute an agreement of accession. The parties accede to the System Rules by accepting them in their entirety. The Rules and tariffs that form part of the Rules are published publicly on the System Operator's official website at https://uniuni.market/payments. The System Rules are interpreted in accordance with the laws of the United Arab Emirates.

1.2. To conclude an agreement with the Operator for participation in the System, an interested party (potential Participant) sends the Operator an Application for participation in the System in the form approved by the Operator.

1.3. From the moment the Operator concludes a relevant agreement with a potential Participant or Partner in the form of a bilateral written document, the Rules become binding for compliance and execution between them.

1.4. Participants and Partners are responsible for compliance with the System Rules. Failure to comply with the System Rules is grounds for termination of cooperation with a Participant and/or Partner.

1.5. The procedure for risk management and ensuring the uninterrupted operation of the System is determined by these Rules, as well as by internal regulatory documents developed by the Operator in accordance with the Rules.

2. Terms and definitions

2.1 The terms used in the text of these Rules have the following meaning:

2.1.1 **System Services-** types of money transfers approved by the Operator, including those using electronic means of payment:

- without opening an account / from a bank account for cash withdrawals to individuals;
- without opening an account / from a bank account for crediting to accounts of individuals in financial institutions;
- without opening an account / from a bank account for crediting to electronic payment methods (electronic wallets);
- The Operator has the right to expand the list of System Services.

Transfers and settlements in the System are carried out using the following forms of non-cash payments: payments by payment orders and payments in the form of funds transfers at the recipient's request (direct debit). The following types of payment documents are used within these forms of non-cash payments: payment orders, payment requests, bank orders, and, where specified by agreements, other types of payment documents.

2.1.2 **Operations center-** an organization that provides, within the System, access to Transfer services for Participants and their Clients, including the use of electronic means of payment, as well as the exchange of information between Participants.

2.1.3 **Payment clearing center-** an organization that ensures, within the System, the acceptance for execution of Participants' orders for the transfer of funds and the performance of other actions.

2.1.4 **Settlement center (SC)**– a financial institution that has entered into an agreement with the System Operator to ensure the execution of Participants' orders received from the Settlement Center by debiting and crediting funds to the Participants' bank accounts (for Direct Participants) – legal entities, or by facilitating settlements through their accounts opened with other credit institutions (for Indirect Participants), in accordance with the terms of the concluded agreements, and by sending confirmations regarding the execution of Participants' orders. The terms of the legal relationship and interaction between the Operator and the Settlement Center are governed by these Rules and the agreement concluded between the Operator and the Settlement Center. The Operator may simultaneously have several Settlement Centers engaged in the System.

2.1.5 **Participants –**the following organizations, subject to their accession to the Rules of the payment system in the manner established by the rules of the payment system:

— financial institutions that have the right, in accordance with personal law, to carry out the transfer of funds/electronic money;

— non-financial organizations that have the right, in accordance with personal law, to carry out the transfer of funds/electronic money.

Participants in the payment system may be international financial organizations, central (national) banks, banks, and payment service providers.

Depending on the type of participation in the System, Participants are divided into direct and indirect:

— Direct participation requires adherence to these Rules, the conclusion of a Participation Agreement with the System Operator, and the opening of a bank account with the Settlement Center for the purpose of making settlements with other Participants.

— Indirect participation requires adherence to these Rules, the conclusion of an Agreement with the Direct Participant, and the opening of a bank account by the Direct Participant for the purpose of making payments to other Participants.

Relationships between Direct andIndirect participants of the payment system are governed by the Payment System Rules and concluded bank account agreements.

2.1.6 **Parties**– all persons providing the System Services.

2.1.7 Sending Party – the Party that directly receives from the Sender the order and funds for the execution of the Transfer.

2.1.8 **The performing party**– The party that directly makes the payment/crediting of funds to the Recipient.

2.1.9 **Money transfer (hereinafter referred to as Transfer)**– actions of Participants and Partners within the framework of the applied forms of non-cash payments to provide the recipient with funds from the payer.

2.1.10 **Client of the System (hereinafter referred to as the Client)-** a person (resident or non-resident) sending and/or receiving a Transfer through the System, who may act as a Sender and/or Recipient, respectively.

2.1.11 Sender – the Client who gives the order to carry out the Transfer.

2.1.12 **Recipient –**The Client for whom the Translation is intended to be issued.

2.1.13 **Client Representative (also referred to as Representative)**– a person authorized to act on behalf of the Sender and/or Recipient.

2.1.14 **API**(Application Programming Interface) is a set of methods and rules by which different programs communicate with each other and exchange data. All these interactions occur through functions, classes, methods, structures, and sometimes constants of one program that are accessed by others.

2.1.15 **Electronic message (hereinafter referred to as the Message)**– information exchanged between the Parties in real time using the API.

2.1.16 Agreed communication channel **-** means and methods:

– determined by the System Operator and the Participant for information exchange and settlements;

– Agreed upon by the Operator and System entities for information exchange and settlements. System entities independently verify, on a daily basis, the information transmitted by the Operator via the Agreed Communication Channels.

Unless otherwise established by agreement of the Parties, the primary means and method of information exchange is the API.

2.1.17 **ATM**– a hardware and software system that allows Senders to independently process a Money Transfer by creating a Money Transfer order and paying for it by depositing cash or by bank transfer.

2.1.18 **Outgoing Transfer**– A transfer sent by the sending Party to the executing Party.

2.1.19 Incoming Transfer – a Transfer accepted by the executing Party from the sending Party.

2.1.20 **Remote banking services (hereinafter referred to as RBS)-** Services provided by the Parties through ATMs, Internet banking systems, and electronic means of payment.

2.1.21 **Transfer Currency-** currency of funds from among those established by the Operator for Transfers.

2.1.22 **Transfer Amount-** the amount of funds to be paid/credited to the Recipient by the Contracting Party.

2.1.23 **System Tariffs-** a system of rates and commission amounts charged to the Sender for the provision of the System Services.

2.1.24 Transfer Commission – a monetary reward for the Transfer, paid by the Sender through the Sending Party at the time of sending the Transfer in addition to the Transfer Amount.

2.1.25 **Translation Status**– information about the stage of the Transfer, defining the nature of the obligations of the Parties to the System among themselves and to the Clients regarding the implementation of the Transfer and regarding settlements related to the implementation of Transfers.

2.1.26 **Cancellation of Transfer**– cancellation of a Transfer, the irrevocability of which has not occurred or at the initiative of the Operator.

2.1.27 Party Account – a bank account of a Participant opened in the Settlement Center for the purposes of settlements on the Participant's obligations arising in accordance with the Rules for the transfer of funds for the purpose of fulfilling the monetary obligations of the Parties.

2.1.28 **Bi-currency/FX transfer-** a transfer of funds in which the currency of the Transfer issuance differs from the currency of the Transfer being sent.

2.1.29 **Irrevocable transfer of funds-** absence or termination of the possibility of cancellation of the transfer at a certain point in time.

2.1.30 **Unconditional transfer of funds-** absence of conditions or fulfillment of all conditions for the transfer of funds at a certain point in time.

2.1.31 **Finality of the transfer of funds-** provision of funds to the recipient of funds at a certain point in time.

2.1.32 **Identification**– procedures for combating the legalization (laundering) of proceeds from crime and the financing of terrorism, established by the personal law of the Participant or Partner.

2.1.33 OUPI is a payment infrastructure services operator – an operations center, a payment clearing center, and a settlement center.

2.1.34 **Partner-** a person who holds a permit (license) to conduct money transfers in accordance with personal law and who has entered into an agreement with the Participant to conduct Transfers within the System. Opening a bank account with the Settlement Center is not required.

2.1.35 **Electronic money-** funds that are previously provided by a person to a financial institution that, in accordance with personal law, is authorized to work with electronic money, taking into account information on the amount of funds provided without opening a bank account, for the fulfillment of the person's monetary obligations to third parties and in relation to which the person has the right to transmit orders exclusively using electronic means of payment (electronic wallets).

3. Principles of participation in the System

3.1 The rules of the System provide for both direct and indirect participation.

3.2.1 Responsibilities of Participants:

a) Ensure interaction with the System Operations Center to obtain information on financial messages in accordance with the specifics of payment clearing provided for by the Rules.

б) Pay for services provided by the Payment Infrastructure Service Operators within the timeframes and in the manner specified by the Rules.

в) Open an account with the Settlement Center designated by the System Operator. Ensure sufficient funds are available in the Settlement Center account. Indirect Participants are required to open an account with a Direct Participant.

г) Immediately inform the Operator of any circumstances that may affect the Participant's fulfillment of its obligations.

д) Ensure that consent is obtained for the processing (including automated processing) of data from individuals (senders and recipients of money transfers).

е) Comply with the security requirements of the System in accordance with the Rules.

ж) In the event of changes to the constituent documents, as well as changes to other data of the Participant, the said changes must be provided no later than 5 (Five) working days from the date of their state registration.

з) In the event of revocation of the Participant's license, permission to carry out activities, as well as circumstances that may worsen the financial condition of the Participant and/or the occurrence of circumstances affecting the continuity of the Participant's activities, report this fact immediately on the day of its occurrence, but no later than the end of the working day of the occurrence of the fact (in cases where the Operator involves the operations center),
agreed communication channels.

и) Independently develop your own risk analysis methodology.

3.2 Participants of the System must meet the following criteria:

3.2.1 Technological:

а) compliance of the Participant's technical equipment with the technological requirements for work in the System established by the System Operator;

б) compliance with the information security requirements defined by these Rules.

3.2.2 Organizational:

а) the presence within the Participant's structure of a special division or authorized person for interaction with the System Operator;

б) provision by the Participant of qualified personnel;

в) the willingness of the Participant to provide the System Operator with periodic reports on the work in the System.

3.2.3 Legal:

а) availability of legal confirmation of the Participant's status in accordance with personal law;

б) compliance by the Participant with the requirements for combating money laundering and terrorist financing in accordance with personal law;

3.3 After concluding the Participation Agreement, the status of a System Participant is acquired, and the necessary technological procedures for connecting to the API are carried out.

3.4 After concluding the Agreement on participation in the System, the Participant is assigned a corresponding identifier, which allows for the unambiguous identification of the Participant of the System and the type of his participation in the System.

3.5 Participants may not engage third parties to provide services for the implementation of Translations without the consent of the Participant.

3.6 If there is any information that gives reason to believe that the activities of the said third parties do not comply with the principles of the System, the System Operator has the right to unilaterally, for any reason, at any time suspend the implementation of Transfers through third parties involved by the Participants, or by the Participant itself, with subsequent notification of the Participants.

3.7 The activities of any Participant in the System may be suspended for the following reasons:

1) at the initiative of the Participant - on the day of receipt of the relevant written application from the Party indicating the reasons for the suspension;

2) at the initiative of the Operator - on the day the following grounds arise:

а) the emergence of risks of improper functioning of the System;

б) violation of the Rules by the Participant;

в) provision by the Participant to the System Operator of false information and documentation required by the Operator;

г) refusal of the Participant to provide the Operator with the necessary information and documentation required by the Operator;

д) alienation by the Participant of all or a significant part of its assets;

е) failure of the Participant to provide additional security at the request of the System Operator, if the agreement with the relevant Participant contains conditions on the availability of security, or the discovery that any security, regardless of its form, provided by the Participant to cover settlement obligations related to participation in the System is or becomes invalid, unsatisfactory or subject to the influence of significant unfavorable factors;

ж) in the event of unfavorable changes in the Participant's activities, including payment discipline within the framework of the concluded agreement, the financial position, business processes, products or services of the Participant, including information about which is received from official media;

з) attempts by the Participant to assign, delegate or otherwise transfer rights and obligations in connection with participation in the System in whole or in part to a third party, including during reorganization, without the prior consent of the Operator.

The System Operator shall notify the Participant of the suspension of the Participant's activities in the System by a written message via the Agreed Communication Channel, sent no later than the business day preceding the day of termination of the activities, indicating the reasons for the termination.

3.8 Suspension of cooperation within the System shall entail the following consequences:

а) The Operator suspends the receipt of Electronic Messages from the Participant;

б) The Participant is obliged to provide the Operator with a full financial report on its activities for all operations related to the implementation of Transfers;

в) The Participant is obliged to ensure that there are sufficient funds in the account opened with the Settlement Center and, if necessary, to replenish it with all amounts due for payment by the Participant to the Settlement Center in connection with the implementation of Transfers;

3.9 Cooperation with the Participant may be carried out on the following grounds:

1) at the initiative of the Participant - on the basis of written notice via an agreed communication channel at least 30 calendar days in advance, followed by the signing of an agreement to terminate the contract;

2) at the initiative of the System Operator - on the day the following grounds arise:

а) revocation of the Participant’s license to carry out money transfers;

б) initiation of bankruptcy proceedings against a Participant in accordance with the legislation of the Participant's state of incorporation relating to bankruptcy, insolvency, reorganization, liquidation or debt settlement;

в) continued existence of grounds for suspension of cooperation with the Participant;

г) termination of the implementation of Transfers in the territory of all states in which the Participant operates;

д) if there are no transactions in the System by the Participant for three months;

е) The Operator shall notify the Participant of the termination of transfers through the System by a written message sent no later than the next business day after termination, indicating the reasons for termination.

3.10 Cooperation with the Participant may be terminated on the following grounds:

1) at the initiative of the Participant – on the basis of notification via the Agreed Communication Channel at least 30 calendar days in advance;

2) at the initiative of the System Operator - on the day the following grounds arise:

а) revocation of the Participant’s license to carry out money transfers;

б) initiation of bankruptcy proceedings against a Participant in accordance with the personal law of the Participant related to bankruptcy,

в) insolvency, reorganization, liquidation or debt settlement;

г) continued existence of grounds for suspension of cooperation with the Participant;

д) termination of the implementation of Transfers in the territory of all states in which the Participant operates;

е) if there are no transactions in the System by the Participant for three months;

The Operator shall notify the Participant of the termination of cooperation by a message via the Agreed Communication Channels, sent no later than the next business day after termination, indicating the reasons for termination.

3.10 Termination of a Participant’s activity in carrying out transfers through the System entails the following consequences:

а) On the day of receiving notification from the Participant of the intention to terminate the Participation Agreement, the System Operator disables the ability to send Electronic Messages from the Participant;

б) These Rules and any other obligations of the Participant with respect to the services for carrying out Transfers shall remain in force and apply until all outstanding services for carrying out Transfers are finally provided by the Participant and/or until settlements for them are made between the Participant and the Clients and between the Participant and the Operator, and until all other obligations of the Participant related to its participation in the System are fulfilled.

3.11 The procedure for attracting OUPI:

The System Operator has the right to engage a private individual entrepreneur. The System Operator engages an organization to participate in the System as a private individual entrepreneur by concluding an appropriate agreement with the organization. The System Operator and the private individual entrepreneur may enter into additional agreements/contracts defining the procedures for their interaction within the System.

The OUPI, its personnel, business and technological processes, and software and hardware systems used by the OUPI within the System for the provision of services to the relevant OUPI must comply with the requirements of the System.

The list of OUPI is maintained by the System Operator independently by including information about the OUPI, indicating its type.

The System Operator maintains an up-to-date list of service providers. If the list of service providers changes, the Operator will amend it immediately upon the occurrence of the grounds for making the change.

4. Principles of organization and functioning of the System

4.1. Requirements for the OUPI:

— the presence of a license from a state regulator and other legal documents (constituent documents, certificates, etc.) required to carry out the relevant activities in accordance with personal law;

— the organization has been providing payment infrastructure services for money transfers for at least 1 (one) year;

— financial stability (the amount of the authorized capital is not less than that established in accordance with personal law);

— the ability to provide payment infrastructure services in accordance with personal law;

— technological feasibility of carrying out activities within the System in accordance with the Rules;

4.2 Responsibilities of the Payment Clearing Center:

— Ensure information and technological interaction between the subjects of the System.

— Ensure the acceptance of Participants' orders for funds transfers within the System. Verify that Participants' orders comply with established requirements.

— Transfer to the Settlement Center the Participants' orders subject to execution.

— Determine payment clearing positions (on a net basis for each of the settlement currencies).

— Calculate remuneration for services rendered by Participants, the Operations Center and the Payment Clearing Center.

4.3. Responsibilities of the Operations Center:

— Ensure the routing of authorization messages transmitted in real time between Participants and Partners of the payment system.

— Receive electronic messages containing the Participants' instructions to transfer funds and transmit these messages to the Payment Clearing Center, to the Settlement Center, and also transmit notifications (confirmations) of the acceptance and execution of the Participants' instructions.

— Ensure that Participants are provided with information on financial messages.

— Ensure registration (integration) of Participants in the System and access to money transfer services.

— Ensure the exchange of information other than authorization and financial messages.

— Ensure the receipt, processing, provision and maintenance of up-to-date information necessary for conducting transactions using ATMs in accordance with the requirements established by the Operator and provided by the System Participants.

4.4 Responsibilities of the Settlement Center:

— Ensure the execution of orders of System Participants within the System by debiting and crediting funds to the Accounts of System Participants.

— Ensure that confirmations are sent to the System Operator regarding the execution of Participants' orders.

— Ensure the receipt of information about Transfers from the Payment Clearing Center and execute them in accordance with the Rules or the agreement.

— Send a report to the Payment Clearing Center on the execution of information on Transfers based on the results of settlements.

— Send information to the Operator about the availability of funds (the exact amount is indicated) located in the Participants' Accounts.

— Provide the Operator, upon its request, with reports and any information related to the implementation by the Settlement Center of the functions assigned to it and compliance with the requirements set out in the Rules and the agreement.

— Notify the System Operator of the suspension of the Participants' activities, the opening/closing of the Participants' Accounts, as well as in the event of receipt of documents from the Participants regarding the intention to close the Accounts, immediately on the day of knowledge of its occurrence, but no later than the end of the working day of the occurrence of the fact through agreed communication channels.

— Ensure the uninterrupted provision of settlement services rendered to the Participants and, as well as organize risk management in terms of the powers delegated to it by the System Operator.

4.5 Unconditionality of Translation

For Transfers in favor of individuals for payment in cash, the unconditional nature of the Transfer occurs at the moment the Recipient applies to the payment point, provided that the conditions specified in the Rules are met, namely: the information on the transaction number matches the number specified by the Recipient, and the data on the Recipient transmitted along the transaction chain matches the data in the presented identity document.

4.6 Finality of Translation

If the Sender and Recipient are served by different Participants or Partners or other third parties, the finality of the transfer of funds occurs at the moment the funds are credited to the bank account of the Participant or Partner or other third party.

4.7 Irrevocable Translation

Irrevocable nature of Transfers occurs from the moment funds are debited from the Sender's account for the purpose of making the Transfer or from the moment the Sender provides cash for the purpose of transferring funds without opening a bank account.

4.8 Each Party to the System has the right to act as the sending Party and/or as the executing Party when carrying out Transfers.

4.9 Transfers within the System are carried out subject to the following restrictions:

b) for the Transfer Currency - restrictions may be established by the legislation of the state of incorporation of the sending Party and/or the executing Party or by an agreement concluded with the Operator;

c) for the Transfer Amount - restrictions may be established by the legislation of the state of incorporation of the sending Party and/or the executing Party or by an agreement concluded with the Operator.

On restrictions on the acceptance and/or issuance of Transfers established by the legislation of the state of incorporation of any Party, the latteris obliged to notify the Operator, who introduces these restrictions into the System software, no later than five working days before the start of applying the said restrictions.

4.10 Parties using the API are obliged to ensure that they have the equipment necessary to operate the System and to install and configure the API in accordance with the operating instructions.

4.11 The exchange of information on Transfers between the Parties, including: the transmission, processing and receipt of Electronic Messages, instructions, information on the current status of Transfers, as well as the generation of reports on Transfer transactions carried out by the Parties over a certain period, is carried out in real time by entering and reflecting the relevant information in the API and synchronizing it.

4.12 At each stage of the Transfer, Electronic Messages may be sent via the API containing the following Transfer statuses in the System:

— "accepted and paid";

— "paid";

— "cancelled".

4.13 The Parties are obligated to use the System's trademarks and the System's name in accordance with the Rules and the Agreement and may not do so. The Partner is obligated to use the System's trademarks with the Operator's consent.

4.14 To ensure the uninterrupted operation of the System, the System Operator is obliged, independently or with the involvement of third parties:

4.14.1 Back up the main components of your information technology infrastructure used within the payment system, such as (including, but not limited to the following list):

- data transmission channels;
- network equipment;
- servers, personal computers, thin clients, terminals, ATMs;
- data storage systems;
- power supply and cooling systems in the event of a complete or partial power supply and cooling failure at any time in any area of the equipment.

4.14.2 Ensure daily backup of payment system data.

4.14.3 Ensure the availability of sufficient personnel with the necessary qualifications to support the functioning of the payment system.

4.14.4 Have and maintain up-to-date technical and regulatory documentation necessary to support the System's infrastructure.

4.14.5 Regularly carry out regulatory procedures necessary to support the payment system infrastructure.

4.14.6 Have a System continuity plan and regularly test the System continuity and disaster recovery plan.

4.15 The exchange of financial information between the Parties is carried out with mandatory protection of the transmitted information using modern cryptographic means.

4.16 The Operator reserves the right to disable the functionality of the System, having previously notified other subjects of the System in accordance with the Rules.

5. Time regulations for the operation of the System

5.1. **Operation day.**

5.1.1 The System sets the operating day from 00:00:00 to 23:59:59 in the UTC+ time zone of the calendar day.

5.1.2 In the System, given the operating time regulations, a deviation of up to thirty minutes from the end time of a trading day is permitted. The start time of the next trading day is shifted by the amount of the deviation from the closing time of the previous trading day. Deviations in the start (end) time of a trading day within the established value are normal and do not require special notification to System Participants.

5.2. **Time regulations for the operation of the System.**

5.2.1 Moscow time is used as the standard time scale for calculations in the System. The reference time is the system clock of the Operator's hardware. Calculation times are presented in Table 1.

Table 1. Time for acceptance of orders of payment system participants for execution.

Event	Time in UTC+ time zone <indicate the ordinal numbers of the time zone, for example, +3:00>
Receiving orders from Payers	24/7
Acceptance of orders from Participants (Partners)	24/7

Table 2. Regulations for processing orders and settlements of Participants of the payment system.

Event	Time in UTC+ time zone <indicate the ordinal numbers of the time zone, for example, +3:00>
Execution and processing of orders for the current Reporting Period.	00:00 to 23:59.
Compilation of payment registers and reports for a closed business day and their transfer to the Payment Clearing Center.	From 00:00 to 03:00
Forwarding orders of the Payment Clearing Center to the Settlement Center	From 08:30 to 09:40
Implementation of settlements on the accounts of Participants by the Settlement Center	From 09:41 to 10:00
Sending confirmations to Participants	From 10:01 to 11:00

Table 3. Determination of the settlement day.

Making payments/crediting funds to the Recipient	Every day from Monday to Sunday inclusive from 00:00 to 23:59

The transfer of orders to the Payment Clearing Centre and their processing by the Payment Clearing Centre is carried out:	Every day from Monday to Sunday inclusive from 00:00 to 23:59
The execution of orders by the Settlement Center is carried out:	Every day from Monday to Sunday inclusive from 00:00 to 23:59

5.3. In the event of a one-time change in the time of the change of the operating day, the Operator communicates this information to the System Participants.

6. Work of System Participants with Clients

6.1 General terms and conditions

6.1.1 Clients of the System are served by the Parties provided that there is no contradiction with these Rules.

6.1.2 When servicing Clients, the Parties are obliged to comply with the following requirements:

а) communicate the terms of the Transfers to Clients in a form accessible for review (for example, by posting the text of the terms of the Transfers in electronic form on their websites or remote banking systems, or on paper on information boards);

б) inform Clients about the restrictions in force when making Transfers;

в) accept and issue Transfers in accordance with the temporary regulations for the operation of the System;

г) inform Clients of the list of documents required for Clients to carry out a Money Transfer, as well as provide documents for sending, receiving, changing the terms, and canceling a transfer;

д) ensure the Client's consent to the processing (including collection, recording, systematization, accumulation, storage, clarification (updating, modification), extraction, use, transfer (distribution, provision, access), depersonalization, blocking, deletion, destruction of personal data) of the Client's personal data.

6.2 Commission for carrying out Money Transfers.

6.2.1 For the Transfer, the Sender pays a Transfer Fee, which may be charged:

а) as a percentage of the Transfer Amount;

б) in a fixed amount depending on the Transfer Amount;

в) in a combination of a fixed amount and a percentage of the Transfer Amount.

The commission amount may vary, including depending on:

а) from the Transfer Amount;

б) from the means of transfer used by the Sender, including electronic means of payment and forms of non-cash payments;

в) from the location chosen by the Sender for making the transfer: in offices, using remote banking services, etc.;

г) from the method of payment/crediting of the Transfer;

д) from the Transfer Currency.

6.2.2 Information on fees charged to the Sender is posted on the System Operator's website.

6.2.3 Due to the possibility of varying the commission fee, the exact amount of the commission charged is communicated to the Sender at the Customer service locations.

6.2.4 The Transfer Commission is paid by the Sender simultaneously with the Transfer Amount directly to the sending Party.

6.3 Sending Transfers

6.3.1 The Sender gives an order for the Transfer in the manner established by the Participant, provided that it does not contradict these Rules.

6.3.2 To carry out the Transfer, the sending Party is obliged to:

— inform the Sender of the following information:

— the possible currency of receipt and issue of the Transfer, and also the conversion rate when converting;

— the total amount and currency of the Transfer Commission;

— the availability and possible address of the executing Party for the direction of the Transfer chosen by the Sender;

— possible restrictions on sending the Transfer.

6.3.2.1 ensure the provision of services to the Sender through the RBS, only in relation to which, in the case established by personal law, the Sender was identified on the basis of the original identity documents and other documents submitted by the Sender in accordance with the legislation on combating the legalization (laundering) of proceeds from crime, the financing of terrorism and the financing of the proliferation of weapons of mass destruction, in accordance with the legislation of the state in whose territory the Transfer is accepted, and also carry out a check for signs of the transfer of funds without the voluntary consent of the client;

— receive an order from the Sender for the Transfer in the following sequence:

— The sending Party provides the Sender with the opportunity, by filling out the on-screen forms of the Remote Banking System, to transfer to the sending Party the information necessary for filling out the order for the Transfer in electronic form;

— prior to the signing by the Sender of the Transfer order with an analogue of a handwritten signature, as provided for in a separate agreement between the sending Party and the Sender on the use of the RBS, provide the Sender with the opportunity to review the information specified in the Transfer order and, after verification of the information by the Sender, receive from him an electronic Transfer order signed with an analogue of a handwritten signature via the RBS;

— Ensure the safekeeping and accessibility of the Transfer order in electronic form sent using the Remote Banking Service at any time within the time period established by the legislation of the state in whose territory the Transfer is accepted.

— Receive the Transfer Amount and Transfer Fee from the Sender.

6.3.3 Upon receipt of the above documents, the Transfer Amount and the Transfer Fee from the Sender, the sending Party is obliged to:

a) immediately generate and send an Electronic Message regarding the assignment of the Transfer status “accepted and paid”.

A Transfer that is not assigned the "accepted and paid" status in the Electronic Message is considered unsent and is treated as a Transfer unpaid by the Sender. Such a Transfer is not included in settlements with the Sendering Party.

6.4 Payment of Transfers

6.4.1 The Transfer must be paid to the Recipient after the Transfer has been assigned the status “accepted and paid”.

6.4.5.1 When making a payment of a Transfer to the Recipient using the Remote Banking System of the Executing Party:

1) ensure the provision of services to the Recipient through the Remote Banking Service, only in relation to whom, in the case established by applicable law, the Recipient has been identified on the basis of the original identity documents and other documents submitted by the Recipient in accordance with the legislation on combating the legalization (laundering) of proceeds from crime, the financing of terrorism and the financing of the proliferation of weapons of mass destruction, in accordance with the legislation of the state in the territory of which the Transfer is issued;

6.4.2 After the Transfer has been paid to the Recipient, the Executing Party is obliged to immediately generate and send an Electronic Message regarding the assignment of the “paid” status to the Transfer.

6.5 Cancellation of Transfers.

6.6.1 Cancellation of Transfers is carried out:

1) at the initiative of the Sender;

2) at the initiative of the Operator unilaterally in the following cases:

a) termination of cooperation between the Operator and the Contracting Party;

b) the occurrence of other circumstances that make it impossible for the executing Party or another Participant to issue the Transfer to the Recipient for reasons beyond the control of the Sender and the Recipient.

Cancellation (return) of an order to transfer funds is carried out until the moment the transfer of funds becomes irrevocable.

The Transfer fee is non-refundable if the transfer is cancelled at the initiative of the Sender.

When returning a Bi-Currency Transfer, the Sender is given the Transfer Amount at the exchange rate (conversion) at the time of return, set by <indicate by whom the exchange rate should be set upon return>.

The period for returning the Transfer amount depends on the technical integration features, as well as the internal procedures and personal laws of the Participant.

7. System Tariffs

7.1 Tariffs are part of the Rules and are published in the public domain on the Operator’s website in the Internet information and telecommunications network at the address <indicate the link to the Operator’s website>.

7.2 Information about the Transfer Commission is published in the System Tariffs or in agreements between the Parties.

7.3 The payment procedure for payment infrastructure services is uniform across the System. If the functions of the Settlement Center, Payment Clearing Center, Operations Center, or some of these functions are performed by organizations contracted by the Operator, the fee paid by the Participant includes the payment infrastructure services fee.

8. Loyalty program and marketing (incentive) promotions

8.1 The Operator has the right to organize and conduct loyalty programs for clients using the System's services.

8.2 The Operator has the right to establish the rules of loyalty programs organized by the Operator.

8.3 The rules of the loyalty programs are posted by the Operator on its official website.

8.4 The Operator reserves the right to conduct various marketing (incentive) promotions and other marketing activities related to the establishment of a special transfer fee for a specified period in order to promote services and encourage participants and their clients (hereinafter referred to as the "Promotion"). Promotions may apply to a specific territory, individual Participants, individual Services, or individual methods of providing access to Participants' Clients, individual Services, or individual methods of providing access to Participants' Clients. The Operator reserves the right to cancel or amend the terms of any Promotions at any time, as well as extend the validity of such Promotions an unlimited number of times. Information about any Promotions will be communicated to the Participants involved in the Promotion in advance by any means convenient to the Operator.

8.5 Participants have the right to provide Clients with discounts on Services, with the exception of discounts provided for by loyalty programs organized by the Operator solely with the prior consent of the Operator.

9. The procedure for payment clearing and settlement

9.1 General principles

9.1.1 Payment clearing in the System is carried out by the Payment Clearing Center through:

9.1.1.1 executionprocedures for accepting Participants' orders for execution, including checking the compliance of orders with established requirements, determining the sufficiency of funds for the execution of orders and determining payment clearing positions (the amounts of funds to be debited and credited by the Settlement Center to the accounts of Direct Participants, or to their accounts opened in other credit institutions - for Indirect Participants);

9.1.1.2 transfer to the Settlement Center for the execution of accepted orders of the Participants;

9.1.1.3 sending notifications (confirmations) to Participants regarding the acceptance for execution of orders, as well as the transfer of notifications (confirmations) regarding the execution of orders of Participants;

9.1.1.4 monitoring the execution of orders contained in the register for debiting funds from the account in favor of recipients, for compliance with the data in the report on transactions carried out by payers.

9.1.2 The payment clearing position on a gross basis is determined as the total amount of Participants' orders accepted for execution by the Payment Clearing Centre during the Operator's business day, for which the Participants are payers or recipients of funds.

9.1.3 Based on the results of determining the payment clearing position on a gross basis, the Participants' orders are transferred by the Payment Clearing Center to the Settlement Center for execution.

9.1.4 When settling on a net basis in the System, the Participant's largest obligation is fulfilled. The net payment clearing position is determined by the difference between the total amount of Participants' orders to be executed, accepted for execution by the Payment Clearing Center during the System Operator's business day, for which the Participants are payers, and the total amount of Participants' orders accepted for execution by the Payment Clearing Center, for which the Participants are recipients of funds. The net basis may be determined separately for each type of Services provided/received.

9.1.5 It is permissible to determine the position on a net basis separately for each type of Services provided/received by Participants;

9.1.6 Based on the results of determining the payment clearing position on a net basis, the Payment Clearing Centre transfers to the Settlement Centre for execution orders for the amount of certain payment clearing positions on a net basis of the Participants and (or) the accepted orders of the Participants.

9.1.7 The payment clearing position, regardless of the method of its determination (gross or net), on the basis of which funds will be debited from the accounts of the Participants, is the payment clearing position on the basis of which funds will be credited to the account of the Settlement Center, and vice versa;

9.1.8 In order to carry out settlements, the Direct Participant opens correspondent accounts in the Settlement Center in the currencies in which settlements with the Participant are carried out through the System.

9.1.9 Direct Participants must ensure the availability of funds in their correspondent accounts necessary for the uninterrupted settlement and fulfillment of obligations to System Participants and the UUPI. Indirect Participants must ensure the availability of funds necessary to fulfill their obligations to Direct Participants.

9.1.10 The Payment Clearing Center sends to Direct Participantsreports on completed transactions (in accordance with the Operator’s form) by sending them to the Participant via the Agreed Communication Channels.

9.1.11 The Settlement Center sends statements to Direct Participants on transactions carried out in the System in the relevant currency, reflecting the debit/credit to the accounts of the System Participants; for transactions of Indirect Participants, statements are provided by the Direct Participant who has opened the corresponding Indirect Participant accounts;

9.1.12 Direct Participants, when concluding bank account agreements with the Settlement Center, grant the right to write off funds from accounts without additional instructions from the System Participants, subject to the terms of a previously given acceptance upon presentation of a write-off request.

9.1.13 The Settlement Center has the right to issue payment demands to direct Participants for additional payment infrastructure services rendered, as well as to provide loans to System Participants for settlements in the System.

9.1.14 If there are insufficient funds in a Participant's correspondent account, the Settlement Center immediately notifies the Operator via the Agreed Communication Channels, and the Operator blocks the ability to send Money Transfers until the settlement is finalized. If there are insufficient funds in Participants' accounts, the Settlement Center immediately notifies the System Operator via the Agreed Communication Channels. The System Operator informs Participants of the need to top up their accounts.

9.1.15 The settlement center ensures the availability of funds in its correspondent accounts in the amount necessary for the uninterrupted execution of settlements.

9.1.16 Settlements between Participants and the Settlement Center are carried out on business days and in accordance with the temporary regulations for the functioning of the System, as defined in the Rules, on the basis of a specific clearing position, regardless of the method of its determination (gross or net) of each Participant of the System.

9.1.17 The terms of settlements between the Direct and Indirect Participants are determined in the relevant agreement concluded between them.

9.1.18 The frequency and conditions of settlements between the System Participant and the Partner are determined in the relevant Cooperation Agreement of the parties; the conditions of settlements between the Direct and Indirect Participants are determined in the relevant agreement concluded between them.

9.1.19 The procedure for ensuring the fulfillment of obligations of Participants regarding the transfer of funds:

1) Fulfilment of obligations is ensured by the use of risk management methods;

2) Inclusion of a condition in correspondent account agreements regarding the possibility of debiting funds from the bank accounts of Participants without additional instructions from the account owner.

9.2 The procedure for calculating the payment clearing of Participants

9.2.1 Payment clearing for the Participant is carried out in the following order:

9.2.1.1 The Payment Clearing Center, based on the reports generated in the System on completed Money Transfers, maintains daily records of Money Transfers carried out between Direct Participants, as well as mutual claims and obligations of Direct Participants based on the results of these transactions.

Accounting of transactions carried out on weekends and/or holidays and on the working day preceding a holiday and/or day off is carried out daily, regardless of the weekend and/or holiday.

9.2.1.2 The System Operator carries out daily offsetting of counterclaims and obligations between the Settlement Center and the Direct Participant based on the results of transactions carried out between the Parties.

9.2.1.3 If, as a result of payment clearing, the total amount of Money Transfers accepted by the Direct Participant, commissions, Transfer Commissions, commissions due to the System Operator and other third parties for Money Transfers, on a business day exceeds the total amount of Money Transfers issued by the Direct Participant, commissions due to the Participant and other third parties for issued Money Transfers, as well as cancelled Outgoing Transfers, then the Direct Participant shall have an obligation for the amount of the excess.

9.2.1.4 If, as a result of payment clearing, the total amount of Outgoing Transfers accepted by the Direct Participant, Transfer Fees, fees due to the System Operator and other third parties for Incoming Transfers processed and issued on a business day is less than the total amount of Incoming Transfers issued by the Direct Participant, fees due to the Direct Participant for Incoming Transfers, and cancelled Outgoing Transfers of the Direct Participant, then an obligation to the Direct Participant arises in the amount of the difference.

9.2.1.5 The amounts of Transfers Cancelled at the initiative of the Operator are not included in the total amount of the Participants' obligations.

9.2.1.6 The claims and obligations of Direct Participants are accounted for separately in each currency of Money Transfers between Direct Participants. Amounts for the fulfillment of obligations are credited to/debited from the Direct Participants' correspondent accounts.

6.2.5 The Transfer Fee can be paid in the following ways:

а) The Transfer Amount and Transfer Fee are debited from the Participant's account by the Settlement Center. The Settlement Center then transfers the due remuneration to the Participant's account.

б) The Settlement Center debits the Transfer Amount and the Transfer Fee from the Participant's account, minus the remuneration due to the sending Party.

в) In an agreed manner in the agreement between the Operator and the Participant.

The method of transferring the transfer fee is determined by the Operator in agreement with the Participant.

9.2.1.7 In the event of negative net positions of Participants, the Settlement Center immediately notifies the OUPI and the Operator via the Agreed Communication Channels, and the OUPI and the Operator block the ability of such Participants to carry out Transfer transactions until the final settlement of settlements.

9.3 The procedure for making mutual settlements between the Participant and the Partner, who is the Participant’s client

9.4.1 Unless otherwise provided in the relevant agreement between the Participant and the Partner, who is the Participant’s client, mutual settlements between the Participant and the Partner are carried out in the following order:

9.4.1.1 The Participant, on the basis of reports generated in the System on completed Money Transfers, maintains daily records of transactions between the Participant and the Partner, as well as mutual claims and obligations based on the results of these transactions.

9.4.1.2 Accounting of transactions carried out on weekends and/or holidays and on the working day preceding a holiday and/or day off is carried out daily, regardless of the weekend and/or holiday.

9.4.1.3 The System Participant shall daily offset the counterclaims and obligations between the System Participant and the Partner based on the results of transactions conducted between the Parties.

9.4.1.4 If, as a result of mutual settlements between a Participant and a Partner who is the Participant's client, the total amount of money transfers sent by the Partner exceeds the total amount of Incoming and Cancelled Transfers, taking into account commissions due to the Partner, a liability for the excess amount will arise. The Partner is obligated to transfer the difference to the Participant on the day of settlement using the details specified in the agreement.

9.4.1.5 If, as a result of mutual settlements between a Participant and a Partner who is the Participant's client, the total amount of the Partner's Outgoing Transfers is less than the total amount of Incoming and Cancelled Transfers, taking into account the commissions due to the Partner, the Participant will be liable for the difference. On the day of settlement, the Participant is obligated to transfer the difference to the Partner using the details specified in the agreement.

9.4.1.6 The amounts of Transfers Cancelled at the initiative of the Operator are not included in the total amount of the Participants’ obligations.

9.4.1.7 The Partner's claims and obligations are accounted for separately in each currency of the Money Transfers carried out between the Partner and the Participant.

10. Risk Management in the System

10.1 Organizational aspects of interaction between subjects of the Risk Management System

10.1.1 The risk management system in the System is understood as a set of measures and methods for reducing the likelihood of adverse consequences for the smooth functioning of the payment system (hereinafter referred to as the FSPS), taking into account the amount of damage caused.

10.1.2 The organizational model for risk management in the System is the distribution of functions for risk assessment and management between the Operator, the OUPI, and the Participants.

10.1.3 Operations Center:

– authorized and responsible for operational risk management;

– ensures the level of continuity of provision of operational services within the standard values established by the Rules;

– ensures a reduction in the risk of disruption to the continuity of operational services through the continuous, round-the-clock operation of hardware and software systems.

10.1.4 Payment clearing center:

– is authorized and responsible for managing credit and liquidity risk;

– ensures a reduction in the risk of a breach of the BFPS by eliminating delays in the end of the clearing cycle that arise due to the fault of the Payment Clearing Centre.

10.1.5 Settlement center:

– is authorized and responsible for the management of settlement risk (credit risk and liquidity risk), including the creation of an organizational structure for managing credit risk and liquidity risk, and the development of internal regulatory documents, including methods for analyzing credit risks and liquidity risks in accordance with the terms of these Rules;

– ensures a reduction in the risk of violation of the BFPS by eliminating delays in the time of settlements with Participants that arise due to the fault of the Settlement Center.

10.1.6 Participants:

– comply with these Rules, concluded agreements, and personal law;

– ensure adequate protection of information;

– ensure the maintenance of the required balance of funds in their accounts at the Settlement Center.

10.1.7 System participants independently organize and implement risk management specific to their activities and participation in the System. The risk management system of each System participant must include, but not be limited to, the appointment of responsible employees and/or the delegation of appropriate authority to departments responsible for risk management and the development of internal risk management rules.

10.1.8 System entities are responsible for implementing a risk management system in their activities in accordance with the Rules and the requirements of their personal law. All System entities are responsible for risk management within the scope of their authority.

10.2 **Organizational structure of the Operator's risk management system**

10.2.1 The System Operator and the System entities shall, by internal documents, determine the official or structural unit whose responsibilities include ensuring monitoring and carrying out activities related to risk management in the System.

10.2.2 The functional responsibilities of an official or structural subdivision of the Operator and the subject of the System must include:

– approval of the basic principles of the risk management system;

– approval of internal documents in the field of risk management;

– review of reports from structural divisions on the state of the risk management system and assessment of accepted risks;

– making the necessary management decisions on planning activities in the event that the risk level is recognized as increased;

– development, application and evaluation of the effectiveness of risk analysis methods in the System, requirements for the presentation and verification of analysis results.

– development of internal documents in the field of risk management;

– selection and implementation of measures and methods for achieving and maintaining an acceptable level of risks in the System, assessment of their effectiveness and improvement;

– establishing criteria for assessing the risk management system, including systemic risk, and conducting the said assessment;

– monitoring the level of risks in the system;

– analysis and regular assessment of the risk level for each type of risk;

– identification, measurement and determination of the acceptable level of risk for each type of risk;

10.3 Risk management methods

10.3.1 The System uses the following risk management methods:

– implementation of settlements within the limits provided by the Participants of the Funds System;

– ensuring the possibility of providing a loan;

– use of an irrevocable bank guarantee or letter of credit;

– other risk management methods.

10.4 Providing the Operator's management bodies with relevant information about risks

10.4.1 Information about risks in the event of emergency situations or significant violations of the acceptable risk level (including cases of system failures) is immediately communicated to the Operator's management bodies.

10.4.2 Consolidated risk level information is communicated to the Operator's management bodies by the risk management officer based on the results of a risk assessment using the System's risk analysis methods, including risk profiles. Information on the overall risk level in the System is communicated following the completion of a scheduled assessment of all risks or an unscheduled assessment of all and/or individual risks in the System in the form of written reports from the risk management officer.

10.6 Payment System Continuity Indicators

10.6.1 The indicator for the duration of restoration of the provision of payment infrastructure services (hereinafter referred to as indicator P1), which characterizes the period of time for restoration of the provision of payment infrastructure services in the event of suspension of the provision of payment infrastructure services, including due to a violation of the requirements for ensuring the protection of information when making money transfers.

The P1 indicator is calculated for each of the OUPI and for each of the incidents that resulted in the suspension of the provision of payment infrastructure services, as the period of time from the moment of the occurrence of the event that led to the suspension of the provision of payment infrastructure services as a result of the first of the incidents that occurred, until the moment of restoration of the provision of payment infrastructure services.

In the event of incidents resulting in the simultaneous suspension of payment infrastructure services by two or more payment institutions, the P1 indicator is calculated as the period of time from the occurrence of the event that led to the suspension of payment infrastructure services as a result of the first incident until the restoration of payment infrastructure services by all payment institutions that experienced the incidents. The P1 indicator is calculated in hours/minutes/seconds.

10.6.2 The Payment Infrastructure Service Continuity Indicator (hereinafter referred to as "PI2") is the period of time between two consecutive events occurring in the System that resulted in a disruption of payment infrastructure services in compliance with service requirements, including due to violations of information security requirements for funds transfers (hereinafter referred to as "incidents"), resulting in the suspension of payment infrastructure services. Suspension (termination) of participation in the System in cases stipulated by the Rules is not considered an incident for the purposes of the Rules.

The P2 indicator is calculated for each individual payment service provider upon the occurrence of each incident that resulted in the suspension of payment infrastructure services. This indicator represents the period of time between two consecutive incidents that occurred at the individual payment service provider, resulting in the suspension of payment infrastructure services, from the moment the payment infrastructure services suspended as a result of the first incident are restored until the moment the event that led to the suspension of payment infrastructure services as a result of the subsequent incident occurs. The P2 indicator is calculated in hours/minutes/seconds.

10.6.3 The indicator of compliance with the regulations (hereinafter referred to as the P3 indicator) is the compliance by the OUPI with the start time, end time, duration and sequence of procedures performed by the OUPI in the provision of operational services, payment clearing services and settlement services.

The P3 indicator is calculated for each OUPI. For the Operations Center, the P3 indicator is calculated as the ratio of the number of Participant orders for which operational services were provided during the calendar month without violating the procedure regulations to the total number of Participant orders for which operational services were provided during the calendar month, calculated using the following formula:

$$П3_{оц} = (N_{оц} / N_{оц}^{общ}) \times 100\ \%,$$

Where:

$N_{оц}$ - the number of Participants’ orders for which operational services were provided during the calendar month without violating the regulations for the implementation of procedures,

$N_{оц}^{общ}$ - the total number of Participants’ orders for which operational services were provided during the calendar month.

For the Payment Clearing Center, the P3 indicator is calculated as the ratio of the number of Participants' orders for which payment clearing services were provided during the calendar month without violating the procedure regulations to the total number of Participants' orders for which payment clearing services were provided during the calendar month, calculated using the following formula:

$$П3_{пкц} = (N_{пкц} / N_{пкц}^{общ}) \times 100\ \%,$$

Where:

$N_{пкц}$ - the number of Participants’ orders for which payment clearing services were provided during the calendar month without violating the regulations for the execution of procedures,

$N_{пкц}^{общ}$ - the total number of Participants' orders for which payment clearing services were provided during the calendar month.

For the Settlement Center, the P3 indicator is calculated as the ratio of the number of orders of Participants and (or) the Payment Clearing Center, for which settlement services were provided during the calendar month without violating the regulations for the implementation of procedures, to the total number of orders of Participants and (or) the Payment Clearing Center, for which settlement services were provided during the calendar month, calculated using the following formula:

$$П3_{рц} = (N_{рц} \;/\; N_{рц}^{общ}) \times 100\ \%,$$

Where:

$N_{рц}$ - the number of orders of Participants and (or) the Payment Clearing Center, for which settlement services were provided during the calendar month without violating the regulations for the implementation of procedures,

$N_{рц}^{общ}$ - the total number of orders of Participants and (or) the Payment Clearing Center for which settlement services were provided during the calendar month.

The P3 indicator is calculated monthly as a percentage with an accuracy of two decimal places (rounded using the mathematical method).

The value of the P3 indicator for the System as a whole is taken to be equal to the smallest of the values of this indicator calculated for all the OUPIs in relation to all types of services they provide.

The indicator of availability of the Operational Center of the Payment System (hereinafter referred to as indicator P4) characterizes the provision of operational services by the Operational Center of the Payment System.

The P4 indicator is calculated as the average value of the availability coefficient of the System Operations Center for a calendar month, calculated using the following formula:

$$П4 = \left(\sum_{i=1}^{M} \left(1 - \frac{D_i}{T_i} \right) \Big/ M \right) \times 100\ \%,$$

Where:

M - the number of working days of the System in a month,

D_i - the total duration of all suspensions of the provision of operational services by the Operations Center of the payment system for the i-th working day of the month in minutes,

T_i - the total duration of time for the provision of operational services during the i-th working day in minutes, established in accordance with the time regulations for the operation of the System.

The P4 indicator is calculated monthly as a percentage with an accuracy of two decimal places (rounded using the mathematical method).

The value of the P4 indicator for the System as a whole is taken to be equal to the smallest of the values of this indicator calculated for all operating centers of the Payment System.

The indicator of change in the frequency of incidents (hereinafter referred to as indicator P5), which characterizes the rate of increase in the frequency of incidents.

The P5 indicator is calculated for the System as a whole and for each individual OUPI as the growth rate of the average daily number of incidents for the assessed calendar month in relation to the average daily number of incidents for the previous 12 calendar months, including the assessed calendar month, calculated using the following formula:

$$П5 = \left(\frac{\sum_{i=1}^{M} КИ_i \Big/ M}{\sum_{i=1}^{N} КИ_i \Big/ N} - 1 \right) \times 100\%,$$

Where:

$КИ_i$ - the number of incidents during the i-th working day of the System of the assessed calendar month,

M - the number of working days of the System in the assessed calendar month,

N – the number of working days of the System for the 12 previous calendar months, including the month being assessed.

The P5 indicator is calculated monthly as a percentage with an accuracy of one decimal place (rounded mathematically). If there were no incidents over the previous 12 calendar months, including the month being assessed, the indicator value is considered zero.

The System has the following threshold levels for BFPS indicators:

- the threshold level of the P1 indicator is no more than 6 hours for each of the UPI Payment System Operators;
- the threshold level of the P2 indicator must be at least 12 hours for each of the UPI Payment System Operators;
- the threshold level of the P3 indicator must be no less than 98.0% for the Operational and Payment Clearing Centers of the payment system and no less than 99.0% for the Settlement Center of the Payment System;
- the threshold level of indicator P4 must be at least 96.0%;
- the threshold level of the P5 indicator should be no more than 1250.0%.

10.7 Procedure for ensuring the uninterrupted operation of the System

10.7.1 In order to ensure the BFPS, the Operator establishes a procedure for the implementation by the subjects of the System of coordinated activities aimed at achieving, confirming and maintaining an acceptable level of risks of BFPS violation, which are understood as typical possibilities inherent in the functioning of the System of failure to provide, or improper provision of services of the System to Participants due to the occurrence of unfavorable events associated with internal and external factors of the functioning of the System (hereinafter - risk factors of BFPS violation).

10.7.2 Procedure for interaction within the System in emergency and non-standard situations.

10.7.3 In the event of detection of emergency situations within the System, including events that have caused system failures, the subjects of the System that have identified the said circumstances shall immediately take all actions within their power to reduce the harmful consequences, and shall immediately inform the Operator and the subject of the System, in whose functional area of responsibility lies the area of occurrence of the emergency/non-standard situation or failure, via any of the Agreed Communication Channels about the situation that has arisen, including information about the events that, in their opinion, have caused the emergency/non-standard situation, operational failures, their causes and consequences.

10.7.4 Requirements for the content of activities to ensure the BFPS carried out by the Operator, OUPIAndParticipants,should include:

– requirements for detailing the acceptable level of risks of violation of the BFPS in terms of categories of subjects of the System according to the types of their activities or participation in the System;

– the procedure for developing, applying and evaluating the effectiveness of risk analysis methods in the System, requirements for the presentation and verification of analysis results;

– the procedure for assessing the quality and reliability of the functioning of information systems, operational and technological means used by the OUPI;

– the procedure for selecting and implementing measures and methods for achieving and maintaining an acceptable level of risk of violation of the BFPS, the procedure for assessing their effectiveness and improvement;

– requirements for monitoring the risks of violation of the BFPS;

– requirements for business continuity and recovery plans for the UPI.

10.7.5 The procedure for information interaction between the System entities and documentation support for their activities to ensure the BFPS includes:

– a list of documents used by the System entities in the implementation of activities to ensure the BFPS, and the procedure for their preparation;

– the procedure for informing the Operator about events that have caused controversial, non-standard and emergency situations, including cases of system failures, the results of the investigation of these events, and the analysis of their causes and consequences;

– the procedure for informing the Operator about the failure to fulfill or improper fulfillment of the obligations of the Participants;

– the procedure for collecting, documenting and statistically processing primary information on the functioning of the System.

10.7.6 Primary information about the functioning of the System includes:

– information on the time of acceptance for execution, execution of Participants’ orders to transfer funds, the number and amounts of said orders (including for each Participant who is the sender or recipient of funds);

– information on the size of clearing positions and cash balances in the Participants’ accounts opened in the Settlement Center;

– other information about the functioning of the System, as provided for by these Rules.

10.7.7 The System's subjects organize activities to implement the procedure for ensuring the BFPS within the framework of internal risk management systems for their activities.

10.7.8 The Operator's activities to ensure the BFPS include:

– implementation of coordination of the activities of the subjects of the System to ensure the BFPS;

– development of internal documents regarding the implementation of the risk management system and the financial and financial support system;

– Establishing an acceptable level of risk for violation of the BFPS. This is performed by the Operator's risk management body at least once per quarter;

– determination of the duration of the period of time during which the proper functioning of the System must be restored in the event of its disruption, including in the event of suspension (termination) of the provision of payment infrastructure services;

– monitoring the risks of violation of the BFPS in order to identify current changes in the inherent level of risk of violation of the BFPS;

– analysis of the risks of violation of the BFPS (identification of risk factors for violation of the BFPS, determination of the degree and nature of the influence of these factors on the BFPS, assessment of the inherent level of risks of violation of the BFPS and confirmation of the compliance of the inherent level of risks of violation of the BFPS with the established acceptable level of risks);

– taking measures necessary to achieve or maintain an acceptable level of risk of violation of the BFPS;

– conducting investigations of events that caused operational failures, analyzing their causes and consequences;

– Taking measures to eliminate or minimize the risks of violation of the BFPS. Penalties stipulated by the relevant Participation Agreements in the System are applied to Entities in the event of non-compliance with the established BFPS level;

– measures aimed at managing the continuity of the System’s operation in the event of incidents related to the suspension of the provision of payment infrastructure services or the violation of established levels of provision of payment infrastructure services;

– ensuring the restoration of the proper functioning of the System in the event of a disruption, including the restoration of the provision of payment infrastructure services;

– Identification in the System of organizations providing payment infrastructure services to its Participants and their Clients, including in cases where payment infrastructure services are provided to a single Participant or a limited number of Participants and/or their Clients. Involvement of these organizations as payment infrastructure service operators in accordance with the functional responsibilities of the Operator;

– conducting an assessment of the quality of functioning of operational and technological means and information systems at least once a year, as well as making decisions on changing operational, technological means and procedures based on the results of such an assessment;

– conducting an assessment of the risks inherent in the activities of the System Operator to ensure the continuity of the System’s activities;

– assessment of the financial stability of Participants and OUPI (analysis of financial statements and other documents provided by Participants/OUPI);

– coordination of activities and implementation of information interaction between the Entities in order to manage the risks of violation of the BFPS.

10.7.9 Activity ABOUTThe UPI for ensuring the BFPS is carried out in accordance with the functional responsibilitiessubjects of the Systemwithin the frameworkWITHsystems and includes:

– organization and implementation of activities to ensure the uninterrupted provision of services to Participants in accordance with the functional responsibilities of the System entities within the framework of the System risk management system;

– development of internal documents in terms of implementing its activities in the Risk Management System and ensuring the BFPS;

– development of a plan and procedure of action to ensure the continuity of provision of operational services, payment clearing services and settlement services;

– Establishing permissible technological interruptions in the provision of operational services in order to maintain the quality of functioning of operational and technological facilities. The total duration of technological interruptions may not exceed 48 (forty-eight) hours during each year of operation;

– collection and processing of primary information on the time of receipt of Participants' orders by the Payment System, the progress of the execution of said orders, the characteristics of the funds transfers carried out, the quantity, amount and time of finality of the transfers, the size of clearing positions and the balances of funds in the accounts of Participants;

– provision, upon request of the Operator, of primary information on the functioning of the Payment System;

– collection and processing of information on events that caused operational failures, their causes and consequences, as well as in the event of the emergence or realization of a threat of non-fulfillment or improper fulfillment by Participants of their obligations;

– monthly provision by UPI Operators to the Operator of summary information on all incidents identified during the reporting month in the manner prescribed in the Rules.

– organization and implementation of activities to ensure the uninterrupted provision of services to Participants in accordance with the obligations assumed and the requirements of the procedure for ensuring the uninterrupted provision of services to Participants;

– monitoring the risks of violation of the BFPS;

– regular assessment of the quality and reliability of the functioning of the information systems used, the operation of automated systems, software, computing equipment, telecommunications equipment, the operation of which is ensured by the System Operator, the System Participants, and their improvement.

10.7.10 ActivityParticipants in the provision of the BFPS include:

– provision to the Operator in electronic form of financial reports (balance sheet, calculation of mandatory economic standards, calculation of equity and profit and loss statement, other documents at the request of the Operator) for each reporting date (if the said reports are not published on the website of the Participant or the Bank of Russia);

– conducting an assessment of the Participant’s risks inherent in its type of activity in the System in order to ensure business continuity;

– taking measures to ensure compliance with the requirements of the System and proper fulfillment of the obligations assumed;

– immediate (no later than the next business day from the moment of detection) informing the Operator about cases of failure to provide or improper provision of services provided within the System, and events that have caused operational failures, as well as events that have caused controversial, non-standard and emergency situations, including cases of system failures, about their causes and consequences;

– monitoring the risks of violation of the BFPS;

– independently conducting an assessment of the quality of functioning of operational and technological means, information systems, automated systems, software, computing equipment, telecommunications equipment at least once a year, as well as providing the Operator, at its request, with the results of the assessment (in the form of an act on the Participant's testing of the quality of functioning of the module(s) associated with interaction with the System) by e-mail;

– monitoring compliance with the requirements of legislation, these Rules, agreements and conditions for the implementation of money transfers;

– compliance with the requirements of these Rules and the obligations assumed in connection therewith;

– exercising control over the use of the name and trademarks of the System solely within the framework of these Rules.

10.7.11 TOmonitoringThe following requirements are imposed to address the risk of violation of the BFPS:

– monitoring of the risks of violation of the BFPS must be carried out by the subjects of the System on an ongoing basis (daily);

– Analysis of the achieved results should be carried out at least once a month.

10.7.12 MonitoringThe risk of violation of the BFPS should be carried out in the following directions:

– fulfillment of financial obligations;

– availability of technical services.

10.7.13 In order to organize work on ensuring the BFPS, the OUPI must develop and use in their work documents establishing a policy for ensuring business continuity and a plan for restoring the system’s operations after failures (the BCIP Plan).

10.7.14 The following requirements are imposed on the mentioned ONIVD Plans:

– the plan must describe the actions of various categories of employees of the System entity in emergency situations to eliminate their consequences and minimize the damage caused;

– the plan must be as independent as possible from a possible accident; it must be operational regardless of what kind of accident occurs;

– The plan must establish those responsible and their responsibilities for carrying out work to restore functionality.

In addition to the Emergency Management and VED Plan, internal documents may be developed, including:

– the purpose of the plan is to protect the information resources of the System subject, ensure the security of information vital to the organization and provide guarantees for the continuity of service provision;

– description of the procedure for preserving (maintaining) the operability of the hardware and software complex and restoring information processing processes in the event of a malfunction of the hardware and software complex and its main components.

10.7.15 In order to carry out activities to ensure the BFPSsubject of the Systemare required to develop a set of documents:

– Regulations on the Information Security Service;

– access control and registration policy;

– Anti-malware policy;

– Internet usage policy;

– backup policy;

– procedure for recording information infrastructure objects;

– document(s) providing for the actions of employees during emergency situations, the procedure for eliminating the consequences of an emergency, the procedure for investigating the causes of an emergency.

10.7.16 Atdevelopment of documents to ensure the BFPSsubject of the Systemmust take into account the requirements of personal law in the field of information protection.

10.7.17 OperatorThe System develops, verifies (tests) and revises an action plan aimed at ensuring the continuity of operations and (or) restoration of operations (the Continuity and Recovery Plan) of the System Operator, at least once every two years.

10.7.18 OperatorThe System develops and includes in the Operations and Management Plan measures aimed at managing the continuity of the System's operation in the event of incidents related to the suspension of provisionpayment infrastructure servicesor violation of established levels of provisionpayment infrastructure services:

– when combining in a payment system the functions of the System Operator and the Operational and (or) Payment Clearing and (or) Settlement Centers - measures to switch to a backup set of software and (or) technical means, as well as measures carried out in the event of inoperability of the systems and services of service providers, the disruption of which may lead to the suspension of the provision of payment infrastructure services;

– if there are two or more Operational and (or) Payment Clearing and (or) Settlement Centers in the System - measures to ensure the interchangeability of the OUPI within 20 (twenty) business days;

– if the System has one attracted Operational and/or Payment Clearing and/or Settlement Center - measures to attract another OUPI and to transfer the System Participants to the services of the newly attracted OUPI for a period of no more than one year, in the following cases: the OUPI exceeds the time for restoring the provision of payment infrastructure services when their provision has been suspended more than twice within three consecutive months or a violation of the System Rules, expressed in the OUPI unilaterally refusing to provide services to the Participant(s) of the System, not related to the suspension (termination) of participation in the System in the cases stipulated by the Rules.

10.7.19 The System Operator organizes the development and monitors the availability of the OUPI's OH&S Plans, their verification (testing) and revision of the OH&S Plans at least once every two years.

The payment infrastructure management plans must include measures to switch to a backup set of software and/or technical means of the payment infrastructure in the event of a suspension of the provision of payment infrastructure services and/or a violation of the established levels of provision of payment infrastructure services, as well as measures taken in the event of the inoperability of the systems and services of service providers, the disruption of which could lead to the suspension of the provision of payment infrastructure services.

10.8 Requirements for risk analysis methods in the System, including risk profiles

10.8.1 The risk analysis methods in the System provide for the following activities:

– formation and maintenance of up-to-date lists of business processes;

– development and maintenance of up-to-date classifiers (structured lists) of risks in the System, risk events, and causes of risk events;

– conducting an analysis of business processes in the System, including an analysis of software and (or) technical means of the OUPI, taking into account the fact that they engage service providers, and other factors influencing the BPFS;

– formation of a list of possible risk events for each business process, indicating the causes of risk events and their consequences;

– determining for each of the identified risks in the System the level of inherent risk before applying risk management methods in the System and establishing the level of acceptable risk;

– comparison of the level of inherent risk prior to the application of risk management methods in the System and the level of acceptable risk for each of the identified risks in the System to determine significant risks in the System;

– application of risk management methods in the System for each of the significant risks in the System, and subsequent determination of the level of residual risk for them after application of risk management methods in the System;

– comparison of the level of residual risk after the application of risk management methods in the System and the level of acceptable risk for each of the significant risks in the System and making a decision on the need to apply other risk management methods in the System in addition to the previously applied methods;

– monitoring risks in the System, including the level of residual risk after applying risk management methods in the System, its compliance with the level of acceptable risk;

– compilation and revision (updating) of the profile of each of the significant risks in the System, including the risk profile of the violation of the BFPS (hereinafter referred to as risk profiles).

10.8.2 The Operator shall prepare risk profiles in accordance with the personal law and shall revise (update) them based on the results of a planned or unscheduled assessment of all risks in the System, as well as an unscheduled assessment of individual risks (individual risks) in the System.

10.8.3 Risk profiles are compiled for all significant risks in the System, including the following risks:

– due to the risk of providing a UPI that does not meet the requirements for the provision of services, due to the failure of the System Subjects to comply with the requirements of the personal law, the System Rules, agreements concluded between the System Subjects, the documents of the System Operator and the documents of the UPI, or due to the presence of legal conflicts and (or) legal uncertainty in the personal law, regulatory acts of the Bank of Russia, the System Rules and agreements concluded between the System Subjects, as well as due to the UPI and the System Participants being under the jurisdiction of different states (legal risk of the System);

– for the risk of the provision of payment infrastructure services that do not meet the requirements for the provision of services, due to the occurrence of failures, breakdowns and accidents in the operation of information and technological systems of the System entities, deficiencies in the organization and implementation of technological and management processes, errors or illegal actions of the personnel of the System entities, or as a result of the impact of events, the causes of which are not related to the activities of the System entities, including emergency situations, erroneous or illegal actions of third parties (operational risk of the System). The sources of operational risk are: deficiencies in information security processes, including deficiencies in the applied technological measures for information security, deficiencies in the application software of automated systems and applications, as well as non-compliance with the requirements for the specified processes of activity by money transfer operators who are Participants and OUPI;

– for the risk of the provision of UPI that does not meet the requirements for the provision of services by the central payment clearing counterparty or the Settlement Center of the System due to the failure of the System Participants to fulfill their contractual obligations to the specified organizations within the established time frame or in the future (the credit risk of the System);

– due to the risk of providing UPI that does not meet the requirements for the provision of services, due to the lack of funds from the central payment clearing counterparty and (or) the Participants of the System that are sufficient for the timely fulfillment of their obligations to other entities of the System (liquidity risk of the System);

– for the risk of providing a UPI that does not meet the requirements for the provision of services, due to the deterioration of the financial condition of the System Operator and (or) the UPI, not associated with the implementation of the credit risk of the System and the liquidity risk of the System (general commercial risk of the System).

10.8.4 The profile of each significant risk in the System must contain:

– A description of risk events identified using at least one method. Risk events are reflected in the profile of each significant risk in the System;

– description of the cause of each risk event;

– description of business processes in which risk events may occur;

– probability of occurrence of risk events. The probability of occurrence of risk events is determined using at least one method from those providedStandard;

– Description and assessment of the possible adverse consequences of each risk event. If a risk event has several possible adverse consequences, all adverse consequences of the given risk event are indicated. The determination of the adverse consequences of risk events is carried out using the methods providedStandardtaking into account the results of the analysis of incident information;

– description of business processes and a list of System Subjects affected by the risk event;

– the level of inherent risk before risk management methods are applied in the System;

– level of acceptable risk;

– the level of residual risk after applying risk management methods in the System;

– list of risk management methods in the System.

The risk profile for a violation of the BFPS is compiled as a consolidated profile in relation to all significant risks in the System.

10.8.5 The System Operator must store the information contained in the risk profiles for at least five years from the date of preparation and revision (updating) of the risk profiles.

10.9 The procedure for information interaction between the subjects of the System for ensuring the BFPS

10.9.1 To ensure the BFPS, the System Operator, the OUPI, and the Participants maintain information exchange. Information exchange occurs through agreed communication channels.

10.9.2 The operator determines the following procedure for information interaction between the subjects of the System to ensure the BFPS.

10.9.3 **Participants and OUPI**are obliged to immediately (no later than the next business day from the moment of detection) notify the Operator of the following events:

– on the occurrence of violations and malfunctions during the operation of the System, or on circumstances that impede the execution of transactions, payment clearing or settlements, resulting in a significant violation of the acceptable level of risk (including cases of system failures);

– on the occurrence of emergency situations;

– about cases or attempts to transfer funds without the client’s consent.

10.9.4 The Operator’s notification (Appendix No. 2) must include the following information:

– time and date of occurrence of the event (if it is impossible to determine the time of occurrence of the event, the time of its detection is indicated);

– a brief description of the event (characteristics of the event that occurred and its consequences);

– the name of one or more business processes during which the incident occurred;

– the name of one or more business processes affected by the incident;

– measures to eliminate the adverse consequences of the incident, indicating the planned and actual duration of these measures (information is provided after such elimination);

– adverse consequences of the event, including: the amount of funds paid by the Operator and/or recovered from the Operator; the amount of funds paid to the OUPI and/or recovered from the OUPI; the number and amount of unfulfilled, and/or untimely executed, and/or erroneously executed orders of Participants, the execution of which was affected by the incident; the duration of the suspension of the provision of payment infrastructure services.

10.9.5 The OUPI promptly informs the System Operator about:

– the presence (absence) of the fact of suspension of the provision of payment infrastructure services;

– the time and date of restoration of the provision of payment infrastructure services in the event of their suspension;

– the date of restoration of the provision of payment infrastructure services that meet the requirements imposed by the System Operator for the provision of services.

10.9.6 The System Operator, immediately upon receipt of a notification from a System entity regarding the occurrence of events and situations, together with the relevant System entities, shall determine a plan of further actions individually for each event and/or situation that has occurred in order to eliminate any operational failures that have arisen, including their consequences, and prevent the occurrence of new ones.

10.9.7 The OUPI shall, on a monthly basis (no later than 5 (five) business days of the month following the reporting month), provide the Operator with a free-form summary of all identified incidents, indicating the number of incidents during the reporting month, the dates of their occurrence/detection, and the values of the BFPS indicators, as well as additional information on incidents at the OUPI's discretion. If there are no incidents during the reporting month, the OUPI shall, within the same period, send the Operator a report containing zero data.

10.9.8 The System Operator informs about cases and reasons for suspension (termination) of the provision of payment infrastructure services:

– The state regulator exercising control and (or) supervision over the Operator in accordance with the personal law notification of suspension (termination) of the provision of payment infrastructure services;

– Participants, OUPI on the day of such suspension (termination) in any of the following ways:

- posting information on the official website of the Systemhttps://kwikpay.ru/
- sending notification via the Agreed Communication Channels.

10.9.9 The operator collects, systematizes, and accumulates information on the occurrence of emergency situations, and also analyzes the causes of disruptions in the functioning of operational and technological means, devices, and information systems, and develops and implements measures to eliminate them.

10.9.10 System Subjects have no right to unreasonably refuse to provide the Operator with requested information. If the requested information contains information constituting a commercial or other legally protected secret of the System Subject, the Operator undertakes to ensure the preservation of such information in accordance with the requirements of personal law.

10.10 Monitoring compliance by the System Subjects with the procedure for ensuring the BFPS

10.10.1 The System Operator verifies compliance by the Payment System Operator and Participants with the procedure for ensuring the BFPS established by these Rules.

10.10.2 To monitor compliance by UPI Operators and Participants with the BFPS procedure, the Operator has the right to request from System entities any information necessary to ensure the BFPS procedure. System entities are obligated to provide the Operator with the requested information within the timeframe specified in the Operator's request.

10.10.3 The operator monitors the compliance of the documents of the OUPI and Participants with the procedure for ensuring the BFPS and, if any discrepancies are identified, sends recommendations for eliminating the identified discrepancies.

10.10.4 Upon detection of a violation of the procedure for providing the BFPS by the OUPI and Participants, the Operator:

– informs the OUPI and Participants about violations identified in their activities and sets deadlines for eliminating the violations;

– carries out an audit of the results of the elimination of violations and informs the OUPI and Participants in whose activities violations were identified about the results of the audit.

10.10.5 The Operator establishes liability for failure to comply with the procedure for ensuring the BFPS for the OUPI and Participants in the Rules, including in agreements with them.

10.11 **The procedure for changing operational and technological means and procedures**

10.11.1 The decision on the need to change operational and technological means and procedures is made by the Operator.

10.11.2 The basis for changing operational and technological means and procedures are:

– inclusion of new types of Transfer transactions or introduction of significant changes to existing transactions;

– replacement or modernization of operational and technological means aimed at improving the quality of the provision of Translation services;

– making changes to the functioning of the risk management system;

– change of the Operator's personal law.

10.11.3 If a change in operational and technological means and procedures requires changes to these Rules, the Operator shall make the appropriate changes in the manner prescribed by these Rules.

10.11.4 If a change in operational and technological means and procedures does not require changes to these Rules, the Operator shall send the Participants a corresponding notice describing the changes no later than 15 (fifteen) calendar days prior to the date of entry into force of the relevant changes.

10.12 The procedure for assessing the quality of functioning of information systems, operational and technological means

10.12.1 The Operator shall evaluate the quality of functioning of information systems, operational and technological means and procedures of the System independently or with the involvement of an independent organization.

10.12.2 To independently assess the quality of functioning of information systems, operational and technological means, the Operator collects primary information from the OUPI:

– information about violations and malfunctions that have arisen during the operation of information systems, operational and technological means;

– results of the self-assessment of the level of BFPS and the level of risk of BFPS violation;

– comparison of calculated values of the risk level with those accepted in the System;

– analysis of the dynamics of changes in the risk level.

In the event that the risk level exceeds acceptable values or there is a negative trend in the risk level, the issue of modernizing or replacing the information systems, operational and technological means used is considered.

10.12.3 The assessment of the quality of functioning of information systems, operational and technological means with the involvement of an independent organization includes the following activities carried out by the Operator:

– making a decision to involve an independent organization;

– selection of an independent organization;

– concluding an agreement with an independent organization;

– providing an independent organization with the information necessary to conduct the assessment;

– performance by an independent organization of work to assess the quality and reliability of the functioning of information systems, operational and technological means;

– receiving a report from an independent organization with the assessment results and recommendations for improving information systems, operational and technological means.

10.12.4 Based on the results of the assessment of the quality of functioning of the operational and technological means and information systems of the System by an independent organization and recommendations for improvement, the Operator makes changes to the functioning of the operational and technological means and procedures of the System in the manner prescribed by these Rules.

10.12.5 The Participant has the right to independently make changes to the operational and technological means and procedures for interaction with the System on the Participant's side, provided that the introduction of such changes does not contradict these Rules, the Participant's personal law, and does not lead to a change in the procedure and type of provision of services within the System.

11. Ensuring information security in the System

11.1 General provisions on information protection in the System

11.1.1 The Rules establish general requirements for the protection of information processed by subjects of the System.

11.1.2 Information security is ensured through the implementation by the System's entities of legal, organizational and technical measures aimed at:

– to maintain confidentiality of information;

– to exercise the right of access to information in accordance with personal law;

– to ensure the protection of information from unauthorized access, destruction, modification, blocking, copying, provision and distribution, as well as from other illegal actions in relation to information.

11.1.3 Each System Subject independently determines the procedure for ensuring information security in accordance with its personal law and the Rules and approves internal documents establishing specific information security requirements and the procedures for their implementation. In the event that the requirements of these Rules conflict with the personal law of a System Subject,

11.1.4 In order to ensure the protection of information in the System, the System Operator:

– develops a list of requirements for ensuring the protection of information in the System, mandatory for all Participants;

– carries out checks of Participants for compliance with the requirements when joining the Rules in a role defined by the Rules, as well as when changing the technological or organizational conditions of the Participant's work;

– carries out checks of Participants in terms of compliance with the requirements for information protection in the System.

11.2 Information protected in the System

11.2.1 The requirements for ensuring the protection of information established by these Rules, when making money transfers, are applied to ensure the protection of the following information (hereinafter referred to as protected information):

– information on completed transfers of funds, including information contained in notifications (confirmations) concerning the acceptance for execution of orders of the System Participants, as well as in notifications (confirmations) concerning the execution of orders of the System Participants;

– information about the balances of funds in bank accounts;

– information contained in the orders of clients of money transfer operators, orders of System Participants, orders of the Payment Clearing Center;

– information stored in the System’s operational centers on completed money transfers using payment cards;

– information on payment clearing positions;

– information necessary to verify clients' right to dispose of funds;

– configuration information that determines the operating parameters of automated systems, software, computing equipment, telecommunications equipment, the operation of which is ensured by the money transfer operator, the payment infrastructure services operator, and used to carry out money transfers, as well as configuration information that determines the operating parameters of technical means for information security;

– key information of cryptographic information protection tools used in money transfers.

11.3 Requirements for ensuring information security

11.3.1 The requirements define the basic principles of information protection and are aimed at minimizing the risks of information security breaches.

11.3.2 Compliance with the requirements for the implementation of Transfers is ensured by:

– selection of organizational measures for information protection; determination in internal documents of the procedure for applying organizational measures for information protection; determination of persons responsible for applying organizational measures for information protection; application of organizational measures for protection; implementation of control over the application of organizational measures for information protection; performance of other necessary actions related to the application of organizational measures for information protection;

– selection of technical means of information protection; determination in internal documents of the procedure for the use of technical means of information protection, including configuration information defining the operating parameters of technical means of information protection; appointment of persons responsible for the use of technical means of information protection; use of technical means of information protection; implementation of control over the use of technical means of information protection; performance of other necessary actions related to the use of technical means of information protection.

11.4 Procedure for ensuring information security in the System.

11.4.1 In order to ensure the protection of information in the System during storage, processing, and exchange of protected information, the subjects of the System ensure the implementation of measures, including, but not limited to, the following:

– compliance with organizational measures to protect information;

– support of vulnerability management program;

– creation and maintenance of a secure network infrastructure;

– network infrastructure monitoring;

– implementation and maintenance of measures to control access to protected information;

– other measures aimed at improving information security.

11.4.2 As part of the implementation of measures to introduce and maintain measures to manage access to protected information, System entities ensure access restrictions and accounting of persons with access to protected information, including:

– ensure access to protected information only to those persons who need such access to perform the functions assigned to them;

– ensure that each employee is provided with access using a unique name, account, password and/or electronic signature verification key to access protected information;

– ensure restricted access to material media containing protected information and strict control over their storage;

– ensure immediate revocation of access upon termination of a person's authority to access protected information.

11.4.3 When using the Internet information and telecommunications network to carry out Transfers, Participants ensure:

– the application of organizational measures to protect information and (or) the use of technical means of protecting information designed to prevent access to the content of protected information transmitted over the Internet information and telecommunications network; unauthorized access to protected information at information infrastructure facilities using the Internet information and telecommunications network; unauthorized access to protected information by exploiting software vulnerabilities;

– reducing the severity of the consequences of impacts on information infrastructure facilities in order to create conditions to prevent the provision of money transfer services or the untimely execution of Transfers;

– filtering of network packets during the exchange of information between computer networks in which information infrastructure objects are located and the Internet information and telecommunications network.

11.4.4 Access to the API is provided using personalized accounts with multi-level roles, including administrator and user. Account passwords must comply with Participants' internal requirements, and the following must be ensured:

— use of at least 8 characters in the password (must necessarily contain: uppercase and lowercase letters, numbers, special characters);

— password change frequency no less than once every 40 days with a ban on using any of the three previous passwords;

— Password protection during storage and operation.

— Passwords for administrative accounts must be changed from the default and meet the following requirements:

— use at least 12 characters in the password (must contain: uppercase and lowercase letters, numbers, special characters);

— the frequency of changing the password is at least once every 30 days, with a ban on using any of the previous passwords;

— Password protection during storage and operation.

11.4.5 The Operator sets the following indicators for the Participant's information security risk level:

	Number of information security breach incidents in the System	Restrictions on the parameters of Transfer transactions in the event of detection of an excess of indicator values

Participants	No more than 3 per quarter	The System Operator may impose restrictions on the amount of a single Transfer transaction.
Settlement centers	No more than 3 per quarter	The System Operator may impose restrictions on the amount of a single Transfer transaction.
Payment clearing center	No more than 3 per quarter	The System Operator may impose restrictions on the amount of a single Transfer transaction.
Operations center	No more than 3 per quarter	The System Operator may impose restrictions on the amount of a single Transfer transaction.
Participants; Settlement centers; Payment clearing center; Operations center	The share of transactions without customer consent is no more than 5% per quarter of the total number of transactions	The System Operator may impose restrictions on the amount of a single Transfer transaction.

11.4.6 The procedure, forms and timeframes for informing the System Operator, Participants and the OUPI about incidents identified in the System related to violations of requirements for ensuring information security when making money transfers, the procedure for interaction in the event of detection of the above incidents in the System.

Incidents in the field of information security include events related to the violation of requirements for ensuring the protection of information when carrying out Transfers, which have led or may lead to the implementation of Transfers without the voluntary consent of the client, or the failure to provide Transfer services.

The System Operator establishes the following requirements for the content, form and frequency of submission of information sent by Participants and the OUPI for the purposes of analyzing the provision of information security in the System when making Transfers, as well as for the purposes of interaction in the event of incidents in the field of information security (information is provided only in relation to activities within the System):

Content	**Form**	**Periodicity**
1) on compliance with the requirements for ensuring information security, including the results of the conducted conformity assessments	an official letter and/or electronic survey conducted by the System Operator	at the request of the System Operator once every three years

2) on the implementation of the procedure for ensuring information security	an official letter and/or electronic survey conducted by the System Operator	at the request of the System Operator once every three years
3) on identified threats and vulnerabilities in ensuring information security	in real time regarding unauthorized access, transactions without the client's voluntary consent - a message by email	When detected
4) on identified incidents related to violations of information security requirements	in real time regarding unauthorized access, transactions without the client's consent - a message by email	When detected

11.4.7 The System Operator defines the following requirements for interaction in the event of incidents related to violations of information security requirements when carrying out Transfers within the System:

Incident	Actions of the Participant, OUPI	Actions of the System Operator
When incidents are detected.	Security: - informing our own information security services about the detection of incidents; - registration of identified incidents; - application of organizational measures to protect information and (or) use of technical means of protecting information designed to identify incidents; - responding to identified incidents, including contacting law enforcement agencies when it is discovered that funds are being transferred on the instructions of persons who do not have the right to dispose of these funds; - analysis of the causes of identified incidents, assessment of the results of incident response; - promptly informing the System Operator about identified incidents in the form of a monthly report; - implementation of restoration of the normal functioning of information infrastructure facilities.	Takes possible and accessible actions in the current circumstances to: — minimizing the consequences of identified incidents; — preventing the possibility of using funds by Recipients when it is discovered that funds are being transferred on the instructions of persons who do not have the right to dispose of these funds; — verification of compliance with information security requirements on the System Operator's side and compliance with requirements for processing transfers; — informing the Participant and the Settlement Center about the results of the actions taken.
Upon detection of a fact of compromise of key information of cryptographic information protection tools used in the implementation of Transfers.	Informing the System Operator via the Agreed Communication Channels.	Blocks the Participant's ability to make transfers in the System.
When malicious code is detected or the fact of exposure to malicious code is detected.	Ensure that measures are taken to prevent the spread of malicious code and eliminate the consequences of its impact. If necessary, money transfers are suspended for the period of eliminating the consequences of infection by malicious code, as well as the consequences of other impacts. Provide prompt information to the System Operator via the Agreed Communication Channels.	Suspends settlements with the involved Settlement Center, also temporarily suspending the work of the Participant making settlements through it. In case of problems in the functioning of the System, it sends out notifications via the Agreed Communication Channels. In the event of detection of malicious code or the fact of exposure to malicious code within the System, the Operator shall inform the Participant and the involved Settlement Center via the Agreed Communication Channels.

11.4.8 The System Operator ensures the recording and availability of information for the System Participant and the OUPI:

– on incidents identified by the System Operator related to violations of requirements for ensuring information security when making money transfers;

– information is sent through agreed communication channels on a monthly basis in the presence of incidents; the absence of sent information is considered to be the absence of incidents;

– on the methods of analysis and response of the System Operator to incidents related to violations of requirements for ensuring information security when making money transfers;

The analysis methodology consists of collecting, summarizing information, and analyzing information on the causes of incidents for compliance with the requirements of Regulation No. 821-P of the System Rules;

The incident response methodology is described in Section 12 of these Rules.

The System Operator, based on the accumulation and consideration of experience in responding to information security incidents and restoring the functioning of the System after their implementation, in order to reduce the risk of information security, implements improvement mechanisms in terms of ensuring the accounting and availability of information for money transfer operators who are Participants and UPI operators:

– on information security incidents identified in the payment system;

– on methods of analyzing and responding to information security incidents.

12. Use of cryptographic information protection tools

12.1 The Rules, as well as the agreements concluded between the subjects of the System, use cryptographic information protection tools (encryption) or software and hardware containing modules of cryptographic information protection tools (hereinafter referred to as CIPF) to protect information.

12.2 The internal documents of the Participants must define and implement the procedure for using the cryptographic information protection tool, including:

– the procedure for commissioning, including procedures for integrating cryptographic information protection tools into automated systems used to carry out money transfers;

– procedure for operating the cryptographic information protection tool;

– the procedure for restoring the functionality of cryptographic information protection tools in cases of failures and (or) malfunctions in their operation;

– the procedure for making changes to the cryptographic information protection tool software and technical documentation for the cryptographic information protection tool;

– procedure for decommissioning of cryptographic information protection tools;

– key system management procedure;

– the procedure for handling cryptographic key carriers, including the procedure for applying organizational information security measures and using technical means of information security designed to prevent unauthorized use of cryptographic keys, and the procedure for actions in the event of a change or compromise of keys.

12.3 The security of the processes for producing cryptographic keys for cryptographic information protection tools is ensured by a set of technological information protection measures, organizational information protection measures, and technical means of information protection in accordance with the technical documentation for the cryptographic information protection tools.

13. The procedure for providing information about their activities to the Operator by Participants and OUPI

13.1 Participants are obligated to provide the Operator with information about their activities within the System in the manner and within the timeframes specified by the Rules and in accordance with individual requests from the Operator. Direct Participants provide information, including information on all their Indirect Participants, Partners, and other third parties. UPPIs are obligated to provide the Operator with information about their activities within the System in the manner and within the timeframes specified in the agreement/contract between the Operator and the UPPI and in accordance with individual requests from the Operator. The deadline for UPPIs to provide information about their activities within the System is 7 (seven) business days from the date of receipt of the relevant request, unless otherwise specified in the agreement/contract between the Operator and the UPPI.

13.2 The Participant, as well as the OUPI, provides the Operator with a report in any form on incidents.

The Report includes information on incidents identified in the system related to violations of information security requirements when making money transfers:

- description of the incident mechanism indicating the causes of its occurrence;
- description of violations of the System's requirements in the field of information security that contributed to the incident;
- a description of the possible goals of the criminals and the extent to which they were achieved;
- description of the identified damage to the parties to the relationship;
- description of corrective measures to prevent similar incidents from occurring in the future.

13.3 The incident report shall be submitted to the Operator monthly via the agreed communication channel, no later than the 5th (fifth) working day of the month following the reporting month.

14. Responsibility of Participants and the OUPI System

14.1 The Participant, Partner, and OUPI are responsible for the proper implementation of these Rules.

14.2 The Operator has the right to demand from the Participant, the OUPI, who has violated its obligations, payment of the penalty accrued:

— at double the LIBOR rate in effect during the period of default on the outstanding amount of debt, expressed in foreign currency, for each day of delay in payment up to and including the date of repayment of the debt.

14.3 Damages caused by late fulfillment of obligations in excess of the penalty will not be compensated.

15. Permissiondisputes

15.1 The procedure for interaction within the System in controversial situations, the procedure for pre-trial resolution of disputes between subjects of the System.

15.1.1 Between the Operator and the Participants and between the Operator and the OUPI, between the Participant and the OUPI - about the occurrence and/or existence of a controversial situation, this Subject (hereinafter referred to as the initiator) immediately notifies the other interested party about the possible occurrence and/or existence of a controversial situation, the circumstances indicating its occurrence or existence, as well as its presumed causes.

15.1.2 The subjects of the System to whom a notice of a dispute has been sent and who are participating in the resolution of the dispute (hereinafter referred to as the disputing parties) are obliged, no later than within the next 5 (five) working days, to verify the presence of the circumstances specified in the notice and, if necessary, to take measures to resolve the dispute on their part.

15.1.3 The review of claims includes an examination of circumstances that allow us to establish whether Participants have fulfilled (or failed to fulfill) their duties and obligations under these Rules. The Operator reserves the right to request from any Participant any information necessary to clarify these circumstances.

15.2 The procedure for resolving disputes in court.

15.2.1 In the event that it is impossible to resolve disputes and disagreements regarding a controversial situation in the working order, based on the results of the commission's work or through the claims procedure, the resolution of disputes and disagreements regarding the conflict situation is referred for consideration in accordance with the agreements between the subjects of the System.

16. Procedure for monitoring compliance with the Rules

16.1 The Operator shall monitor compliance with these Rules by Participants and the OUPI on an ongoing basis by monitoring the activities of the System entities in the process of providing services within the System.

16.2 Methods of implementing control.

16.2.1 The Operator monitors compliance with the Rules in the following ways:

– requests and receives from the subjects of the System primary information and documents concerning the activities of the subjects of the System;

– accepts and considers requests received from Clients, Participants, and UUPI regarding the actions (inactions) of Participants in the provision of Services;

– carries out checks of the activities of Participants within the System at Customer service points, including without prior notification of Participants;

– carries out actions and applies enforcement measures in accordance with these Rules in the event of a violation by Participants and (or) the OUPI of the obligations they have assumed in accordance with these Rules.

16.3 Actions of the Operator upon detection of cases of violation of the Rules:

16.3.1 In cases where violations of the requirements of these Rules by subjects of the System do not affect the BFPS, and also do not affect the services provided to Participants and their Clients, the Operator shall carry out the following actions:

– notifies the System subject of the identified violation in writing, indicating the violation committed and the period within which such violation must be corrected, while the specified period cannot be less than 5 (Five) working days;

– sends recommendations to the System entity on how to eliminate the identified violation and recommends that they submit to the Operator a program of measures aimed at eliminating the violation;

– exercises control over the elimination of the identified violation by the System entities within the time period specified in the notification.

16.3.2 In cases where violations of the requirements of these Rules by subjects of the System affect the BFPS or the services provided to Participants and their Clients, the Operator shall apply one of the following enforcement measures:

– sends an order to eliminate the violation, indicating the time period for its elimination;

– restricts (suspends) the provision of operational services and (or) payment clearing services;

– sends a notice of suspension (termination) of the Participant's participation in the System.

16.4 Enforcement measures are imposed based on a notice sent by the Operator. The notice identifies the violation and specifies the timeframe within which it must be corrected.

16.5 In the event of repeated failure to comply with notifications requiring the elimination of a violation affecting the BFPS, within one year from the date of the first notification sent by the Operator to eliminate such violation, the Operator has the right to terminate the Participant's participation in the Payment System in accordance with the terms of suspension and termination of participation in the Payment System established by the Rules.

17. Change of Rules

17.1 The Operator has the right to unilaterally make any necessary changes to these Rules.

17.2 The Operator shall provide Participants with the opportunity to review the proposed changes in advance and send their opinion to the Operator via the Agreed Communication Channels within one month from the date of posting the proposed changes on the Operator's website in the Internet information and telecommunications network.

17.3 The period for entry into force of amendments to the Rules is one month from the date of expiration of the period for posting the proposed amendments for preliminary review.

17.4 Changes to the Rules are approved by the Operator and communicated to the Participants by posting a new version of the Rules on the Operator's website in the Internet information and telecommunications network.

18. Interaction with other payment systems.

18.1 The system can interact with other payment systems on the basis of concluded agreements on interaction between payment system operators.

18.2 The System Operator maintains a list of payment systems with which interaction takes place and keeps it up to date.

18.3 The procedure for interaction with the involved payment systems (hereinafter referred to as PPS):

18.4 Information interaction between the System and the PPS is carried out in accordance with agreements on interaction with the PPS.

18.5 The PPC settlement of the payment clearing position is performed by the Payment Clearing Center for each trading day at the end of the trading day that is a business day. If a trading day is not a business day, the settlement of payment clearing positions for such a trading day will be performed on the following trading day that is a business day.

18.6 Settlements are carried out by the System Settlement Center with the PPS Settlement Center in the amount of amounts determined on a net basis of payment clearing positions in the relevant currencies.

18.7 Information on the specific amount of the PPS commission is established in the agreement on interaction with the PPS.

18.8 The procedure for interaction with payment systems, including payment clearing, and settlements, defined in this section applies to all PPS, unless a different procedure is specified in the agreement on interaction with the PPS.

19. Sanctions policy (sanctions clause).

19.1 **Sanctioned person-** any person who is subject to Blocking Sanctions or a general prohibition on transactions (i.e. any person with whom any transactions are generally prohibited by the Sanctions), including as a result of such person: (a) being included on (i) the Specially Designated Nationals List maintained by the Office of Foreign Assets Control of the United States Department of the Treasury (OFAC); (ii) the United Kingdom Sanctions List maintained by the Office of Financial Sanctions Enforcement (OFSI); (iii) the European Union Consolidated List of Financial Sanctions; (iv) the United Nations Security Council Consolidated List; and/or (v) any other list of persons subject to Blocking Sanctions maintained by any specified sanctions authority; or (b) is owned (by 50% or more) or controlled by (or otherwise acts on behalf of) one or more persons subject to Sanctions.

19.2 **Sanctions**— these are mandatory regulatory acts that provide for special economic measures of a restrictive nature in the form of a ban on certain actions aimed, inter alia, at freezing assets, blocking accounts, prohibiting exports, re-exports (supplies of technologies and equipment), on transactions with certain persons and/or in certain areas, and other restrictions that may be introduced by the Council and the Commission of the European Union (hereinafter referred to as the EU, a list of which is available at the following Internet address:https://www.eeas.europa.eu/eeas/european-union-sanctions_en), His Majesty's Government (including the Secretary of State, HM Treasury and the Office of Financial Sanctions Inspectorate (OFSI), a list of which can be found at:http://www.hm-treasury.gov.uk/d/sanctionsconlist.htm; The United Nations (hereinafter referred to as the UN, a list of which is available at the following Internet address:https://www.un.org/securitycouncil/content/un-sc-consolidated-list; and the Government of the United States of America, including the Office of Foreign Assets Control (OFAC) of the US Department of the Treasury (hereinafter referred to as the US, a list of which is available at the following Internet address: https://ofac.treasury.gov/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists.

19.3 Sanctions clause.

19.3.1 The Parties acknowledge the possibility of applying Sanctions to the Parties and/or to their relations related to the implementation of the Rules.

19.3.2 The Parties represent and warrant that: (i) the Party, as well as its shareholders/participants, ultimate beneficiaries, group companies, affiliates, members of collegial bodies and/or sole executive body are not Sanctioned Persons; (ii) does not engage in any direct transactions or operations with any person subject to Sanctions, including export, import, delivery, sale or provision of services to Sanctioned Persons, to the extent that such activities violate the Sanctions; (iii) does not enter into the Agreement for the purpose of circumventing the Sanctions or for the benefit of persons subject to Sanctions, or for the provision of financing to them.

19.3.3 A party has the right to unilaterally and extrajudicially refuse to perform the Agreement and demand compensation for damages in the event that:

— the representation in accordance with these Rules was false at the time of submission or becomes invalid after the date of accession to the Rules, including if the Party commits violations of the Sanctions;

— after the date of accession to the Rules, Sanctions will be imposed on the Party, including inclusion in the sanctions lists of jurisdictions specified in the definition of the term Sanctions.

19.3.4 The parties may negotiate and discuss the possibility of changing or terminating obligations under the Rules in a manner that does not violate the Sanctions.

19.3.5 In the event that obligations can be fulfilled ahead of schedule without violating the Sanctions, a Party has the right to demand that other Parties fulfill all or part of their obligations ahead of schedule.

20. Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Policy

20.1 Participants are obliged to comply with the requirements of the current personal law in the area of combating money laundering and terrorist financing and to implement the measures (hereinafter referred to as “countermeasures”) provided for by the Participant’s personal law, but at a minimum, the Client is not:

— a person included in the lists of organizations and individuals associated with terrorism or the proliferation of weapons of mass destruction, compiled in accordance with decisions of the UN Security Council.

20.2 Participants servicing the Sender, when carrying out Transfers at all stages of their implementation, are obliged to ensure control over the availability, completeness, transfer as part of payment documents or by other means, compliance with the information available to the Participant, as well as storage for at least 5 years from the date of termination of relations with the Client (from the date of the Transfer) of the following information:

— about the Sender - an individual: last name, first name, patronymic (unless otherwise provided by law or national custom), unique assigned transaction number (if any), taxpayer identification number (if any) or address of place of residence (registration) or place of stay;

— about the Sender - a legal entity: name, unique assigned number (code, password) of the transaction, taxpayer identification number or foreign organization code.

20.3 If the Client is not personally present for the purposes of identification, the Participants are obliged to ensure reliable identification of this Client by other adequate measures provided for by the Participant’s personal law.

20.4 Third parties involved in the implementation of Transfers by Participants must meet the following requirements:

— mandatory professional registration and licensing required by the personal law of that third party;

— application of due diligence measures to Clients of the specified third parties;

— maintaining records on countermeasures provided for by the personal law of the specified third parties and these Rules;

— provision by the said third parties to the Participants, upon request, of the latter's necessary documents or other information required by the latter or required from the latter by authorized bodies in accordance with countermeasures.

20.5 Participants are obliged to refrain from making Transfers in cases where they have sufficient and justified assumptions that the Transfer is made for the purpose of laundering proceeds from crime or financing terrorism.

20.6 Participants shall not have the right to disclose to Clients information on the procedure for the implementation of countermeasures by Participants, including the transfer of information about Clients or Transfers to state authorized bodies for the implementation of countermeasures.

These Rules are accompanied by appendices, which are part of these Rules:

- Appendix No. 1. Application for participation in the UniUni.Market Money Transfer Payment System as a Direct Participant;
- Appendix No. 2. Form for informing the Operator System subject about money transfers identified in the UniUni.Market Payment System;
- Appendix No. 3.List of payment systems with which interaction is carried out.

Appendix No. 1. Application for participation in the UniUni.Market Money Transfer Payment System

To the Payment System Operator
money transfers "UniUni.Market"
UNIUNI PAYMENTS TECHNOLOGIES - FZCO
From____________________________
____
Address:_________________________

Statement
to participate in Ppayment system
money transfers "UniUni.Market"
as a Participant

____

(full name of the organization)

represented by ____________________________, acting on the basis of __________________, hereinafter referred to as the Applicant, sends to the operator of the Payment system of money transfers "UniUni.Market" UNIUNI PAYMENTS TECHNOLOGIES - FZCO, hereinafter referred to as the Operator, this application for participation in the Payment system of money transfers "UniUni.Market" as a Participant, for which, the Participant:

- simultaneously with the application, provides the Operator with the documents stipulated by the Rules of the Payment System of Money TransfersUniUni.Market
- confirms that he/she has read the Rules of the Payment System of Money TransfersUniUni.Market, posted on the websiteOperatorin the Internet information and telecommunications network;
- hereby declares its agreement with the specified Rules and confirms the ability to comply with all requirements of the Operator;
- signs a confidentiality agreement.

The Applicant understands and agrees that the fact of receipt of this Application by the Operator does not entail automatic connection of the Applicant to the Money Transfer Payment System.UniUni.Marketand does not impose any obligations on the Operator.

On behalf of the Applicant:

____

(position, full name, signature)

Form for informing the Operator about incidents identified in the UniUni.Market Money Transfer Payment System

N p/p	Incident details	Description
1	Name and status of the System Subject	
2	Date and time of occurrence/detection of the incident	
3	Brief description of the incident (characteristics and consequences)	
4	Name of the business process during which the incident occurred	
5	Name of the business process affected by the incident	
6 *	The presence (absence) of the fact of suspension (termination) of the provision of payment infrastructure services as a result of an incident	
7 **	Impact of the incident on the BFPS	
8 **	The degree of impact of the incident on the functioning of the System depending on the number of OUPI, and (or) the number and significance of Participants who were directly affected by the incident, and (or) the number and amount of unfulfilled, and (or) untimely fulfilled, and (or) erroneously fulfilled orders of Participants, and other factors	
9 *	Date and time of restoration of provision of payment infrastructure services in case of suspension of their provision	
10	Measures to eliminate the adverse consequences of the incident, indicating the planned and actual duration of these measures;	
11 *	The date of restoration of the provision of payment infrastructure services that meet the requirements for the provision of services;	
12	Adverse consequences of the incident for the Subjects, including:	
12.1	- the amount of money paid by the Operator and (or) collected from the Operator	

12.2	- the amount of money paid to the OUPI and (or) collected from the OUPI	
12.3	- the number and amount of unfulfilled, and (or) untimely fulfilled, and (or) erroneously fulfilled orders of Participants, the execution of which was affected by the incident	
12.4 *	- the duration of the suspension of payment infrastructure services	

Information on items 1-5, 10, 12, 12.1, 12.2, 12.3 is provided by all subjects of the System.

* Information on paragraphs 6, 9, 11, 12.4 is additionally provided by the OUPI.

**Information under items 7 and 8 is filled in by the System Operator.

List of payment systems with which interaction is carried out