



ADOPTED
by the Resolution of the NSPK JSC Supervisory
Board (Minutes No. 64 dated 28 June 2022)
Effective date 29 June 2022

Mir Payment System Regulations

P.070

Version 4.0

The official language of the “Mir Payment System Regulations” (Version 4.0, Moscow 2022) is Russian. This English language text is not an official translation and is provided for information purposes only.

In the event of any discrepancies between the English version and the Russian original, the Russian original shall prevail. The recipient is solely responsible for the use of the information contained herein

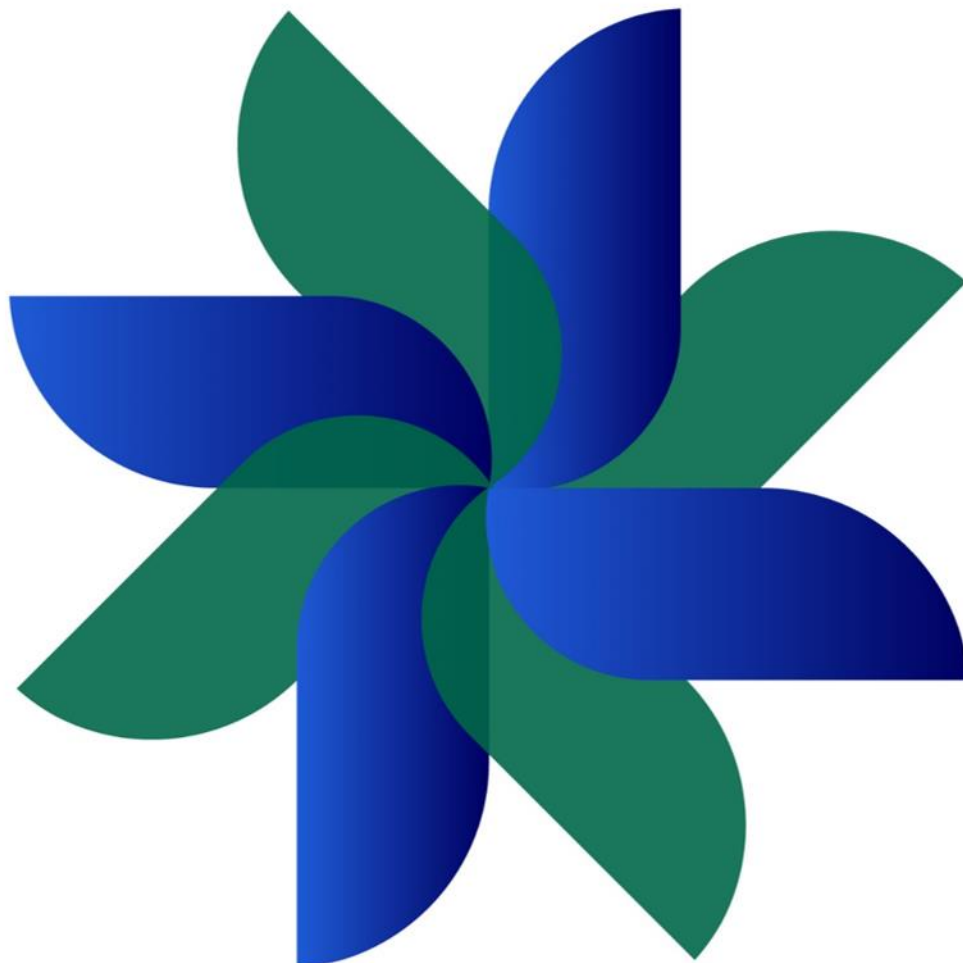


Table of Contents

1. General Provisions	6
1.1. Introduction	6
1.2. Procedure for Changing the Mir Regulations and Standards	7
1.3. System Subjects.....	7
1.3.1. Operator.....	7
1.3.2. Payment Infrastructure Service Providers.....	7
1.3.3. Participants.....	8
2. Confidentiality	9
3. Trademarks, Service Marks, and Logo Usage Guidelines	11
4. Interaction Between System Subjects	13
4.1. Operator’s Rights and Obligations	13
4.2. Operations Center's Rights and Obligations.....	15
4.3. Payment Clearing Center's Rights and Obligations	16
4.4. Settlement Center's Rights and Obligations	17
4.5. Central Payment Clearing Counterparty’s Rights and Obligations.....	18
4.6. Participants’ Rights and Obligations	18
4.6.1. Direct Participants	18
4.6.2. Indirect Participants	24
4.6.3. Participant Payment Systems	28
5. Procedure for Maintaining the List of Payment Infrastructure Service Providers and the List of Participants	32
6. Procedures of Entry (Accession) to and Secession from Mir Payment System	33
6.1. System Participation Criteria.....	33
6.2. System Participant’s Activity Type.....	35
6.3. System Entry (Accession) Procedure	36
6.4. System Participation Suspension and Termination Procedure.....	38
6.4.1. Suspension of Participation in the System at the Participant’s Initiative.....	38
6.4.2. Termination of Participation in the System at the Participant’s Discretion.....	39
6.4.3. Suspension of Participation at the Operator’s initiative.....	40
6.4.4. Termination of Participation at the Operator’s initiative	42
6.4.5. Termination of Participation in the System in the Event of Revocation (Cancellation) of RF Participant’s License for Banking Operations or Removal by the Bank of Russia of the Participant System’s Operator from the Payment System Operator Register	44
6.4.6. Termination of Participation in the System in the Event of Revocation (Cancellation) of Non-RF Participant’s Permit.....	45
7. Issuing	48

7.1. Issuing Participant's (Issuer's) Rights and Obligations	48
7.2. Types and Features of the System Products	50
7.3. BIN Assignment	50
7.4. Requirements for Storage, Transfer and Destruction of Cards	51
7.5. Requirements for the Issuer's Agreement with the Customer	52
8. Acquiring	54
8.1. Acquiring Participant's (Acquirer's) Rights and Obligations	54
8.2. Transaction Types	57
8.3. Transaction Performance Procedure	60
8.3.1. Transaction Performance Environment.....	60
8.3.2. Transaction Amount.....	60
8.3.3. Authorization.....	60
8.3.4. Cardholder Authentication Procedure	61
8.3.5. Additional Requirements to Purchase Transaction and Cash Disbursement Transaction	62
8.3.6. Additional Requirements to Card-to-Card Transactions and Cash-to-Card Transactions	62
8.3.7. Additional Fees	63
8.3.8. Refund Transactions.....	63
8.4. Source Documents. Requirements to Contents and Storage	64
8.5. Retained and Recovered Cards.....	66
8.6. Acquirer's Relationship with Merchants.....	67
8.7. Requirements to Merchant Agreements	67
8.8. Requirements to Card Acceptance (Servicing) Points	68
8.9. Procedure for Acceptance (Servicing) Cards Issued by the Bank of Russia within the Participants' Card Acceptance Network	69
9. Funds Transfer Procedure.....	70
9.1. Non-Cash Transactions	70
9.2. Support of Transactions with the Payer Details if They are not Provided in the Order of the Participant's Customer	70
9.3. Funds Transfer and Settlement Currency in the System	70
9.4. Transaction Performance in the System. General Procedure	71
9.5. System Payment Clearing Procedure	72
9.6. Processing and Verification of Payment Orders Received from the Participants.....	73
9.7. Calculation of Clearing Positions.....	74
9.8. Net Position Log Generation and Submission to the Settlement Center and/or the Central Payment Clearing Counterparty	75
9.9. Payment Clearing Reports Generation and Submission to the Participants Based on the Payment Clearing Results	75
9.10. Settlements.....	75

9.10.1. Procedure for Settlement with the Use of the Participant's Account Opened with the Settlement Center	75
9.10.2. Procedure for Settlement with the Non-RF Participant conducting settlement without the Participant's Account opening with the Settlement Center	78
10. System Functioning Time Specifications	80
11. Collateral for Participants' Obligations	82
11.1. General Provisions	82
11.2. Participant's Limit	82
11.3. Guarantee Fund	83
11.4. Independent Guarantee	87
11.5. Other Means for Collateral of Participant's Obligations	89
12. Funds Transfer and Payment Infrastructure Services Payment Procedure	91
12.1. Procedure for Documents Exchange via SEDO and Hard-Copy Documents Exchange	92
12.2. Procedure for Exchange of Hard-Copy Documents Only	94
12.3. Electronic Documents Exchange Procedure	95
12.4. Fees and Procedure of Payment for the Settlement Center's Services	98
13. System Services	99
14. Stop List	101
15. Card Fraudulent Transaction Information	102
16. Participant Compliance	103
16.1. Procedure for Monitoring the Participants' Compliance with the Regulations	103
16.2. Procedure for Monitoring the Payment Infrastructure Service Providers' compliance with the Regulations	105
17. Liability for Non-Compliance	107
18. System Business Continuity (BC) Procedure	112
18.1. General Provisions	112
18.2. System Risk Management	113
18.2.1. System Risk Management Model	114
18.2.2. Operator's Risk Management Organizational Structure	114
18.2.3. Risk Management Collective Body	115
18.2.4. Types of Risks in the System	115
18.2.5. SBC Parameters	118
18.2.6. Risk Analysis Methods	119
18.3. System Business Continuity Management	127
18.4. Organization of Interaction with Payment Infrastructure Service Providers and Participants to Ensure SBC	129
18.5. Control over the Payment Infrastructure Service Providers' and Participants' Adherence to the SBC Procedure	132

18.6.	Risk Management System Assessment Procedure	132
18.7.	Procedure for Assessment of Quality and Reliability of Information Systems and Operational and Technological Means by the Third Party Organization.....	133
19.	Data Security Requirements	134
20.	Electronic Document Management System (SEDO)	136
21.	Personal Data.....	137
22.	Interaction Procedure in Exceptional Situations	138
23.	Warranties and Representations	139
24.	Anti-Corruption Undertaking	141
25.	Governing Law. Dispute Resolution.....	142
26.	Participants' Reporting Procedure	144
27.	Interaction with Partner Payment Systems.....	145
28.	Procedure of interaction with the payment system of the Bank of Russia for the purposes of funds transfer using the Faster Payment System of the payment system of the Bank of Russia	146

Appendices to the Regulations:

Appendix 1. Terms and Definitions

Appendix 2. Accession to the Mir Payment System Regulations. Application Form

Appendix 3. Participant's Guarantee Fee Calculation Method

Appendix 4. Fees

1. General Provisions

The Mir Payment System Regulations (hereinafter referred to as the Mir Regulations or the Regulations) regulate the terms and conditions of participation in the System, funds transfer, provision of payment infrastructure services, as well as the informational, technological, and financial interaction between the System Subjects, and set forth the rights, liabilities and functions of the System Subjects.

The terms and definitions used in this document shall be provided in Appendix 1 hereto.

All terms and definitions used herein in the singular, where the context so permits, shall be deemed to include the plural and vice versa.

1.1. Introduction

The Mir Payment System is an aggregate of entities, including the Operator, Payment Infrastructure Service Providers and Participants, interacting under the Mir Regulations for the purpose of funds transferring.

The purpose of the Mir Payment System establishment is to ensure continuity, efficiency and accessibility of funds transfer services rendering with the use of payment cards and other electronic payment instruments being provided to Customers by the Participants in accordance with the Mir Regulations.

The Regulations have been developed in accordance with the requirements of Federal Law No. 161-FZ dd. June 27, 2011 *On the National Payment System* and other legal acts and regulations of the Russian Federation. The Regulations are deemed to be an agreement. The Regulations do not constitute a public offer.

Participants shall accede to the Mir Regulations in accordance with the procedure set forth herein. Accession to the Regulations shall mean the acceptance of the Mir Regulations and Standards by the Participant in their entirety, without any exceptions or limitations.

The Mir Payment System Regulations and Standards shall be binding for all System Subjects.

The Regulations, including the Mir Fees and the *Mir Interchange Fees* Standard that sets forth the interchange fee rates and the fee charging procedure (hereinafter, the *Interchange Fees* Standard), shall be publicly available on the Operator's official Internet website at www.nspk.ru.

The Mir Payment System Standards shall be posted on the System's Information Resource.

The document flow between the Operator and Participants (including submission of documents, letters, reports, etc.) shall be performed in Russian and(or) English.

Business days in the Regulations shall mean business days in compliance with the laws of the Russian Federation, unless otherwise stated herein.

1.2. Procedure for Changing the Mir Regulations and Standards

The Operator shall be entitled to unilaterally change the Regulations as follows.

The Operator shall provide an opportunity for the Participants to preview the pending changes to the Regulations and provide their feedback to the Operator using the Mir System's Information Resource during one month from the date of the draft amendments posting on the Operator's official System Information Resource.

The Operator shall notify the Participants of all the duly approved changes to the Regulations by posting a respective notice on the Operator's official website at www.nspk.ru. The effective date of these changes duly approved by the Operator cannot be earlier than one month from the last date of the preview period allotted to the Participants to become familiar with the changes and to provide their feedback to the Operator. Such notices shall have the same legal force as the Regulations.

The Operator shall have the right to unilaterally change the System Standards. The operator shall notify the Participants of any changes to the System Standards by posting a respective notice on the System's Information Resource.

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

1.3. System Subjects

1.3.1. Operator

The Operator sets forth the Mir Payment System Regulations and Standards and performs other actions as stipulated by the laws of the Russian Federation, other regulatory legal acts of the Russian Federation, and the present Regulations.

The Mir Payment System Operator is National Payment Card System Joint-Stock Company (NSPK).

1.3.2. Payment Infrastructure Service Providers

NSPK shall perform the functions of the Operations Center and the Payment Clearing Center in the System.

The functions of the System Settlement Centers shall be performed by:

1. The Bank of Russia in accordance with cl. 2, Article 30.6, Federal Law No. 161-FZ dd. June 27, 2011 *On the National Payment System* for rendering the settlement services in relation to card transactions between:

- RF Participants;
- RF Participants and Non-RF Participants (excluding Foreign Payment Service Providers).

2. VTB Bank (PJSC) for rendering the settlement services to Non-RF Participants in accordance with the agreement signed with the Operator.

The functions of the Settlement Centers may also be performed by credit organizations, VEB.RF, a foreign bank (foreign credit organization), foreign central (national) bank, and international financial organization engaged by the Operator for the purpose of settlement services rendering in relation to Card Transactions performed between Non-RF Participants. The specified organizations shall have a valid license (permit) if such a license (permit) is required in accordance with the applicable laws.

The functions of the Central Payment Clearing Counterparties in the System shall be performed by the Bank of Russia and VTB Bank (PJSC) in accordance with the relevant agreements signed with the Operator. A credit organization or VEB.RF may also act as the Central Payment Clearing Counterparty in accordance with the relevant agreement signed with the Operator.

1.3.3. Participants

The System shall provide for the following Participant statuses:

- Individual Participants:
 - Direct Participants;
 - Indirect Participants;
- Participant Payment Systems.

The Participant shall issue Cards and/or perform Card Transactions processing in accordance with the laws of the Russian Federation or laws applicable to the Participant, and the System Regulations and Standards.

2. Confidentiality

Confidential information shall mean any restricted information, including trade secrets of the System Subjects, insider information, as well as any other System Subject's proprietary information, regardless of the form of its provision, provided by the disclosing Party to the receiving Party.

To ensure confidentiality, integrity and non-repudiation of information within the System, its Subjects shall use the System's electronic document management system (SEDO) and secure communication channels that ensure secure (encrypted) transmission of documents electronically signed by the Party that generated the document during the information exchange between the System Subjects.

Any communication of confidential information via open communication channels shall be prohibited.

The receiving Party shall not be entitled to disclose or otherwise provide confidential information to third parties without a written consent (permission) of the disclosing Party except as required by the laws of the Russian Federation and the Regulations, and(or) laws applicable to the Participant.

The System Subjects shall maintain confidentiality of the information used and received when acting in the System, and shall be entitled to communicate it to their employees, who need such information for work in the System and who are allowed to work with confidential information, at their own discretion and when reasonably required without obtaining prior written consent of the disclosing party.

The receiving Party shall be responsible for actions (or negligence) of their employees and other persons who have been given access to confidential information.

The receiving Party shall be responsible for any disclosure of confidential information, as well as for any unauthorized use of confidential information, that occurred due to its fault.

The receiving Party shall indemnify the disclosing Party for damages incurred as a result of disclosure of confidential information or its unauthorized use that occurred due to the receiving Party's fault.

The System Subjects agree that any activities by the Operator, the Operations Center and the Payment Clearing Center related to information processing and storage including for the purposes of the information and analysis findings (reports, research opinions and other statistics) generation and use by the Operator, Participants and third parties, development and management of programs, including programs aimed at promotion of Cardholder's active use of Cards, organization of marketing activities and promotions, including personalized offers, do not violate System Subjects' rights with respect to such information and confidentiality requirements.

The Participants shall not to disclose any information regarding the availability and(or) the content of software, technical and other solutions used in the System to any third party without prior written consent of the Operator.

In the event of the disclosing Party's (the System Subject) secession from the System, as well as at any time upon the disclosing Party's request, the receiving Party shall be obliged to return to the disclosing Party, in accordance with a handover certificate, all previously received confidential information, including all copies, any reports, analyses, certificates, extracts, reproductions and other materials containing confidential information (both hard and soft copies), held by the receiving Party and by any persons, to whom such confidential information had been disclosed in accordance with the Regulations. Such information shall be returned within five (5) business days from the date of receipt of the disclosing Party's notice of confidential information return. If it is impossible to return such information, the receiving Party shall destroy it and submit to the disclosing Party a destruction certificate within five (5) business days from the date of receipt of the disclosing Party's notice of confidential information destruction. If it is impossible to return and (or) destroy confidential information within the period specified above, this period shall be changed as agreed by the Subjects.

The non-disclosure obligation of any System Subject shall survive any secession from the System for any reason and remain valid within five (5) years starting from the date of the System Subject's secession.

The Provisions of this Section shall not be applicable to the Bank of Russia that performs the functions of the Settlement Center and the Central Payment Clearing Counterparty for the System. Any arrangements between the Operator and the Bank of Russia for the receipt, storage, use and transfer of confidential information shall be regulated by a separate agreement between the Operator and the Bank of Russia.

3. Trademarks, Service Marks, and Logo Usage Guidelines

The Operator shall be the rightholder of the System trademarks (service marks) designed for the individualization of Mir Cards, the Card acceptance network, and the services/works being rendered/performed within the System. The Operator shall establish the requirements to the Card design and System trademarks (service marks) and logos usage standards to ensure the integrity, security and protection of the use of the System trademarks (service marks) and logos.

The placement procedure and terms of use of System trademarks (service marks) and logos shall be provided in the System Regulations and Standards.

The right to use the System trademarks (service marks) shall be granted to the Participant under the license agreement (contract) entered into by and between the Participant and the Operator.

The Participants are entitled to post information about System and (or) Cards promoting events on their resources including the Internet with consideration of rules specified below.

The Participants shall be obliged to:

- place the System trademarks (service marks) and logos on Cards being issued by them;
- ensure the placement of the System trademarks (service marks) and logos on all Card transactions processing devices and at Cardholder service points, including on the Internet, to inform them about the possibility to perform Card transactions;
- submit for the Operator's approval all the materials created by them (or on the Participant's behalf) that contain a reference to or a mention of the System name and/or use of the System trademarks (service marks), and (or) the System logos;
- discontinue any use of the System trademarks (service marks) and logos upon termination of the System participation and/or termination of license agreement for the right to use System trademarks (service marks) concluded between the Participant and the Operator.

If the Participant violates the procedure for the System trademarks (service marks) and logos placement and use (as well as placement or use of the materials referencing or mentioning the System name and/or System trademarks (service marks) and logos) in the public domain without the Operator's consent, the Operator shall have the right to demand penalty from the Participant in the amount of RUB five hundred thousand (500,000) in accordance with the procedure specified in Section 17 hereof.

Placement of trademarks (service marks) of third parties (airlines', retail chains', etc.) on Cards shall be subject to prior consent/permit of the rightholders of such trademarks. The Operator shall have the right to request the Participant to submit the trademarks rightholders' consent/permit to place their trademarks on Participant's Cards, and the Participant shall submit it in the order and within the timeframe specified

in the Operator's request. The Participant shall bear full liability for the accuracy of the information and documents submitted.

In other cases, the System trademarks (service marks) and logos shall only be used upon a prior written consent of the Operator, and a lack of prohibition shall not be considered a consent (permission).

By acceding to the Regulations, the Participant shall grant the Operator the right to use trademarks (service marks), other designations and intellectual property items individualizing the Participant, the rights to which belong to the Participant, and to indicate its business name (full and (or) abbreviated) for the purpose of informing the public about the System's goods, works and services, free of any charge and during the whole term of the System participation, but not longer than the term of the Participant's intellectual property rights to the above items. The right to use the Participant's trademarks (service marks) shall be granted to the Operator by the Participant based on a written permission in the form as set out in the System Standard - *Notification and Application Forms*¹.

If, as a result of such use, the Operator violates third parties' rights, the Participant shall use its own resources and at its own expense indemnify the Operator of all consequences of such violations, including the losses caused to the third parties whose rights were violated.

In the event of a violation by the Participant of third parties' rights to any intellectual property items and equal means of individualization, the responsibility for such violations shall be borne by the Participant. The Participant shall use its own resources and its own expense indemnify the Operator of all consequences associated with such violations, including the damages caused to the third parties whose rights were violated.

¹ Applicable to Non-RF Participants if such trademark (service mark) is registered in the Russian Federation.

4. Interaction Between System Subjects

4.1. Operator's Rights and Obligations

The Operator shall be obliged to:

- lay down the Mir Regulations and Standards, organize and exercise control over the Participants' and Payment Infrastructure Service Providers' compliance with the Mir Regulations and Standards;
- determine and implement the System development strategy;
- maintain the list of Payment Infrastructure Service Providers;
- establish a risk management system in the System, perform the risk assessment and management in the System, ensure the System's business continuity in compliance with the laws of the Russian Federation;
- ensure an uninterrupted provision of payment infrastructure services to the Participants, and inform the Bank of Russia and the Participants about instances of and the reasons for temporary suspension (termination) of the payment infrastructure services rendering on the date of such suspension;
- ensure pre-court consideration of disputes with the Participants and Payment Infrastructure Service Providers in accordance with the Regulations;
- ensure protection of bank secrecy and data on the information security means and methods, personal data and other information subject to mandatory protection in compliance with the laws of the Russian Federation;
- post the System Regulations, System Fees, the *Interchange Fees* Standard, and the list of Payment Infrastructure Service Providers on the Operator's official web-site at www.nspk.ru;
- ensure the fulfillment of other obligations stipulated by the Regulations, relevant agreements with the System Subjects and the laws of the Russian Federation.

The Operator shall have the right to:

- make changes to the System Regulations and Standards;
- change the System operation terms and conditions;
- make integrated assessment (due diligence) of the Participant and analysis of its financial stability in accordance with the Operator's internal procedures and methods, and to request documents necessary for such assessment;
- request information about the activities of the System Subjects, other than the Bank of Russia, and demand its submission in a timely manner;

- exercise control over the compliance with the Regulations by the System Subjects, other than the Bank of Russia, within the scope of their obligations and liabilities stipulated by the Regulations, including the use of the System trademarks (service marks) and logos;
- extend the time for settlement completion in the System for the time required for the elimination of consequences leading to inability to complete settlement in the System, in case of imposition of any economic, financial or trade limitations or restrictive measures based on laws, regulations, legal acts or individual acts of government bodies or any other authorized bodies in accordance with the applicable laws and(or) in case of occurrence of force majeure circumstances (force majeure), i.e. emergency circumstances, unforeseen circumstances, and unavoidable circumstances that could not have been reasonably anticipated or prevented via reasonable measures and means.
- recalculate interchange fees and(or) Operator's fees, if Participants violate System Regulations and Standards by using an inapplicable rate of interchange fee and (or) Operator's fee. The Operator recalculates interchange fees and (or) Operator's fees in accordance with the procedure and under the terms specified in the System Standards and Regulations;
- request from Participants and organizations planning to accede to the Regulations a questionnaire on anti-money laundering and anti-terrorism measures being taken according to the form provided in the *Notification and Application Forms* Standard for the purpose of confirmation of their compliance with the applicable laws on anti-money laundering and counter-terrorism financing, as well as demand submission of such questionnaire within the timeframe specified in the Operator's request.
- deny an organization established in compliance with the laws of a foreign country and located outside the Russian Federation and planning to accede to the Regulations the agreement signing without giving reasons;
- provide information services and consult Participants on the terms of participation in the System in the form of seminars (face-to-face and remotely). Information about the contents, time, format and the venue of such seminars shall be brought to Participant by way of posting it on the Operator's web site at www.nspk.ru and (or) on the System Information Resource;
- contract third-party organizations to perform its functional responsibilities and obligations set forth by the System Regulations and Standards. The Operator shall bear full responsibility to the System Subjects for these organizations' actions;

- Request information and documents relating to business activities from third parties engaged by the Participant for the performance of its functional responsibilities and obligations established in the System Regulations and Standards;
- exercise other rights envisaged by the Regulations, existing agreements with the System Subjects and the applicable laws of the Russian Federation.

4.2. Operations Center's Rights and Obligations

The Operations Center shall be obliged to:

- perform its activities in accordance with the System Regulations, Standards, and the relevant agreements signed with the Settlement Center;
- ensure a guaranteed level of continuity of operational services rendering, as well as protection and security of Transactions in accordance with the requirements of the laws of the Russian Federation and PCI DSS;
- ensure the exchange of electronic messages between the System Subjects, including the transmission of the Participants' Outgoing clearing files to the Payment Clearing Center, as well as transmission of notices (confirmations) of receipt and processing of the Participants' Outgoing clearing files;
- ensure protection of bank secrecy and data on the information security means and methods, personal data and other information subject to mandatory protection in compliance with the laws of the Russian Federation;
- under the Operator's instructions suspend or terminate routing of Authorization requests for Participants' Card Transactions made in the Participants' card acceptance networks;
- provide information on its activity within the System upon the Operator's reasonable requests within the time frame and the scope specified in the Operator's request;
- perform other actions with the use of information and telecommunication technologies necessary for the System functioning, and ensure the fulfillment of other liabilities provided for in the Regulations, relevant agreements with the System Subjects and the laws of the Russian Federation.

The Operations Center shall have the right to:

- render operational services within other payment systems;
- exercise other rights stipulated by the Regulations, relevant agreements with the System Subjects and the laws of the Russian Federation.

The Operations Center shall have no right to:

- unilaterally suspend (terminate) provision of operational services to the Participants and their Customers, unless otherwise provided for herein;
- communicate details of any funds transfer made within the System in the Russian Federation, to the territory of a foreign state, or provide access to such information from the territory of a foreign state, unless otherwise provided for by the laws of the Russian Federation.

4.3. Payment Clearing Center's Rights and Obligations

The Payment Clearing Center shall be obliged to:

- perform its activities in accordance with the System Regulations, Standards, and the relevant agreements signed with the Settlement Center;
- ensure acceptance of the Participants' Outgoing clearing files for processing in accordance with the System Regulations and Standards;
- calculate Net positions; generate Net position logs containing the amounts of the Participants' Net positions and other pertinent information, and submit them to the Settlement Center. The format, contents and submission procedures of the Net positions logs shall be determined by the relevant agreement signed between the Payment Clearing Center and the Settlement Center;
- generate Reports, the format, contents and the submission procedure of which shall be specified in the System Regulations and Standards, and forward them to the Participants;
- provide information on its activity within the System upon the Operator's reasonable requests within the time frame and the scope specified in the Operator's request;
- Indemnify the Participants and the Settlement Center for any damages caused by its nonperformance and (or) improper rendering of payment clearing services;
- ensure protection of bank secrecy and data on the information security means and methods, personal data and other information subject to mandatory protection in compliance with the laws of the Russian Federation;
- ensure the fulfillment of other obligations stipulated by the Regulations, relevant agreements with the System Subjects and the laws of the Russian Federation.

The Payment Clearing Center shall have the right to:

- render payment clearing services within other payment systems;
- exercise other rights stipulated by the Regulations, relevant agreements with the System Subjects and the laws of the Russian Federation.

The Payment Clearing Center shall have no right to:

- unilaterally suspend (terminate) provision of payment clearing services to the Participants unless otherwise provided for herein;
- communicate details of any funds transfer made within the System in the Russian Federation, to the territory of a foreign state, or provide access to such information from the territory of a foreign state, unless otherwise provided for by the laws of the Russian Federation.

4.4. Settlement Center's Rights and Obligations

The Settlement Center shall be obliged to:

- perform its activities as the Settlement Center in accordance with the relevant agreements with the Operator, the Regulations and in accordance with bank account agreements (contracts) entered into by and between the Participants;
- exercise control over the risks of the Participants' non-fulfillment (improper fulfillment) of funds transfer obligations;
- ensure protection of bank secrecy and data on the information security means and methods, personal data and other information subject to mandatory protection in compliance with the laws of the Russian Federation, as well as in compliance with the laws applicable to the Settlement Center;
- provide the Operator with the information on its activity in the System within the time frame and in the scope specified in the relevant agreement entered into by and between the Operator and the Settlement Center;
- ensure fulfillment of other obligations set forth by the laws of the Russian Federation or other laws applicable to the Settlement Center, the agreement between the Operator and the Settlement Center, the Regulations, and relevant agreements with the System Subjects.

The Settlement Center shall have the right to:

- determine the procedures and conditions for opening and maintaining the Participants' accounts and the Guarantee Fund Account in accordance with the laws of the Russian Federation or laws applicable to the Settlement Center, as well as with consideration of the conditions set forth in the Regulations;
- in the event of the Bank of Russia operating as the Settlement Center, provide settlement services for Card Transactions made between RF Participants and Non-RF Participants

to Non-RF Participants in cooperation with the Central Payment Clearing Counterparty without opening accounts to Non-RF Participants with the Bank of Russia;

- exercise other rights stipulated by the Regulations, relevant agreements with the System Subjects, the laws of the Russian Federation or the laws applicable to the Settlement Center.

4.5. Central Payment Clearing Counterparty's Rights and Obligations

The Central Payment Clearing Counterparty shall be obliged to:

- perform its activities as a Central Payment Clearing Counterparty in accordance with the relevant agreements with the Operator;
- have a sufficient amount of funds to fulfill its obligations as the Central Payment Clearing Counterparty in the System;
- exercise a daily control over the risks of non-fulfillment (improper fulfillment) of the Participants' obligation to ensure the availability of sufficient funds on the Participants' accounts for settlement.

4.6. Participants' Rights and Obligations

4.6.1. Direct Participants

The Direct Participant shall be:

- a credit organization established in accordance with the laws of the Russian Federation;
- VEB.RF;
- a bank (a credit organization) established in accordance with the laws of a foreign country and located outside the Russian Federation;
- a central (national) bank established in accordance with the laws of a foreign country and located outside the Russian Federation;
- an international financial organization;
- foreign payment service provider (if System settlement is performed in the currency other than the Russian ruble).

The Direct RF Participant shall conduct settlement payments within the System using the Participant's account opened to it with the Settlement Center (the Bank of Russia).

The Direct Non-RF Participant shall conduct settlement payments within the System using the Participant's account opened to it with the Settlement Center (other than the Bank of Russia).

The Non-RF Participant acting as type C or C1 Participant within the System may conduct settlement within the System without opening accounts with the Settlement Center in accordance with the procedure set forth herein.

The Direct Participant shall be obliged to:

- perform its activities in accordance with the System Regulations and Standards, as well as the terms and conditions of the relevant agreements signed with the Settlement Center;
- ensure a secure connection to the Operations Center and the Payment Clearing Center (directly or through external Third-party Processors);
- notify the Operator, in the format provided in the *Notification and Application Forms* Standard, about the appointment or change of the Processor;
- comply and make third parties engaged to provide services within the System comply with the requirements of the System Regulations, System Standards, and relevant agreements;
- conclude a license agreement with the Operator to obtain the right to use the System trademark (service mark);
- give written permissions to the Operator to use the Participant's trademarks (service marks) in the form provided in the *Notification and Application Forms* Standard;
- pay for the services provided to the Participant within the System, pay interchange fees to other Participants and effect other payments as set forth by the System Regulations, System Fees and the *Interchange Fees* Standard, according to the procedures described in the System Regulations, Standards, and Fees;
- sign an addendum to the bank account agreement with the Settlement Center (in the event of a RF Participant) and a bank account agreement (in the event of a Non-RF Participant);
- grant the right to the Settlement Center to charge the Participant's account transaction amounts, interchange fees to other Participants and the Operator's Fees based on the Net positions log without any additional instructions from the Participant. A Non-RF Participant conducting settlement without Participant's Account opening with the Settlement Center shall submit banking details to the Operator to allow the Central Payment Clearing Counterparty to transfer funds to the Participant in the amount of credit Participant's Net Positions using the form from the System Standard *Notification and Application Forms*;

- ensure the availability of funds on the Account at the Settlement Center, sufficient for the subsequent settlement of Transactions, Interchange fees to other Participants and Operator's Fees according to the System Regulations, System Fees and the *Interchange Fees* Standard; A Non-RF Participant conducting settlement within the System without Participant's Account opening with the Settlement Center shall ensure settlement of Transaction sums, payment of Interchange fees to other Participants and Operator's Fees on the basis of Reports submitted to the Participant by the Payment Clearing Center in the manner and within the time frames set by the Regulations and System Standards;
- ensure the transfer of a guarantee fee to the Guarantee Fund account in the amount and within the time period specified by the Operator;
- ensure the data security within their own information systems according to the requirements of the applicable laws, the Regulations and the *Security Program* Standard.
- service other Participants' Cards in its Card acceptance network according to the terms and conditions stipulated by the System Regulations, Standards and Fees;
- provide Card issuance in accordance with the requirements established by the System Regulations and Standards;
- independently or through a Third-party Processors, ensure that Indirect Participants receive operating and payment clearing services for their Card Transactions;
- be liable to the System Subjects for all obligations arising from Card Transactions made within the Card acceptance network of the Direct Participant and Indirect Participants sponsored by it;
- conclude with Indirect Participants being sponsored by it a bank account agreement and an agreement regulating their interaction within the System with due regard for the Regulations' requirements (the requirement to conclude a bank account agreement with a sponsored Indirect Participant is inapplicable, if the Direct Participant conducts settlement with an Indirect Non-RF Participant without opening of a bank account for the latter with such Direct Participant);
- settle accounts with Indirect Participants in accordance with the procedures set in correspondent agreements signed by and between the Direct and Indirect Participants;
- bear responsibility for its sponsored Indirect Participants' compliance with the requirements of the System Regulations and Standards in their activities within the System;
- be fully accountable for actions (or failure to act) of any third-party provider contracted by the Direct Participant for the fulfillment of its obligations within the System;
- provide assistance to the Operator in dispute resolution;

- submit reports to the Operator in accordance with the System Regulations and Standards;
- timely notify the Operator of any changes in the form of incorporation, reorganization (at least three (3) months prior to the supposed reorganization date), location and mailing address, bank details, authorized persons, as well as of any other changes that may significantly affect the fulfillment by the Participant of its obligations under the Regulations and System Standards;
- in the event of RF Participants, submit to the Operator hard copies signed by the Participant's sole executive body or their proxy and stamped with the Participant's seal (the authority of the proxy shall be evidenced by the original or a duly certified copy of the document confirming the authorities), or notarized copies of the following documents:
 - a copy of license within 15 (fifteen) business days from the date of receipt of a new license;
 - copies of changes in/amendments to the Articles of Association or a revised version thereof, certificates of entries to the Uniform State Register of Legal Entities (USRLE) and/or copies of List of Records in the Uniform State Register on amendments made no later than fifteen (15) days from the amendments registration date;
 - copies of documents confirming election of the Participant's new sole executive body, extension of powers of a person appointed as a Participant's new sole executive body, submitted within fifteen (15) days from the date when such decision has been made by an authorized body;
- RF Participants shall provide the Operator with quarterly reports in electronic format according to All-Russia Classifier of Management Documentation Form No.0409813 to risk@nspk.ru within the time frames similar to the time frames set in the Ordinance of the Bank of Russia No. 4983-U dd. 27.11.2018 'On the Forms, Procedure and Timeframe for Disclosing Information on Activities by Credit Institutions'. If the financials are posted on the Participant's official web site, their provision shall not be required;
- in the event of Non-RF Participants, submit financial and tax accounts in the electronic form executed according to IFRS or other national reporting rules to risk@nspk.ru on a quarterly basis, not later than the last business day of the month following the financial quarter;
- at the Operator's request, provide financial statements and other information within the time specified in the request;

- on an annual basis from December 1 to December 31 provide a Questionnaire on Anti-Money Laundering and Counter-Terrorism Financing Measures Being Taken according to the form set in the System Standard *Notification and Application Forms*;
- in the event of Non-RF Participants, inform the Operator via the System Information Resource about any suspension, revocation (cancellation) of a special permit (license) for the relevant type of activity (operations) (hereinafter – the Permit) not later than the day following such suspension (cancellation) of the Permit;
- inform the Operator via the System Information Resource about any suspension, revocation (cancellation) of Permits of Non-RF Participants being Indirect Participants sponsored by it not later than the day following such suspension, revocation (cancellation) of the Permit;
- Non-RF Participants conducting settlement without Participant's Account opening with the Settlement Center shall at the Operator's request provide a set of documents required for the Settlement Center also acting as the Central Payment Clearing Counterparty to identify the Non-RF Participant in accordance with requirements of laws of the Russian Federation and (or) internal regulations of the Settlement Center;
- in the event of failure to participate in a face-to-face seminar held by the Operator or refusal to participate in such a seminar in less than five (5) business days before the date of the seminar, pay the Operator five thousand five hundred (5,500) rubles for each registered seminar participant who failed to participate in the seminar;
- pay the Operator the amount of the service fee set in the Mir Fees in case of the Participant's unilateral refusal of such service (provided that the Operator has already started to render this service);
- contribute to the System's development;
- the Non-RF Participant shall be solely liable for the discharge of taxes due to be paid in the country where it conducts its business and shall defend, indemnify and hold the Operator harmless against all claims, actions, and suits, as well as any consequences related to their non-payment;
- RF Participants shall ensure for the Cardholders the possibility to use Cards with payment applications of payment application providers in accordance with the procedures and under terms and conditions set forth in System Standards concerning such payment application providers;
- ensure availability of a special permit (license) required for the Participant to conduct business within the System in accordance with the laws of the state in which the

Participant is registered and (or) conducts its business, including E-commerce, if such a permit (license) is required in accordance with the laws applicable to the Participant;

- fulfill other obligations stipulated by the System Regulations and Standards, and the relevant agreements concluded with the System Subjects.

The Direct Participant shall have the right to:

- issue Cards, incorporating the System's trademarks (service marks) and logos of its own (individual) design and under the BINs provided by the Operator to the Participant upon its request;
- issue Co-badged Cards, including those issued under the BINs designated to the Participant by other payment systems within the framework of its participation in them, in accordance with the requirements set forth by the System Regulations, and Standards (applicable to RF Participants only);
- receive Acquiring services within the System's Card Acceptance Network for any Cards issued by the Direct Participant within the System under the terms and conditions established by the System Regulations, Standards and Fees;
- act as a Sponsor to Indirect Participants. The Foreign Payment Service Provider or the Non-RF Participant acting within the System without the Participant's Account opening with the Settlement Center in accordance with the procedure set forth herein have the right to act as a Sponsor only to Indirect Participants acting as type C.1 Participant within the System;
- settle accounts with Indirect Non-RF Participants without bank accounts opening with the Sponsor Direct Participant;
- in compliance with the System's Regulations and Standards, directly or through third-party providers, provide operating, settlement and payment clearing services to its Indirect Participants for any transactions performed between the Direct Participant and its Indirect Participants, as well as for any transactions performed between its Indirect Participants. The Direct Participant shall be entitled to set its own operating, payment clearing services and interchange fees different from those set forth in the System Fees and the *Interchange Fees* Standard;
- arrange interaction with Direct and Indirect Participants that are participants of the same bank group or bank holding as the Direct Participant including the provision of operating, payment clearing and settlement services for Card Transactions made between such participants in compliance with the System Regulations and Standards at the fees for operating, settlement, payment clearing services, as well as at the interchange fees

different from those set forth in the System Fees and the *Interchange Fees* Standard (provisions of the present paragraph are applicable to RF Participants);

- in agreement with other Individual Participants, establish the interchange fee rates, different from those set forth in the System *Interchange Fees* Standard, for the types of Transactions agreed with the Operator according to the procedure specified in the System Standards;
- submit requests to the Operator for changing the Participant's type of activity in the System in accordance with the procedures established by the Regulations;
- change the status in the System from the Direct Participant to the Indirect Participant;
- retain the Direct Participant's BIN upon the status change in the System;
- In case of any restrictions for settlement with the use of the Participant's Account opened with the Settlement Center including those provided for by the laws applicable to the Non-RF Participant, such Non-RF Participant shall be entitled to perform settlement within the System without the Participant's Account opening with the Settlement Center as agreed with the Operator;
- come up with proposals on improvements to the System operations, on introduction of new services within the System, and on other issues regarding the System's operations;
- participate in seminars (face-to-face and remotely) held by the Operator;
- refuse to participate in a seminar not later than five (5) business days before the date of the seminar;
- exercise other rights envisaged by the System Regulations and Standards, and the relevant agreements concluded with the System Subjects.

4.6.2. Indirect Participants

The Indirect Participant shall be:

- a credit organization established in accordance with the laws of the Russian Federation;
- VEB.RF;
- a bank (a credit organization) established in accordance with the laws of a foreign country and located outside the Russian Federation;
- a central (national) bank established in accordance with the laws of a foreign country and located outside the Russian Federation;
- an international financial organization;
- a foreign payment service provider.

The Indirect Participant shall conduct settlement payments within the System through bank accounts opened with its Sponsor Direct Participant. The Indirect Non-RF Participant is entitled to conduct settlement payments within the System without opening of bank accounts with its Sponsor Direct Participant.

The Indirect Participant shall be obliged to:

- conclude with the Sponsor Direct Participant a bank account agreement and an agreement regulating their interaction within the System with due regard for the Regulations' requirements (the requirement to conclude a bank account agreement with the Sponsor Direct Participant is inapplicable, if the Sponsor Direct Participant conducts settlement with an Indirect Non-RF Participant without opening of a bank account for the latter with such Sponsor Direct Participant);
- open a bank account with the Direct Participant for the settlement within the System (the requirement is inapplicable, if the Sponsor Direct Participant conducts settlement with an Indirect Non-RF Participant without opening of a bank account for the latter with such Sponsor Direct Participant);
- perform its activities in accordance with the System Regulations and Standards, as well as the terms and conditions of the relevant agreements signed with the Direct Participant;
- comply and make third parties contracted by the Indirect Participant to provide services within the System comply with the requirements of the System Regulations, System Standards, and relevant agreements;
- conclude a license agreement with the Operator to obtain the right to use the System trademark (service mark);
- give written permissions to the Operator to use the Participant's trademarks (service marks) in the form provided in the *Notification and Application Forms* Standard;
- ensure the data security within their own information systems according to the requirements of the applicable laws, the Regulations and the *Security Program* Standard.
- provide Card issuance in accordance with the requirements established by the System Regulations and Standards;
- service other Participants' Cards in its own Card acceptance network according to the terms and conditions stipulated by the System Regulations, Standards and Fees;
- be liable to the System Subjects for any obligations arising from Transactions made with Cards issued by the Indirect Participant and within its own Card acceptance network;
- be fully accountable for actions (or failure to act) of any third-party provider contracted by the Indirect Participant for the fulfillment of its obligations within the System;

- submit reports to the Operator in accordance with the System Regulations and Standards;
- timely notify the Operator of any changes in the form of incorporation, reorganization (at least three (3) months prior to the supposed reorganization date), location and mailing address, bank details, authorized persons, as well as of any other changes that may significantly affect the fulfillment by the Participant of its obligations under the Regulations and System Standards;
- RF Participants shall provide the Operator with quarterly reports in electronic format according to All-Russia Classifier of Management Documentation Form No.0409813 to risk@nspk.ru within the time frames similar to the time frames set in the Ordinance of the Bank of Russia No. 4983-U dd. 27.11.2018 ‘On the Forms, Procedure and Timeframe for Disclosing Information on Activities by Credit Institutions’. If the financials are posted on the Participant’s official web site, their provision shall not be required;
- in the event of Non-RF Participants, submit financial and tax accounts in the electronic form executed according to IFRS or other national reporting rules to risk@nspk.ru on a quarterly basis, not later than the last business day of the month following the financial quarter;
- at the Operator’s request, provide financial statements and other information within the time specified in the request;
- on an annual basis from December 1 to December 31 provide a Questionnaire on Anti-Money Laundering and Counter-Terrorism Financing Measures Being Taken according to the form set in the System Standard *Notification and Application Forms*;
- provide assistance in dispute investigation;
- the Non-RF Participant shall inform the Operator about any suspension, revocation (cancellation) of the Permit via the Sponsor Direct Participant with the use of the System Information Resource not later than the day following such suspension, revocation (cancellation) of the Permit;
- in the event of failure to participate in a face-to-face seminar held by the Operator or refusal to participate in such a seminar in less than five (5) business days before the date of the seminar, pay the Operator five thousand five hundred (5,500) rubles for each registered seminar participant who failed to participate in the seminar;
- pay the Operator the amount of the service fee set in the Mir Fees in case of the Participant’s unilateral refusal of such service (provided that the Operator has already started to render this service);
- contribute to the System’s development;

- the Non-RF Participant shall be solely liable for the discharge of taxes due to be paid in the country where it conducts its business and shall defend, indemnify and hold the Operator harmless against all claims, actions, and suits, as well as any consequences related to their non-payment;
- RF Participants shall ensure for the Cardholders the possibility to use Cards with payment applications of payment application providers in accordance with the procedures and under terms and conditions set forth in System Standards concerning such payment application providers;
- ensure availability of a special permit (license) required for the Participant to conduct business within the System in accordance with the laws of the state in which the Participant is registered and (or) conducts its business, including E-commerce, if such a permit (license) is required in accordance with the laws applicable to the Participant;
- fulfill other obligations stipulated by the System Regulations and Standards, and the relevant agreements concluded with the System Subjects.

The Indirect Participant shall have the right to:

- conduct settlement within the System without bank accounts opening with the Sponsor Direct Participant (applicable to Indirect Non-RF Participants only);
- issue Cards with the System trademarks (service marks) and logos of its own (individual) design and under the BINs provided by the Operator to the Indirect Participant. The use of the Direct Participant's BINs for Issuing Indirect Participant's Cards is prohibited;
- issue Co-badged Cards, including those issued under the BINs designated to the Participant by other payment systems within the framework of its participation in them, in accordance with the requirements set forth by the System Regulations, and Standards (applicable to RF Participants only);
- receive Acquiring services within the System's Card Acceptance Network for any Cards issued by the Indirect Participant within the System on the terms and conditions established by the System Regulations, Standards and Fees and in accordance with separate agreements concluded with a Direct Participant;
- obtain the Direct Participant status;
- not change the Indirect Participant's BINs when changing the Sponsor Direct Participant or the status in the System;
- directly approach the Operator in the event of the Sponsor's non-fulfillment of its obligations, if such non-fulfillment causes damage to the Indirect Participant's business and/or goodwill;

- contract with several Sponsors in order to accomplish Card Issuing and Acquiring objectives within the System;
- arrange interaction with Direct and Indirect Participants that are participants of the same bank group or bank holding as the Indirect Participant including the provision of operating, payment clearing and settlement services for Card Transactions made between such participants in compliance with the System Regulations and Standards at the fees for operating, settlement, payment clearing services, as well as at the interchange fees different from those set forth in the System Fees and the *Interchange Fees* Standard (provisions of the present paragraph are applicable to RF Participants);
- in agreement with other Individual Participants establish the interchange fee rates, different from those set forth in the System *Interchange Fees* Standard, for the types of Transactions agreed with the Operator according to the procedure specified in the System Standards;
- submit requests to the Operator for changing the Participant's type of activity in the System in accordance with the procedures established by the Regulations;
- participate in seminars (face-to-face and remotely) held by the Operator;
- refuse to participate in a seminar not later than five (5) business days before the date of the seminar;
- come up with proposals on improvements to the System operations, on introduction of new services within the System, and on other issues regarding the System's operations;
- exercise other rights envisaged by the System Regulations and Standards, and the relevant agreements concluded with the System Subjects.

4.6.3. Participant Payment Systems

The Participant Payment System shall be a payment system.

The Participant Payment System shall ensure Card acceptance by all organizations and individual entrepreneurs with whom participants of the Participant Payment System have relevant agreements on Card Transaction settlement.

For Card Acquiring, participants of the Participant Payment System shall accede to the Mir Payment System Regulations.

For Card Issuing, the Participant Payment System shall ensure the connection of its participants to the System as Individual Participants through their accedence to the System Regulations (directly or

indirectly) via the Direct Participant who may simultaneously be a participant of the Participant Payment System.

The Participant Payment System shall conduct settlements within the System using an Account opened by the Participant Payment System's settlement center with the Settlement Center. If there are several settlement centers within the Participant Payment System, the Participant Payment System shall designate one settlement center for Transaction settlement within the System.

The Participant Payment System shall be obliged to:

- perform its activities in accordance with the laws of the Russian Federation, the System Regulations and Standards, as well as in accordance with relevant agreements between the Participant Payment System's settlement center and the Settlement Center;
- comply and make third parties contracted by participants of the Participant Payment System to provide services within the System comply with the requirements of the laws of the Russian Federation, the System Regulations, System Standards, and relevant agreements;
- conclude a license agreement with the Operator to obtain the right to use the System trademark (service mark);
- ensure that the Participant Payment System's participants conclude license agreements with the Operator enabling them to use the System participants' trademarks (service marks);
- give a written permission to the Operator to use the Participant Payment System trademarks (service marks) according to the form provided in the *Notification and Application Forms* Standard;
- ensure that the Participant Payment System's participants give the Operator written permissions to use the Participant Payment System participants' trademarks (service marks) in the form provided in the *Notification and Application Forms* Standard;
- ensure the connection of the Participant Payment System's participants to the Operations Center and Payment Clearing Center in accordance with the System Regulations and Standards;
- be liable to the System Subjects for any obligations arising from Card Transactions made in the Participant Payment System participants' Card Acceptance Network;
- ensure that the Participant Payment System's settlement center concludes an addendum to the bank account agreement with the Settlement Center whereunder the Settlement Center would have the right to charge transaction amounts, fees to other Participants and

the Operator's fees, based on the Net Position Log, to the Participant's account without any additional instructions;

- pay for the services provided to the Participant Payment System within the System, pay interchange fees to other Participants and effect other payments as set forth by the System Regulations, System Fees and the *Interchange Fees* Standard, according to the procedures described in the System Regulations, Standards, and Fees;
- conduct settlements within the System using an Account opened for the Participant Payment System's settlement center with the Settlement Center;
- ensure the availability of funds on the Account at the Settlement Center, sufficient for the subsequent settlement of Transactions, Interchange fees to other Participants and Operator's fees according to the System Regulations, System Fees and the *Interchange Fees* Standard;
- ensure the transfer of a guarantee fee to the Guarantee Fund account in the amount and within the time period specified by the Operator;
- ensure settlements with the Participant Payment System's participants on the Card Transactions performed;
- ensure the data security within their own information systems according to the requirements of the applicable laws, the Regulations and the *Security Program* Standard;
- service other Participants' Cards in the Card Acceptance Network of the Participant Payment System's participants according to the terms and conditions stipulated by the System Regulations, Standards and Fees;
- be responsible for the compliance with the System Regulations and Standards by all the Participant Payment System's subjects operating within the System;
- take full responsibility for the actions/inaction of the Participant Payment System's subjects when they conduct their activities within the System;
- immediately notify the Operator of any changes in the form of incorporation, reorganization, location and mailing address, bank details, as well as of any other changes that may significantly affect the fulfillment by the Participant Payment System of its obligations under the Regulations, including any facts of bankruptcy, forfeiture of any special license to conduct professional activities, etc.;
- ensure the provision of financial statements and other information at the Operator's request within the time specified in such request;
- provide assistance to the Operator in dispute resolution;
- submit reporting to the Operator in accordance with the Regulations;

- in the event of failure by the Participant Payment System's authorized persons to participate in a face-to-face seminar held by the Operator or refusal to participate in such a seminar in less than five (5) business days before the date of the seminar, pay the Operator five thousand five hundred (5,500) rubles for each seminar participant registered who failed to participate in the seminar;
- pay the Operator the amount of the service fee set in the Mir Fees in case of the Participant's unilateral refusal of such service (provided that the Operator has already started to render this service);
- contribute to the System's development;
- ensure the fulfillment of other obligations stipulated by the System Regulations, Standards, relevant agreements with the System Subjects and the laws of the Russian Federation.

The Participant Payment System shall have the right to:

- participate in seminars (face-to-face and remotely) held by the Operator;
- refuse to participate in a seminar not later than five (5) business days before the date of the seminar;
- come up with proposals on improvements to the System operations, on introduction of new services within the System, and on other issues regarding the System's operations;
- exercise other rights envisaged by the Regulations, System Standards, existing agreements with the System Subjects and the laws of the Russian Federation applicable to the Participants.

5. Procedure for Maintaining the List of Payment Infrastructure Service Providers and the List of Participants

The Operator shall maintain a list of Payment Infrastructure Service Providers and shall post it on the Operator's official website at www.nspk.ru.

The list shall include the following information on each Payment Infrastructure Service Provider:

- name of the Payment Infrastructure Service Provider;
- area of activity of the Payment Infrastructure Service Provider within the System;
- location (address) of the Payment Infrastructure Service Provider;
- contact telephone number of the Payment Infrastructure Service Provider and its official web-site.

The Operator shall maintain a list of Participants and shall post the information about the Participants on the System's Information Resource.

The list shall include the following information on each Participant:

- name of the Participant;
- location (address) of the Participant;
- contact telephone number and the Participant's official web-site.

6. Procedures of Entry (Accession) to and Secession from Mir Payment System

6.1. System Participation Criteria

6.1.1. *A credit organization established in accordance with the laws of the Russian Federation and intending to become a Direct Participant shall meet the following criteria:*

1. Have a valid license issued by the Bank of Russia for performing banking operations.
2. Comply with the requirements of the laws of the Russian Federation on anti- money laundering and counter-terrorism financing.
3. Meet at least one of the criteria below:
 - a) be recognized by the Bank of Russia in the order established by it as an important actor of the payment service market;
 - b) its business activity (operations) or that of its affiliated persons is restricted or prohibited outside of the Russian Federation as a result of legislative or other acts passed by foreign states or associations;
 - c) it undertakes to ensure, within three (3) years of its accession to the Regulations as a Direct Participant, the issuance of Mir Cards in the volume not less than one hundred thousand (100,000) or the setting up of a Card Acceptance Network containing at least one thousand (1,000) ATMs or at least one thousand (1,000) devices installed at Merchants (including online stores) for Card/Card details acceptance;
 - d) a credit organization shall perform functions of the PPS settlement center and accede to the Regulations under the instructions of the PPS Operator (organizer) for the purpose of settlement between the System and PPS for Cross-system transactions.

In the event of failure by the Participant to meet the criteria listed in clause 3 hereof, including the conditions envisaged in subclause c), clause 3, the Operator shall have the right to request the Participant to change its status from the Direct Participant to the Indirect Participant, and the Participant shall, within 6 months upon receipt of the Operator's request, unless otherwise agreed with the Operator, ensure that all measures for changing the participation status are taken. If the Participant fails to change the status from Direct Participant to Indirect Participant within the time period specified, the Operator shall have the right to unilaterally suspend the participation of the Participant in the System.

Participants who acceded to the Regulations before November 10, 2017 shall be recognized as compliant with the criteria listed in clause 3 herein.

A credit organization intending to become a Type D Direct Participant shall meet the criteria specified in clauses 1 and 2.

6.1.2. *A credit organization established in accordance with the laws of the Russian Federation and intending to become an Indirect Participant shall meet the following criteria:*

1. Have a valid license issued by the Bank of Russia for performing banking operations.
2. Comply with the requirements of the laws of the Russian Federation on anti- money laundering and counter-terrorism financing.

6.1.3. *A payment system represented by the payment system's operator registered by the Bank of Russia and intending to become a Participant Payment System shall meet the following criteria:*

1. The payment system is recognized by the Bank of Russia as an important (system important/socially important/nationally important) payment system.
2. Chip-based payment cards are issued and acquired within the payment system.
3. Chip-based payment system cards contain their own payment application or a payment application the right to the use of which is exercised under an agreement signed with the rightholder of this payment application.
4. The Participant Payment System's operator is not undergoing a bankruptcy procedure.
5. The Participant Payment System's settlement center meets the following criteria:
 - a) it has a valid license issued by the Bank of Russia for conducting banking operations;
 - b) Comply with the requirements of the laws of the Russian Federation on anti- money laundering and counter-terrorism financing.

6.1.4. *An organization intending to become a Direct or Indirect Participant and being a bank (a credit organization) established in accordance with the laws of a foreign country and located outside the Russian Federation; or a central (national) bank established in accordance with the laws of a foreign country and located outside the Russian Federation; or an international financial organization shall meet the following criteria:*

1. Have a valid Permit (license) for performing banking operations, if such is required by the applicable laws.
2. Comply with the requirements of the laws on anti- money laundering and counter-terrorism financing, if such is required by the applicable laws.

6.1.5. *Foreign payment service provider intending to become a Direct or Indirect Participant shall meet the following criteria:*

1. Have a valid license or any other permit for transactions performance via electronic payment instruments in accordance with the laws of a foreign country where the organization is registered (hereinafter referred to as the Permit).

2. Comply with the requirements of the laws on anti- money laundering and counter-terrorism financing, if such is required by the applicable laws.

System Participation Criteria of a foreign payment service provider being the Direct Participant is the performance of settlement within the System in the currency other than the Russian ruble.

6.1.6. *VEB.RF shall have the right to become either a Direct or an Indirect Participant, if it meets the following criteria: compliance with the requirements of the laws of the Russian Federation on anti-money laundering and counter-terrorism financing.*

6.1.7. *Participation criteria regardless of the Participant status:*

1. Participant's technological infrastructure meets the System's operational requirements as specified in the System Regulations and Standards.

2. Participants ensure the data security within their own information systems and when interacting with the System according to the requirements of the applicable laws, the System Regulations and Standards.

6.2. System Participant's Activity Type

The following types of activity in the System shall be envisaged for Direct Participants:

type A: - Issuing, Acquiring: Purchase Transaction, Cash Disbursement, Cash-to-Card, Card-to-Card, Balance inquiry, PIN change;

type B: - Issuing, Acquiring: Cash Disbursement, Cash-to-Card, Card-to-Card, Balance inquiry, PIN change;

type C: - Acquiring: Purchase Transaction, Cash Disbursement, Cash-to-Card, Card-to-Card, Balance inquiry, PIN change;

type C.1 - Acquiring: Purchase Transaction, Cash Disbursement, Balance inquiry, PIN change (applicable to Non-RF Participants only);

type D - funds transfer via Instant Payment Service of the payment system of the Bank of Russia (applicable to RF Participants only).

- type E - Settlements between the System and PPS for cross-system transactions (applicable to Participants acting as PPS settlement centers).

The following types of activity in the System shall be envisaged for Indirect Participants:

- type A: - Issuing, Acquiring: Purchase Transaction, Cash Disbursement, Cash-to-Card, Card-to-Card, Balance inquiry, PIN change;
- type B: - Issuing, Acquiring: Cash Disbursement, Cash-to-Card, Card-to-Card, Balance inquiry, PIN change;
- type C: - Acquiring: Purchase Transaction, Cash Disbursement, Cash-to-Card, Card-to-Card, Balance inquiry, PIN change;
- type C.1 - Acquiring: Purchase Transaction, Cash Disbursement, Balance inquiry, PIN change (applicable to Non-RF Participants only).

The following types of activity in the System shall be envisaged for Participant Payment Systems:

- type A: - Acquiring: Purchase Transaction, Cash Disbursement, Cash-to-Card, Card-to-Card, Balance inquiry, PIN change;
- type B: - Acquiring: Cash Disbursement, Cash-to-Card, Card-to-Card, Balance inquiry, PIN change.

The Participant shall have the right to conduct only the type of activity stated by it at the accession to the Regulations or when changing the activity type.

6.3. System Entry (Accession) Procedure

An organization shall accede to the Regulations by providing a duly executed set of documents listed in Appendix 2 to the Operator. Accession to the Regulations shall mean the acceptance by the organization of the Regulations in their entirety, without any exceptions or limitations.

An organization intending to become a Direct Participant or a Participant Payment System shall provide the above set of documents directly to the Operator.

An organization intending to become an Indirect Participant shall provide the above set of documents to the Operator via their Direct Participant.

A participant of the Participant Payment System shall provide the above set of documents to the Operator via the Participant Payment System.

The Operator shall review the documents submitted within 30 (thirty) calendar days.

The Operator shall have the right to request additional documents by sending a written request to the organization, which intends to accede to the Regulations.

If the documents review results are positive, the Operator shall assign a unique Participant Identifier allowing to identify each Participant and its status in the System, and shall send to the Participant's address specified in the Application for Accession to the Mir Payment System Regulations a System Entry (Accession) and a Participant Identifier assignment notification.

In the event of a negative result of the documents review, the Operator shall send a respective notification via email to the organization's address specified in the Application for Accession to the Mir Payment System Regulations.

A Participant is considered to be acceded to the Regulations on the date specified in a System Entry (Accession) and a Participant Identifier assignment notification.

Upon receipt of the Identifier assignment notification:

- The RF Participant shall conclude an addendum to the bank account agreement with the Bank of Russia, as the System Settlement Center and the Central Payment Clearing Counterparty, on the provision of settlement services to the Participant in the System (this requirement is not applicable to the Indirect Participants);
- The Non-RF Participant shall conclude a bank account agreement with a Settlement center (other than the Bank of Russia) for transaction settlement services (this requirement is not applicable to the Indirect Participants and Non-RF Participants performing settlements within the System without the Participant's Account opening with the Settlement Center according to the procedure stipulated by the Regulations).

The Participant's Card issuing and Card acquiring activities within the System shall be allowed only after the necessary setting up of the Participant's basic/initial configuration in the Operations Center in accordance with the System Standards has been performed, the mandatory payments in accordance with the System Fees have been made, a bank account agreement or an addendum to the bank account agreement with the Settlement Center has been concluded and the guarantee fee has been transferred to the Guarantee Fund account, and (or) other types of collateral specified in Section 11 herein have been provided.

The Participant may request the Operator to change its status or Sponsor by submitting a relevant application according to the form provided in the *Notification and Application Forms* Standard.

6.4. System Participation Suspension and Termination Procedure

Participation in the System may be suspended on the following grounds:

- at the initiative of the Participant;
- at the initiative of the Operator;
- as agreed by the Subjects;
- the Participant's activity (operations) within the System has been restricted or prohibited in accordance with the laws applicable to the Participant or the Operator.

Participation in the System may be terminated on the following grounds:

- at the initiative of the Participant;
- at the initiative of the Operator;
- as agreed by the Subjects;
- the Participant's activity within the System has been prohibited in accordance with the laws applicable to the Participant or the Operator.

6.4.1. Suspension of Participation in the System at the Participant's Initiative

The Participant shall have the right to initiate suspension of its participation in the System for the period not exceeding one hundred eighty (180) calendar days.

If the Participant decides to suspend its participation in the System, it shall notify the Operator of the suspension using the form set out in the *Notification and Application Forms* Standard.

The Sponsor Direct Participant may initiate suspension of participation of the Indirect Participant sponsored by it by sending a relevant notification of the Indirect Participant participation suspension executed in the form set out in the *Notification and Application Forms* Standard.

The Operator shall review the notification of the Indirect Participant participation suspension and give the Participant a notification of its suspension indicating the suspension date within twenty (20) business days. Starting from the date of suspension of the Participant participation in the System, the Operator shall stop rendering all System services to the Participant.

Transactions made via Participant's Cards before the Participant participation suspension shall be transferred by other Participants for payment clearing within the time limits set forth by the Regulations.

Transactions made via Participant's Cards before the Participant participation suspension and transferred by other Participants for payment clearing with violation of the time limits set by the Regulations shall not be accepted by the System.

Participant's reentry into (reaccession to) the System shall be made automatically at the expiration of its participation suspension period. The Participant shall be entitled to resume its participation in the System prior to the expiration of the suspension term, if a relevant notification on the resumption of Participant's participation in the System is sent to the Operator in the form set out in the *Notification and Application Forms* Standard.

6.4.2. Termination of Participation in the System at the Participant's Discretion

The Participant shall have the right to unilaterally terminate its participation in the System, in particular, if participation in the System becomes illegal according to the applicable laws. If such a decision is made, the Participant shall send an Application for termination of its participation to the Operator according to the form provided in the *Notification and Application Forms* Standard.

The Sponsor Direct Participant may initiate termination of participation of the Indirect Participant sponsored by it by sending an Application for termination of the Indirect Participant's activity within the System executed according to the form provided in the *Notification and Application Forms* Standard.

Upon sending the Application for the System participation termination, the Participant shall immediately stop to perform all Card Transactions within the System and in the Participant's Card Acceptance Network.

The Operator shall review the Application for the Participant's System participation termination and, within twenty (20) business days, shall:

- take measures to stop processing Participant's Card Transactions and Transactions in the Participant's Card Acceptance Network by the Operations Center;
- send a notification with the participation termination date to the Participant.

Transactions made before the termination of the Participant Card Transaction processing by the Operations Center shall be transferred by other Participants for payment clearing within the time limits set forth by the Regulations.

Transactions made before the termination of the Participant Card Transaction processing by the Operations Center and transferred by other Participants for payment clearing with violation of the time limits determined by the Regulations shall not be accepted by the System.

Participation in the System shall be terminated not earlier than one hundred eighty (180) calendar days from the date on which the Operations Center stops processing Participant's Card Transactions or Transactions in the Participant's Card Acceptance Network, provided that the Participant has no financial obligations to any of the System Subjects. Participation in the System may be terminated earlier than 180

(one hundred eighty) calendar days, if no Card Transactions or Transactions in the Participant's Card Acceptance Network were performed as on the date of Operations Center's activities aimed at elimination of a capability to process Participant Card Transactions or Transactions in the Participant's Card Acceptance Network.

Before the participation termination date, the Participant shall:

- fulfill all the financial and other obligations by the Participant to all the System Subjects incurred during the period of its activity in the System as its Participant;
- hand over all confidential information to the Operator in accordance with the Regulations;
- remove decals and information materials with the System trademarks, service marks and logos from all ATMs serviced by the Participant, Unattended Payment Terminals (Self-service terminals), Point-of-Sale Terminals and other devices designed for the Transaction performance, as well as from the information signs designed to inform Cardholders about the location of the said devices, within 10 (ten) business days following the date of submission of the Application for the participation termination.

After the expiry of the above obligation settlement period, the Operator shall:

- give the Participant a notice containing the reason for and the date of termination of its participation;
- notify the Settlement Center in writing of the fact of voluntary termination of the Participant's participation in the System;
- within 2 (two) business days after the day of termination of participation, give instructions to the Settlement Center to return to the Participant the unused guarantee fee in the amount remaining after all the Participant's obligations to other System Subjects during its operations in the System have been fulfilled.

Termination of participation in the System shall not release the Participant from the obligations arising from its activities in the System.

6.4.3. Suspension of Participation at the Operator's initiative

The Operator may suspend participation in the following cases:

- inability to reimburse the Transaction amounts charged to the Participant's account in the Settlement Center, in particular, due to arrest of the funds on the Account, blocking or suspension of the Account operations in accordance with the laws of the Russian Federation or the laws applicable to the Participant;

- a failure of a Non-RF Participant conducting settlement within the System without Participant's Account opening with the Settlement Center to pay Transaction amounts, Interchange fees to other Participants and Operator's Fees in the manner and within the time frames set by the Regulations and System Standards;
- multiple failures to take all necessary measures related to Anti-money laundering / Antiterrorism financing activity;
- prohibition by the Bank of Russia of certain banking transactions, which impedes the fulfillment of the Participant's obligations within its activity in the System;
- prohibition of Participant's System operations by the laws applicable to the Participant;
- identification of negative factors that may cause the risk of the Participant's jeopardizing the System's uninterrupted operation and a failure to eliminate the specified factors within the timeframe set by the Operator;
- identification of the Participant's violations of the System data security requirements that may affect the System's safe operation and a failure to eliminate the specified violations within the timeframe set by the Operator;
- detection of violations affecting the System's and/or Operator's goodwill;
- Participant's delay in adding funds to the Guarantee Fund Account to make its balance equal to the guarantee fee amount determined by the Operator;
- Participant's failure to meet the criteria described in Subclause 6.1.1 hereof if the participation status does not change from the Direct Participant to the Indirect Participant within the period set forth in item 3 of Subclause 6.1.1;
- Participant's incompliance with the participation criteria listed in Subclause 6.1.7 hereof.
- receipt from the Sponsor Direct Participant of an Application for termination of the sponsored Indirect Participant's activity (participation) within the System. Within 180 (one hundred eighty) calendar days from the date of suspension of the Indirect Participant participation within the System, the Indirect Participant shall be obliged to ensure a switch to the new Sponsor's services or change the status to the Direct Participant in accordance with the Regulations;
- multiple (two times and more) Participant's failure to remedy the revealed violations of System Standards and Regulations within the time frames set by the Operator, excluding the cases listed above.

The System participation may also be suspended based on the type of activity (issuing/acquiring).

If the Operator makes a decision to suspend the Participant's participation in the System, the Operator shall forward to such Participant a notification of its participation suspension specifying the circumstances

preventing the Participant from continuing its operation within the System and/or the violation that caused the suspension, as well as the period within which such violation must be remedied.

The Participant's activity in the System may be resumed, provided the violation specified by the Operator in the notification has been remedied or in case of cessation of circumstances preventing the Participant from continuing its operation within the System.

If the violation is not remedied within the dates specified, the Operator shall have the right to initiate the procedure of termination of the Participant's participation in the System.

6.4.4. Termination of Participation at the Operator's initiative

The Operator shall have the right to unilaterally decide to terminate Participant's participation in the System on the grounds below:

- failure by the Participant to remedy the violations of the Regulations and Standards, indicated in subclause 6.4.3, within the time period determined by the Operator;
- Settlement Center's refusal to open an Account or Settlement Center's closure of the Account of the Non-RF Participant being the Direct Participant;
- termination of the license agreement for the right to use System trademarks (service marks) concluded between the Participant and the Operator including in case of the unilateral termination of the license agreement at the Participant's discretion;
- presence of auditor's modified opinion expressed in the auditor's opinion on financial statements of the Participant or the Participant's parent company, or presence of doubts in applicability of the assumption of Participant's or such parent company's going concern;
- undertaking of investigations by public authorities in respect of the Participant or Participant's parent company, their owners (beneficiary owners), senior managers (management body members) based on suspicion of fraud, financial statement fraud, money laundering, etc.;
- Indirect Participant's failure to switch to the new Sponsor's services or change the status to the Direct Participant in accordance with the Regulations within 180 (one hundred eighty) calendar days from the date of suspension of the Indirect Participant's participation within the System due to the receipt from the Sponsor Direct Participant of an Application for termination of the sponsored Indirect Participant's activity (participation) within the System.

- participation in the System becomes illegal in accordance with the laws applicable to the Participant or the Operator.

Upon the Operator's decision to terminate the Participant's participation in the System, the Operator shall send the Participant a notification containing the reasons for and the intended date of the proposed termination.

The Operator shall cause the Operations Center to terminate processing of the Participant's Card Transactions and Transactions in the Participant's Card Acceptance Network.

Participation in the System shall be terminated not earlier than one hundred eighty (180) calendar days from the date on which the Operations Center stops processing Participant's Card Transactions or Transactions in the Participant's Card Acceptance Network, provided that the Participant has no financial obligations to any of the System Subjects. Participation in the System may be terminated earlier than 180 (one hundred eighty) calendar days, if no Card Transactions or Transactions in the Participant's Card Acceptance Network were performed as on the date of Operations Center's activities aimed at elimination of a capability to process Participant Card Transactions or Transactions in the Participant's Card Acceptance Network.

From the date of the above Operator's notification and until the date of termination of participation in the System, the Participant shall:

- fulfill all the financial and other obligations by the Participant to all the System Subjects incurred during the period of its activity in the System as its Participant;
- hand over all confidential information to the Operator in accordance with the Regulations;
- remove decals and information materials with the System trademarks, service marks and logos from all ATMs serviced by the Participant, Unattended Payment Terminals (Self-service terminals), Point-of-Sale Terminals and other devices designed for the Transactions performance, as well as from the information signs designed to inform Cardholders about the location of the said devices, within 10 (ten) business days following the date of receipt of the Notification of the participation termination.

After the expiry of the above obligation settlement period, the Operator shall:

- give the Participant a notice containing the reason for and the date of termination of its participation;
- notify the Settlement Center in writing of the fact of termination of the Participant's participation in the System and the lack of Participant's financial debts;
- within 2 (two) business days after the day of termination of participation, give instructions to the Settlement Center to return to the Participant the unused guarantee fee in the amount

remaining after all the Participant's obligations to other System Subjects during its operations in the System have been fulfilled.

Termination of participation in the System shall not release the Participant from the obligations arising from its activities in the System.

6.4.5. Termination of Participation in the System in the Event of Revocation (Cancellation) of RF Participant's License for Banking Operations or Removal by the Bank of Russia of the Participant System's Operator from the Payment System Operator Register

In the event of revocation (cancellation) of Participant's license to perform banking operations, the Operator, as of the date of the incurrance of the above grounds, shall suspend the Participant's participation in the System, stop to provide all services to the Participant within the System and inform the Participant about the intended date of termination of the Participant's participation in the System within five (5) business days from the date of the above revocation (cancellation).

The Operator shall cause the Operations Center to terminate processing of the Participant's Card Transactions and Transactions in the Participant's Card Acceptance Network on the date of the revocation.

In the event of revocation (cancellation) of the Sponsor Direct Participant's license, on the date of the license revocation, the Operator shall take measures to stop the Operations Center's processing of transactions performed via Cards of Indirect Participants and within the Card Acceptance Network of Indirect Participants for whom the Direct Participant is a Sponsor.

Transactions made before the termination of the Operations Center's processing of Transactions performed via Cards of Participants or Indirect Participants for whom this Participant is a Sponsor shall be transferred by other Participants for payment clearing within the time limits set forth by the Regulations.

Transactions made before the termination of the Operations Center's processing of Transactions performed via Cards of Participants or Indirect Participants for whom this Participant is a Sponsor and transferred by other Participants for payment clearing with violation of the time limits set forth by the Regulations shall not be accepted by the System.

Participation in the System shall be terminated not earlier than 180 (one hundred eighty) calendar days from the date of the above grounds for termination in the System. Participation in the System may be terminated earlier than 180 (one hundred eighty) calendar days from the date of the revocation of the license for banking operations from the Participant, if no Card Transactions or Transactions in the Participant's Card Acceptance Network were performed as on the date of the revocation.

After the expiry of the above time limits, the Operator shall:

- give the Participant a notice containing the reason for and the date of termination of its participation;
- notify the Settlement Center in writing of the fact of termination of the Participant's participation in the System;
- within 2 (two) business days after the day of termination of participation, give instructions to the Settlement Center to return to the Participant the unused guarantee fee in the amount remaining after all the Participant's obligations to other System Subjects during its operations in the System have been fulfilled.

In the event of removal by the Bank of Russia of the Participant Payment System's Operator from the Register of payment system operators, the termination procedure (similar to the termination procedure in case of banking license revocation) shall be applied as described above, provided that the Operator takes measures to terminate processing of Transactions in the Participant Payment System Participants' Card Acceptance Network by the Operations Center on the date of the above grounds incurrance.

In the event of insufficiency of the guarantee fee of the Direct Participant or the Participant Payment System whose banking license has been revoked (cancelled), the Guarantee Fund resources shall be used to fulfill all its obligations. If the Guarantee Fund resources are used to fulfill obligations of such Participant, the Operator is entitled to reimburse the amount of the used Guarantee Fund resources using the funds of the Operator. However, the Operator shall have the right to collect from the Participant the funds used to provide for the fulfillment of the Participant's obligations in the order envisaged by the laws of the Russian Federation.

In order to ensure the fulfillment of obligations of the Indirect Participant whose banking license has been revoked (cancelled), the Direct Participant's Guarantee Fee shall be used as well. However, the Direct Participant shall have the right to collect from its Indirect Participant the funds used to provide for the fulfillment of the Indirect Participant's obligations in the order envisaged by the laws of the Russian Federation.

Termination of participation in the System shall not release the Participant from the obligations arising from its activities in the System.

6.4.6. Termination of Participation in the System in the Event of Revocation (Cancellation) of Non-RF Participant's Permit

If the Operator becomes aware of revocation (cancellation) of the Non-RF Participant's Permit, the Operator, as of the date of receipt of the above information, shall suspend the Participant's participation in

the System, stop the provision of all services to the Participant within the System and inform the Participant about the intended date of termination of the Participant's participation in the System.

The Operator shall cause the Operations Center to terminate processing of the Participant's Card Transactions and Transactions in the Participant's Card Acceptance Network on the date of receipt of the above information.

In the event of revocation (cancellation) of the Sponsor Direct Participant's license, on the date of the Permit revocation (cancellation), the Operator shall take measures to stop the Operations Center's processing of transactions performed via Cards of Indirect Participants and within the Card Acceptance Network of Indirect Participants for whom the Direct Participant is a Sponsor.

Transactions made before the termination of the Operations Center's processing of Transactions performed via Cards of Participants or Indirect Participants for whom this Participant is a Sponsor shall be transferred by other Participants for payment clearing within the time limits set forth by the Regulations.

Transactions made before the termination of the Operations Center's processing of Transactions performed via Cards of Participants or Indirect Participants for whom this Participant is a Sponsor and transferred by other Participants for payment clearing with violation of the time limits set forth by the Regulations shall not be accepted by the System.

Participation in the System shall be terminated not earlier than 180 (one hundred eighty) calendar days from the date of the above grounds for termination in the System. Participation in the System may be terminated earlier than 180 (one hundred eighty) calendar days from the date of the revocation (cancellation) of the Participant's Permit if no Card Transactions or Transactions in the Participant's Card Acceptance Network were performed as on the date of the revocation (cancellation).

After the expiry of the above time limits, the Operator shall:

- give the Participant a notice containing the reason for and the date of termination of its participation;
- notify the Settlement Center in writing of the fact of termination of the Participant's participation in the System;
- within 2 (two) business days after the day of termination of participation, give instructions to the Settlement Center to return to the Participant the unused guarantee fee in the amount remaining after all the Participant's obligations to other System Subjects during its operations in the System have been fulfilled.

In the event of insufficiency of the guarantee fee of the Direct Participant whose Permit has been revoked (cancelled), the Guarantee Fund resources shall be used. If the Guarantee Fund resources are used to fulfill obligations of such Participant, the Operator is entitled to reimburse the amount of the used

Guarantee Fund resources using the funds of the Operator. However, the Operator shall have the right to collect from the Participant the funds used to provide for the fulfillment of the Participant's obligations in the order envisaged by the Regulations and the laws of the Russian Federation.

In order to ensure the fulfillment of obligations of the Indirect Participant whose Permit has been revoked (cancelled), the Direct Participant's Guarantee Fee shall be used as well. However, the Direct Participant shall have the right to collect from its Indirect Participant the funds used to provide for the fulfillment of the Indirect Participant's obligations in the order envisaged by the applicable laws.

Termination of participation in the System shall not release the Participant from the obligations arising from its activities in the System.

7. Issuing

7.1. Issuing Participant's (Issuer's) Rights and Obligations

The Issuer shall perform the following functions in the System:

- issue Cards with the System trademarks (service marks) and logos in accordance with the requirements specified in the System's Regulations and Standards;
- ensure settlements with Customers based on the Cardholder Transaction Reports received from the Payment Clearing Center;
- ensure settlements with Acquiring Participants (Acquirers) on the Issuer's Card Transactions in the Acquirers' Card Acceptance Network;
- ensure the security of the Card Issuing and Authorization processes;
- participate in the resolution of disputes on Issuer's Card Transactions made in the Acquirers' Card Acceptance Network.

The Issuer shall:

- perform its activity in accordance with the requirements of the System Regulations and Standards;
- use only the BINs provided to the Participant by the Operator for Cards issuing;
- use the Blank Cards manufactured only by the companies approved by the Operator;
- contract third-party organizations for Card personalization or, if personalization is performed by the Issuer, ensure that the Issuer's Card Personalization Center and personalization procedures comply with the System Regulations and Standards;
- notify the Operator of the Participant's personalization center, on the change of the Participant's personalization center in the form provided in the *Notification and Application Forms* Standard;
- obtain an approval of the Card design from the Operator in accordance with the procedure envisaged by the System Standards;
- ensure the successful pass of validation of Cardholder data, card product parameters, and other data placement in the payment application and on the Card magnetic stripe in accordance with the System Standards (check of the electrical Card personalization);
- comply with the System's security requirements for storage, transfer and destruction of Cards;
- support all types of Transactions (except for the restrictions for certain types of the System's Products, set forth by the *Mir Payment System Products* Standard);

- ensure round-the-clock Issuer's Card Transaction Authorization including the Stand-in Authorization;
- inform the Operator using the System Information Resource about a scheduled suspension of its hardware and software systems for more than 1 hour at least five (5) business days prior to the suspension;
- ensure the level of readiness of the Issuer's software and hardware complex, determined in the System in accordance with the System Standards requirements;
- have qualified personnel on the staff who will be directly responsible for all aspects of the Card security and who will be, in particular, obliged to:
 - monitor Card Transactions in order to identify illegal use of Cards;
 - investigate the cases of illegal use of Cards;
 - plan and monitor the production, personalization, encoding, printing and other procedures related to Card issuing;
 - plan and monitor the protection level of the Participant's Card personalization center.
- ensure that the Acquirers are compensated for the Issuer's Card Transactions in the amount confirmed by the Issuer's Authorization, performed in accordance with the requirements of the System Regulations and Standards, in the event of the Stand-in authorization, for Offline transactions, as well as for certain types of Transactions, for which the System Regulations and Standards allow for an overdraft of the Transaction amount presented by the Acquirer for clearing as compared to the Authorization amount;
- at the Operator's request provide statistical data on the Issuer's Card Transactions made in the Card Acceptance Network within the time limits indicated in the request;
- provide full information to Cardholders about the Card acceptance by the System and consult them on the Issuer's Cards usage rules;
- organize a round-the-clock Cardholder Support during their use of Cards;
- accept Transactions presented for Clearing later than the date stipulated by the Regulations but no later than 120 days after the Transaction, provided that the Cardholder's account exists and there are funds on it sufficient for transaction settlement by the Issuer;
- notify the Operator of third-party providers contracted by the Issuer for the performance of its functional responsibilities and obligations set forth by the System Regulations and Standards, if the System Standards set the procedure obliging the Issuer to notify the Operator of engagement of such third-party providers. The Issuer is obliged to ensure that

agreements with the specified third parties contain provisions describing the Operator's rights to request information and documents from such third parties relating to their business activities, as well as provisions obliging such third parties to provide the Operator with the information and documents in accordance with the procedure and within the terms set in the Operator's request.

The Issuer shall have the right to:

- issue Cards with the System trademarks (service marks) and logos of its own (individual) design and under the BINs provided by the Operator to the Issuer;
- issue Co-badged Cards, including those issued under the BINs designated to the Issuer by other payment systems within the framework of its participation in them, in accordance with the requirements set forth by the System Regulations, and Standards;
- independently determine financial relationships with Customers on Cards provision and Card Transactions performed in the Card Acceptance Network;
- contract third-party organizations to perform its functional responsibilities and obligations set forth by the System Regulations and Standards. The Issuer shall be responsible to the System Subjects for the activities of these organizations.

7.2. Types and Features of the System Products

The description of the System Products is provided in the System Standard - *Mir Payment System Products*.

7.3. BIN Assignment

A BIN can be assigned to the Participant only after the accession to the Regulations.

BINs are unique and may not be used by other Participants.

The Participant may not transfer the right to use BIN assigned to it by the Operator to other organizations conducting their business both in the Russian Federation and in other countries.

An individual BIN shall be used for each type of Cards, excluding Guarantee Corporate Cards. Combination of different types of card products under one BIN shall not be allowed except for the cases of issuing:

- Business Cards for legal entities for whom the Participant shall have the right to use both an individual BIN and the BIN of the corresponding Card type in accordance with the System Standard *Mir Payment System Products*;
- Guarantee Corporate Cards for which the Participant shall use BIN or the BIN-range used to issue Business Cards.

To issue Cards without a physical medium, the Participant shall have the right to use both an individual BIN and the BIN assigned to the material Cards of the same type.

The procedure of combining various card products for the issuance of Co-badged Cards under BINs designated to the Participant by another payment system shall be regulated by the System Standards.

For BIN obtaining (assignment modification), the Participant shall file an appropriate application to the Operator according to the form provided in the *Notification and Application Forms* Standard.

The Operator shall have the right to modify Participants' BIN assignment, if the Operator suspends the card product within the System. At least one hundred eighty (180) calendar days prior to the date of the potential modification of the Participant BIN assignment, the Operator shall notify Participants of the Participant BIN assignment modification by sending relevant notifications to Participants and (or) by posting relevant information on the System Information Resource.

The Participant may refuse to use the BIN by sending an appropriate application to the Operator according to the form provided in the *Notification and Application Forms* Standard. The Operator shall block the BIN in the Operations Center.

Transactions performed via Participant's Cards with BIN before the its blocking by the Operations Center shall be transferred by other Participants for payment clearing within the time limits set forth by the Regulations.

Transactions performed via Participant's Cards with BIN before the its blocking by the Operations Center and transferred by other Participants for payment clearing with violation of the time limits set by the Regulations shall not be accepted by the System.

The Operator's Fee for the BIN assignment shall not be refunded.

7.4. Requirements for Storage, Transfer and Destruction of Cards

The Issuer shall comply with the security requirements for storage, transfer and destruction of Cards, specified in the System Regulations and Standards.

The Issuer shall:

- approve the list of officials responsible for the storage and the order of distribution of Cards and PIN-envelopes, Blank Cards and PIN-envelopes in the Participant's area of responsibility, as well as for the transfer of Cards for personalization;
- plan and monitor the degree of protection of the Issuer's Card and PIN-envelopes Personalization Center, including the building where this center is located;
- ensure that Cards, Blank Cards, and PIN-envelopes are stored in a special vault the protection degree of which is comparable to the protection degree of a cash vault;
- ensure control and recording of relocation (transfer) of Cards, Blank Cards, and PIN-envelopes, as well as perform inventory when receiving/sending out batches of Cards and Blank Cards;
- plan and monitor personalization and destruction of Cards and Blank Cards using the dual control methods;
- ensure that PIN-envelopes and Cards are personalized separately;
- ensure that personalized Cards and PIN-envelopes are stored and relocated (transferred) separately;
- develop operating procedures for the Card and Blank Cards destruction, document the Cards and Blank Cards destruction procedure and prepare correspondent destruction certificates;
- perform Card and Blank Cards stock-taking in the Card storage vault at least once a year;
- ensure that details of Cards issued without a physical medium or as various form factors are transferred to the Cardholder in a safe way.

The Issuer shall promptly notify the Operator of any events of damage to, tampering with and lack/loss of Cards, Blank Cards and envelopes when receiving/sending out batches of Cards and/or Blank Cards in order to jointly determine further actions.

7.5. Requirements for the Issuer's Agreement with the Customer

The Issuer's agreement with the Customer shall define both the relationship of the Issuer and its Customer in connection with the provision of Cards to the Customer.

The Issuer's agreement with the Customer shall contain the following provisions:

- requirements to security provision when using the Cards including the prohibition to hand the Card and the PIN over to third persons;

- the Card shall not be used for any illegal purposes, including but not limited to purchase of goods, works or services prohibited by the laws of the Russian Federation or the laws applicable to the Issuer and/or Customer;
- the Cardholder's responsibility to the Issuer for the reimbursement of Transactions performed with the use of the Card;
- requirements to the procedure and time limits pursuant to and within which the Cardholder shall inform the Issuer about unauthorized usage or loss of the Card;
- amount of the Issuer fee and procedure for its charging to the Cardholder;
- methods of filing claims regarding Transactions and their review procedure.

The Operator shall not consider claims of the Issuer's Customers for the Issuer's *mala fide* fulfillment of the terms and conditions of the agreements signed with the Customers. However, the existence of such claims may result in initiation of auditing the Participant for compliance with the System Regulations and Standards.

8. Acquiring

8.1. Acquiring Participant's (Acquirer's) Rights and Obligations

The Acquirer shall perform the following functions in the System:

- maintain and control the Card Acceptance Network designed to perform Card Transactions;
- process Transactions determined in the Regulations in its Card Acceptance Network;
- participate in the resolution of disputes on Transactions made in the Acquirers' Card Acceptance Network;
- ensure secure functioning of the Card Acceptance Network.

The Acquirer shall be obliged to:

- perform its activity within the System in accordance with the requirements of the System Regulations and Standards;
- ensure uninterrupted and equal service for all Participants' Cards in its Card Acceptance Network;
- ensure a round-the-clock serviceability of the Acquirer's hardware and software systems to collect, process, transfer, and store Transaction data;
- ensure the compliance of the level of readiness of the Acquirer and its Card acceptance devices and equipment with the requirements of the System Standards;
- use only the devices and equipment certified by the Operator to service and accept the Cards;
- ensure the safety and protection of Card Transactions within the Acquirer's Card Acceptance Network in accordance with the System Regulations and Standards, the laws of the Russian Federation or the laws applicable to the Acquirer;
- inform the Operator using the System Information Resource about a scheduled suspension of the Card acceptance (processing) for more than 1 hour at least five (5) business days prior to the suspension;
- ensure routing of Authorization requests related to Transactions performed by Cardholders of other Participants within the Card Acceptance Network to the Operations Center in accordance with the BIN table provided by the Operations Center;
- no later than the next business day after the submission by the Operations Center of an updated BIN table, update routing parameters of Authorization Request for Transactions performed with the use of Participant's Cards within the Acquirer's Card Acceptance Network;

- ensure the placement of the System trademarks (service marks) and logos on all Card Transactions processing devices and at Cardholder points of service, including on the Internet, to inform them about the possibility to perform Card Transactions;
- provide Participant's Cardholders with full information on the terms and conditions of Cards servicing within the Acquirer's Card Acceptance Network, including the information on any additional fees charged, if any;
- provide, at the Operator's request, statistical data on Card Transactions processed in the Acquirer's Card Acceptance Network within the time limits indicated in such request;
- not set for Cardholders the minimum and/or maximum limits for Transaction amounts (the requirement to limit the maximum Transaction amount shall not be applicable to the Card-to-Card Transactions), unless otherwise provided for by the laws of the Russian Federation or the law applicable to the Acquirer, and allow the Cardholder to determine at his own discretion the amount of funds to be withdrawn in the Acquirer's Card Acceptance Network;
- notify the Cardholder prior to the Card-to-Card Transaction performance of the maximum amount set by the Operator for such Transactions;
- involve Merchants for the Card acceptance for Purchase Transactions provided that the Acquirer enters into an Agreement with each Merchant on Card Transactions settlement and inspects each Merchant using the Merchant inspection service according to the procedure set in the System Standard - *Merchant Screening Service Guide*;
- assign a Merchant Category Code (MCC) to each Merchant in strict compliance with the Merchant activity classification and make sure that the MCC is used, in particular in Authorization requests and clearing messages, in accordance with the System Standards. The list of MCCs shall be provided in the System Standards;
- prohibit performance of Transactions at a Merchant, if business activity of such a Merchant is classified as a prohibited business activity in accordance with the System Standard *Requirements to High-risk Activities at the Acquirer*, as well as prohibit Cross-border Transactions at a Merchant, if business activity of such a Merchant is classified using Merchant Category Codes (MCC) set in the System Standard *Requirements to High-risk Activities at the Acquirer*;
- have in-house staff experts in risk management and security, to be able to timely and effectively detect suspicious or fraudulent activity in the Acquirer's Card Acceptance Network;
- monitor activity in the Acquirer's Card Acceptance Network, as well as exercise control over the Merchant's activity in order to monitor and prevent:

- misuse and fraudulent use of Cards acceptance devices including the ones provided by the Acquirer to the Merchant or approved by the Acquirer;
- acceptance of counterfeited or stolen cards as a means of Purchase Transaction performance or illegal use of Card details;
- notify the Operator in cases and according to the procedure set by the System Standard - *Merchant Screening Service Guide*;
- notify the Operator of third-party providers contracted by the Acquirer for the performance of its functional responsibilities and obligations set forth by the System Regulations and Standards, if the System Standards set the procedure obliging the Acquirer to notify the Operator of engagement of such third-party providers. The Acquirer is obliged to ensure that agreements with the specified third parties contain provisions describing the Operator's rights to request information and documents from such third parties relating to their business activities, as well as provisions obliging such third parties to provide the Operator with the information and documents in accordance with the procedure and within the terms set in the Operator's request.

The Acquirer shall have the right to:

- contract third-party organizations to perform its functional responsibilities and obligations set forth by the Regulations. The Acquirer shall be responsible to the System Subjects for the activities of these organizations;
- charge additional Cardholders service fees for Transactions performed in its Card Acceptance Network on the conditions set forth in the System Regulations and Standards;
- set the maximum Transaction amount for Card-to-Card Transactions performed by the Cardholder in the Acquirer's Card Acceptance Network.

The Acquirer shall not:

- involve a Merchant for the purpose of Transactions performance, if business activity of such a Merchant is classified as a prohibited business activity in accordance with the System Standard *Requirements to High-risk Activities at the Acquirer*;
- involve a Merchant for the purpose of Cross-border Transactions performance, if business activity type of such a Merchant is classified using Merchant Category Codes (MCC) set in the System Standard *Requirements to High-risk Activities at the Acquirer*.

8.2. Transaction Types

The following transactions may be performed using the Participants' Cards:

- Financial transactions;
- Non-financial transactions.

The following types of financial Transactions shall be allowed to be made in the System:

1) *Cash Disbursement (Cash Advance)*

A Card Transaction, the result of which is a disbursement of cash to the Cardholder;

2) *Purchase Transaction / Purchase Return (works, services cancellation);*

A Card Transaction performed in order to pay for goods (works or services) provided for the Cardholder or in order to return the cost of goods (work or services);

3) *Cash-to-Card Transaction (Account crediting)*

A Card Transaction, the result of which is a cash lodgement (crediting) to the Cardholder bank account or to the balance of the Cardholder's electronic money;

4) *Card-to-Card Transaction.*

A Card Transaction, the result of which is:

- a transfer of funds by the Cardholder to the bank account or balance of electronic money of the payee in accordance with the procedure and under the terms provided in the System Standards;
- a transfer of funds by the payer to the Cardholder to the bank account or balance of electronic money of the Cardholder in accordance with the procedure and under the terms provided in the System Standards.

5) *payments to Cardholder from the Russian Federation State Budgets and other sources (Disbursements with indication of a relevant source, hereinafter collectively referred to as the Disbursement Transaction).*

A Card Transaction, the result of which is crediting the Cardholder's bank account with funds from Russian Federation State Budgets and other sources.

The Government Disbursement Transaction is performed by the Federal Treasury out of funds of the budgeting system of the Russian Federation to physical persons – Cardholders – in accordance with Federal Law No. 161-FZ of 27 June 2011 *On the National Payment System*, System Regulations and Standards, and the agreement on daily settlement of payments made from the budgeting system of the Russian

Federation to physical persons – holders of Mir Cards, concluded between the Operator, the Bank of Russia and the Federal Treasury.

In case of conclusion of agreements with other organizations for crediting of other Disbursement Transactions, such Transactions will be performed in accordance with the laws of the Russian Federation, System Regulations and Standards, and the agreement on daily settlement of payments made from the budgeting system of the Russian Federation to physical persons – holders of Mir Cards, concluded between the Operator, the Bank of Russia and the relevant organization performing disbursements.

The Organization performing Disbursement Transactions to perform settlement for Disbursement Transactions shall provide the Operator with data on each Disbursement Transaction included in the Net Position Log.

The Disbursement Transaction is performed out of funds of the Operator to give a financial incentive to Cardholders within Operator's campaigns aimed at improvement of the System image and promotion of active Card use.

When conducting daily settlement for Disbursement Transactions, the Bank of Russia shall act as the Settlement Center and the Central Payment Clearing Counterparty.

Special aspects of the Disbursement Transaction are as follows:

- Interchange fees are not envisaged;
- Issuers are prohibited to charge any additional fees to its Cardholders;
- the Issuer is obliged to make funds available to the Cardholder within 30 minutes upon Authorization (the requirement is not applied to Disbursement Transactions performed out of funds of the Operator).

6) *Purchase Transaction via Digital Certificate with the use of a Card (DC-based Purchase) / Purchase Return (cancellation of works, services paid via Digital Certificate with the use of a Card) (DC-based Purchase Return).*

A Purchase Transaction via Digital Certificate with the use of a Card (DC-based Purchase) or transactions performed to return funds (part of funds) paid for goods (works, services) via Digital Certificate with the use of a Card) (DC-based Purchase Return) with consideration of provisions of Federal Law No.491-FZ dd.30.12.2020 “*On Purchase of Certain Types of Goods, Works, Services via Digital Certificate*” and (or) legal acts and regulations of the Russian Federation.

DC-based Purchase / DC-based Purchase Return shall be performed by Merchants in accordance with the Laws of the Russian Federation, System Standards and Regulations.

When performing daily settlement for DC-based Purchase / DC-based Purchase Return, the Bank of Russia acts as a Settlement Center, as well as a Central Payment Clearing Counterparty (within settlement with Participants).

The Acquirer shall submit DC-based Purchases for the payment clearing within forty five (45) calendar days upon receipt of the DC-based Purchase Transaction Authorization. If the Acquirer submits DC-based Purchases for the payment clearing after forty five (45) calendar days from the date of receipt of the DC-based Purchase Transaction Authorization, the Payment Clearing Center will refuse to accept such Transactions for payment clearing.

DC-based Purchase Return shall be performed by a Merchant that has performed the relevant DC-based Purchase. Funds (part of funds) paid for goods (works, services) via Digital Certificate with the use of a Card shall be returned.

The Acquirer shall submit the DC-based Purchase Return for the payment clearing within forty five (45) calendar days upon receipt of the DC-based Purchase Return Transaction Authorization. If the Acquirer submits the DC-based Purchase Return for the payment clearing after forty five (45) calendar days from the date of performance of the DC-based Purchase Return, the Payment Clearing Center will refuse to accept such Transactions for payment clearing.

Pre-court settlement procedure for disputes related to performance of (refusal to perform) the DC-based Purchase / DC-based Purchase Return in the Participants' Card Acceptance Network shall be applied in accordance with the System Standard *Dispute Resolution Guide*.

The following types of non-financial transactions shall be allowed to be made in the System:

1) *Balance Inquiry*

Providing information about the current balance of the Cardholder's bank account at the Cardholder's request with the use of the Card;

2) *PIN Change*

The Card PIN change at the Cardholder's request made with the use of the Card;

3) *Guarantee Request*

At a request of the Cardholder acting as an authorized representative of the Customer, a legal entity, provision of confirmation of funds sufficiency on a bank account of such Customer for the purpose of ensuring settlement between the Customer and counterparties.

A list of System products for which Guarantee request is allowed is provided in the System Standard *Mir Payment System Products*.

8.3. Transaction Performance Procedure

The Regulations contain the general Transaction execution procedures, additional requirements are provided in the System Standards.

8.3.1. Transaction Performance Environment

The following types of Transaction execution environment shall be envisaged in the System:

- Card-present, when the Cardholder and the Card are present at a place of the Transaction performance (attended by the Merchant's or the Acquirer's personnel or non-attended by the Merchant's or the Acquirer's personnel). In order to minimize the risk of Transactions not recognized by the Cardholder, Acquirers are recommended to ensure that Card-present transactions in the Acquirer's Card Acceptance Network are performed with the use of the contact or contactless interface of the Card microprocessor (chip) or contactless interface of the Cardholder's mobile device within the use of the mobile payments services. If a Transaction is performed with the use of the Card magnetic stripe (except for the cases stipulated in the System Standard *Methods of Cardholder Authentication when Performing Transactions*) or by manual entering of Card details and if subsequently the Transaction is not recognized by the Cardholder, the Acquirer shall be held accountable for the risks associated with such a Fraudulent Transaction;
- Card-not-present, when the Card and the Cardholder are not present at the place of Transaction performance (the Merchant's or the Acquirer's personnel do not have physical access to the Card).

8.3.2. Transaction Amount

Acquirers shall not have the right to set a minimum or a maximum Transaction amount (maximum Transaction amount setting limit shall not be applicable to Card-to-Card Transactions). The Operator may set a maximum limit for one Transaction for each type of Transaction.

8.3.3. Authorization

All Transactions in the System shall be performed via the Issuer's Authorization, including those on behalf or under the instruction of the Issuer with the use of the Stand-in Service.

The Issuer and the Acquirer are obliged to ensure the round-the-clock Authorization by their own efforts and (or) using the Stand-In Service.

The following types of Authorization are envisaged in the System:

- in the online mode, when Authorization is requested from the Issuer in the real time mode by sending an Authorization request to the Operations Center (Online Transaction);
- in the offline mode, when Authorization is made by the Card Payment Application without sending an Authorization request to the Operations Center (Offline Transaction).

Both types of Authorization are equivalent and both of them are considered to be an eligible expression of the Issuer's position with regard to the performance of the relevant Transaction in the Acquirer's Card Acceptance Network.

Transactions with the use of the contactless interface of the Cardholder's mobile device via the magnetic stripe or manual entry of the Card details shall be performed with Authorization in the online mode only.

Transactions with the use of the Card microprocessor (IC) may be performed with Authorization both in online and offline modes.

Offline Transactions shall be performed on the basis of authorizations set in the Card Payment Application by the Issuer.

When performing an Offline Transaction, the Acquirer shall ensure the check of the Offline Card limit. If the Transaction amount exceeds the Offline Card limit, the Authorization shall be executed online.

When performing an Offline Transaction, the Acquirer shall ensure that restrictions of the Card use are checked against the current Stop List.

In the event the Transaction is declined, the Cardholder shall be informed about the decline and the reason for it.

8.3.4. Cardholder Authentication Procedure

The Acquirer shall perform the Cardholder authentication using the authentication method set in the System Standard *Methods of Cardholder Authentication when Performing Transactions* depending on the Transaction type and performance procedure.

If a Transaction is performed without the Cardholder authentication using the authentication method set in the System Standard *Methods of Cardholder Authentication when Performing Transactions*, and if such Transaction is subsequently not recognized by the Cardholder, the Acquirer shall be held accountable for the risks associated with such a Fraudulent Transaction, except for the cases set in the System Standard *Methods of Cardholder Authentication when Performing Transactions*.

For the purpose of evidencing the fact of an attempt to authenticate the Cardholder with the use of the Secure Authentication Technology during the Transaction, when the Cardholder authentication by the Issuer with the use of the Secure Authentication Technology is not possible due to one of the reasons described in the System Standards that determine the procedure for the use of the Secure Authentication Technology, or when the Issuer does not support the Secure Authentication Technology, the System shall generate the NSPK-CAV cryptogram on behalf of the Issuer, verify the NSPK-CAV cryptogram and provide the verification results to the Issuer.

Starting from October 29, 2019, the Acquirer shall also be liable for risks related to the Transaction performance with the use of the Secure Authentication Technology and subsequent recognition of such Transaction as not recognized by the Cardholder when the Issuer supported MirAccept 2.0 Secure Authentication Technology while the Acquirer authenticated a Cardholder via MirAccept 1.0 Secure Authentication Technology. Liability for risks related to the Transaction performance via MirAccept 1.0 and 2.0 Secure Authentication Technology is set in accordance with the System Standard *Methods of Cardholder Authentication when Performing Transactions*.

8.3.5. Additional Requirements to Purchase Transaction and Cash Disbursement Transaction

The Acquirer shall submit Purchase and Cash Disbursement Transactions for the payment clearing within seven (7) calendar days upon receipt of the Transaction Authorization.

The Acquirer shall have the right to reverse a Transaction submitted earlier for the payment clearing only for the purpose of Transaction errors correction. The Acquirer shall submit the Transaction reversal for the payment clearing within forty-five (45) calendar days from the date of the Transaction performance.

Procedures for executing certain types of Card-not-Present Purchase Transactions related to mail or telephone order, recurring transactions, hotel accommodation booking and payments, car rental, etc. shall be provided in the System Standards.

8.3.6. Additional Requirements to Card-to-Card Transactions and Cash-to-Card Transactions

A Card-to-Card Transaction consists of two parts:

- debiting the payer's account (hereinafter – the Debit part of the Transaction);
- crediting the receiver's account (hereinafter – the Credit part of the Transaction).

A Cash-to-Card Transaction consists of only one Credit part.

Debit part of the Card-to-Card Transaction shall be transferred by the Acquirer for the payment clearing within seven (7) calendar days from the date of receipt of the Transaction Debit part Authorization.

Credit part of the Transaction shall not be transferred for the payment clearing as the Transaction Credit part Authorization request is also a clearing message with Participant's instructions regarding the Transaction.

The Issuer shall make the funds available to the Cardholder within 30 minutes after the performance of the Authorization of the Transaction Credit part.

Transaction Credit part reversal is prohibited.

The Acquirer shall be entitled to reverse the Debit part of a Card-to-Card Transaction previously sent for the payment clearing only for the purposes of the Transaction errors correction. The Acquirer shall submit the reversal of the Debit part of a Card-to-Card Transaction for the payment clearing within forty-five (45) calendar days from the date of the Transaction performance.

8.3.7. Additional Fees

Acquirers shall have the right to charge additional fees to Cardholders in cases and according to the procedures set in the System Standard *Acquirer's Additional Fees*.

8.3.8. Refund Transactions

The Refund Transaction shall be made at a Merchant if the Cardholder returns the goods (services, works) bought at the Merchant earlier and paid for with the Card (Card details). The Merchant shall have the right to decide whether to refund funds or not at its own discretion.

The Refund Transaction shall be made with the same Card with which the purchase of the goods (works, services) being returned was made at the Merchant. If the Cardholder is unable to present the Card used for the goods (works, services) purchase to the Merchant because of its loss, re-issue with a change of PAN, closure of the bank card account opened for Card Transactions, etc., the Refund Transaction shall be performed according to the Acquirer's internal procedure, requirements of the laws of the Russian Federation and the regulatory acts of the Bank of Russia, or of the laws applicable to the Acquirer. The amount of the Refund Transaction at the Merchant shall not exceed the amount of the Purchase Transaction.

The Refund Transaction shall be processed by the Acquirer and submitted for the payment clearing within seven (7) calendar days after the date of the Refund Transaction performance.

The return of funds shall be performed by the Issuer to the Cardholder within fifteen (15) calendar days from the date of the Refund Transaction processing.

The Acquirer shall have the right to reverse the Refund Transaction submitted earlier for the payment clearing only for the purposes of Refund Transaction errors correction. The Acquirer shall submit the Refund Transaction reversal for the payment clearing within fifteen (15) calendar days from the date of the Refund Transaction processing.

8.4. Source Documents. Requirements to Contents and Storage

A document (other than the cash register receipt) confirming the Card Transaction performance and containing the following details on such a Transaction (hereinafter referred to as the transaction receipt) shall be generated and issued for each Transaction successfully performed in the System's Card Acceptance Network:

- System name;
- Acquirer's name (optional for Transactions performed at Merchants);
- Merchant name;
- device ID;
- device location (address) (optional for e-commerce Transactions);
- masked PAN: four last digits of the Card number (PAN) are explicit, or not more than first six digits and last four digits of the Card number (PAN) are explicit. all other digits of the Card number (PAN) must be replaced with a masking symbol, e.g. "X", "*" or "#";
- Transaction date and time;
- Transaction type;
- Transaction currency;
- Transaction amount (if the Cardholder is charged with the Acquirer's Transaction fee, the cost of goods (works, services) and the amount of the commission (fee) charged shall be indicated separately);
- Transaction number;
- Authorization code;
- other details required by the System Standards, the laws of the Russian Federation or the laws applicable to the Acquirer.

A transaction receipt shall never contain the following information:

- Card PIN or a part of the Card PIN, or any data on the basis of which the PIN can be reckoned;
- Card Verification Value 2 (CVV2);
- Card expiration date.

A transaction receipt provided to the Cardholder shall be executed in hard copy or generated and sent to the Cardholder electronically to the subscriber's number or the email address specified by the Cardholder prior to the Transaction performance, provided that:

- for an ATM Transaction the transaction receipt shall be executed in hard copy as an ATM receipt. The Cardholder can opt not to receive the transaction receipt when offered by the ATM scenario during the cash disbursement;
- when performing a Card-present Transaction at the Cash Advance Office, the Electronic terminal transaction receipt shall be issued in hard copy. When performing a transaction with a Card issued by the Participant at the Cash Advance Office of this Participant, the Receipt may be issued in hard copy or sent to the Cardholder electronically in accordance with the procedure and under the terms specified by the agreement signed by and between the Participant and the Customer;
- when performing a Card-present Transaction at the Self-service terminal, the transaction receipt shall be issued in hard copy or sent to the Cardholder electronically; when performing a Card-present Purchase of Goods (Works, Services) at the Merchant via the Self-service terminal, it is allowed not to provide the transaction receipt to the Cardholder in cases when the laws of the Russian Federation or laws applicable to the Merchant allow no to provide the Cardholder with a document on card transactions confirming the performance of the latter (the source document);
- when performing a Card-present Transaction at the Merchant with a Merchant's authorized person, the transaction receipt shall be issued in hard copy or sent to the Cardholder electronically. It is allowed not to provide the Cardholder with the transaction receipt on Purchase of Goods (Works, Services) within the Instant Payment Service;
- when performing e-commerce Transactions, the source document shall be issued in soft copy and sent to the Cardholder.

If a Transaction is declined, the Cardholder shall be informed about the fact of and the reason for the decline. Such information shall be submitted as a paper receipt of the device/a record on the electronic device screen.

The Acquirer shall ensure the storage of source documents for Card Transactions performed in its Card Acceptance Network within the time specified by the laws of the Russian Federation or the laws applicable to the Acquirer.

8.5. Retained and Recovered Cards

A Card may be retained (recovered) in the Acquirer's Card Acceptance Network for the following reasons:

- a technical failure of the Acquirer's hardware and software system, ATM or the Self-service Terminal;
- a respective message from the Issuer or the Operations center in response to the Authorization request;
- Card in the stop-list with the "Captured Card" or "Fraudulent Transaction" Statuses.

In the event of a technical failure on the Acquirer's side:

- if the Cardholder requests the Acquirer to return the Card within five (5) business days after the Card capture, the Acquirer shall be entitled to return the Card to the Cardholder in accordance with the Acquirer's applicable regulations subject to the following:
 - the Acquirer checks the Card against the stop-list;
 - the Acquirer establishes the identity of the Cardholder;
 - the signature on the Cardholder's identity document matches the signature on the Card (if the Card has a Cardholder signature stipe);
- if the Cardholder does not claim the Card back after five (5) business days after the Card capture, the Participant shall destroy the Card in accordance with the Acquirer's applicable procedures.

When recovering a Card on the basis of the Issuer's or the Operations Center's instructions, or if the Card is in the stop-list with the "Captured" or "Fraudulent Transaction" statuses, the Acquirer shall take immediate action to stop any further use of the Card. The recovered Card shall be destroyed in accordance with the Acquirer's applicable procedure for destruction of invalid Cards.

8.6. Acquirer's Relationship with Merchants

The Acquirer shall sign a separate agreement with each Merchant serviced for the provision of acquiring services. This agreement shall define the relationship between the Acquirer and the Merchant in terms of Cards acceptance by the Merchant for payment for goods (works, services).

Before signing a Merchant Agreement, the Acquirer shall:

- according to the internal rules of the Acquirer, audit the Merchant's financial standing and make sure its activities are in line with the goals stated in the Charter (Articles of Association) and with the requirements of the laws of the Russian Federation or the law applicable to the Merchant. The Acquirer shall also make sure that no person who may undermine its goodwill is associated with the Merchant;
- ensure the Merchant screening using the Merchant screening service according to the procedure set in the System Standard - *Merchant Screening Service Guide*.

The Acquirer shall undertake to inform the Merchants about the System Regulations and Standards in the scope sufficient and necessary for conducting Card acceptance activity and shall make sure that the Merchants comply with these Regulations and Standards. To that effect, the Acquirer shall conduct training of the Merchant's employees on Card acceptance and security procedures.

The Acquirer shall ensure timely settlement for the Merchant and reimbursements for Card Transactions performed at the Merchant's.

The Acquirer shall ensure that the Merchant's interests are represented during the resolution of disputes related to Card Transactions performed at the Merchant's.

The Acquirer shall suspend Transactions at the Merchant's under the instructions of the Operator or at its sole discretion, if the Merchant activities may jeopardize the System reputation.

8.7. Requirements to Merchant Agreements

The Agreement between the Merchant and the Acquirer shall contain the following provisions:

- The Merchant shall have no right to deliberately perform any illegal Transaction (violating the Regulations and/or the laws of the Russian Federation or the law applicable to the Merchant), if the Merchant is aware or should be aware of its illegal nature, and the Acquirer shall have no right to deliberately accept such Transaction from the Merchant for processing;

- The Acquirer shall have the right to refuse to reimburse or to suspend the transfer of funds to the Merchant, if there is a suspicion that the Transaction is illegal or its illegal nature has been identified;
- The Acquirer's right to limit or terminate the agreement with a Merchant at the Operator's request;
- The Merchant shall have no right to:
 - refuse to accept Cards except for the cases provided by the System Regulations and Standards;
 - set the minimum and maximum amounts of a Purchase Transaction;
 - charge both explicit or concealed fees and any additional fees for Purchase Transactions;
 - set higher prices for goods (works, services) paid with the use of the Card as compared to payments made by other means or using cards of other payment systems;
 - offer/impose goods (works, services) during Card payments, that are not offered or imposed if the payments are made by other means or using cards of other payment systems;
 - request the Card number for the purposes other than to make a Purchase Transaction;
- Authorization shall be requested for all Transactions;
- all transactions shall be performed by the Merchant only in the event of a successful Authorization;
- a Card recovered (retained) at the Merchant's shall be handed over to the Acquirer within five (5) business days from the date of its recovery irrespective of the reason;
- The Merchant shall be responsible for the preservation, security and confidentiality of Cardholder and Card details data that became known to it in the course of its Card acceptance (servicing).

8.8. Requirements to Card Acceptance (Servicing) Points

The Acquirer shall display and have its Merchants display decals and other information signs with the System trademark, service mark, and logos on cash-registers, show-windows, front doors of stores and other points of sale, on ATMs, web-sites, in the mobile application and on other Card servicing devices to

indicate to Cardholders the places where Cards are accepted for payment. Requirements to the appearance of Card acceptance (servicing) points shall be provided in the System Standards.

In the event of termination of a Merchant agreement or termination of Card acceptance (servicing) in specific Acquirer's devices, the System logo/trademarks/service marks decals shall be removed within five (5) business days from the date of the Card acceptance (servicing) termination.

8.9. Procedure for Acceptance (Servicing) Cards Issued by the Bank of Russia within the Participants' Card Acceptance Network

Participants shall accept (service) payment cards issued by the Bank of Russia in accordance with the System Standard - *Terms of Acceptance of Mir Cards Issued by the Bank of Russia in the Mir Participants' Card Acceptance Network*, posted on the System's Information Resource, provided that the Bank of Russia and the Participant signed an agreement on the acceptance of Cards with the Mir trademark in the Participant's Card Acceptance Network. The specified agreement shall be concluded by way of the Bank of Russia posting an offer on the official web site (www.cbr.ru) of the Bank of Russia and by the Participant accepting it.

9. Funds Transfer Procedure

9.1. Non-Cash Transactions

The following forms of non-cash settlements shall be used in the System:

- by payment order;
- by collection order;
- on payee's demand (direct debiting);
- electronic money transfer.

9.2. Support of Transactions with the Payer Details if They are not Provided in the Order of the Participant's Customer

The Participants shall comply with the requirements of the laws concerning the Counteraction of the Legitimization of the Proceeds of Crime and the Financing of Terrorism applicable to the Participant with regard to the funds transfer being supported with the payer's details.

9.3. Funds Transfer and Settlement Currency in the System

Card Transactions in the System shall be performed:

- in RF Participants' Card Acceptance Network in Russian rubles, US dollars and euros. RF Participant shall be entitled to perform Transactions in other currencies as agreed with the Operator;
- in Non-RF Participants' Card Acceptance Network in the national currency. Non-RF Participant shall be entitled to perform Transactions in other currencies as agreed with the Operator.

Settlements between RF Participants for Transactions, as well as between RF Participants and the Operator, and the Payment Infrastructure Service Providers shall be effected in rubles.

Settlements between Non-RF Participants for Transactions, as well as between Non-RF Participants and the Operator, and the Payment Infrastructure Service Providers shall be effected, as agreed with the Operator, in currencies set by Non-RF Participants in the Application for Setting the Settlement Currency according to the form provided in the *Notification and Application Forms* Standard.

Conversion of the Transaction currency into the settlement currency shall be made at the System's rate quoted on the day of the payment clearing excluding the cases specified in the System Standards, for which conversion of the Transaction currency into the settlement currency is made at the System's rate

quoted on the day of the Transaction Authorization receipt. The procedure of informing the Participants about the System's rates of exchange shall be provided in the System Standards.

9.4. Transaction Performance in the System. General Procedure

All Transactions in the System shall be performed only subject to the strict observance of the following mandatory conditions:

- the amount of the Authorization request shall not exceed the Participant's Limit;
- the Issuer's Authorization for the requested Transaction shall be received;
- the amount of an Offline Transactions shall not exceed the amount of the Card Offline authorization limit set by the Issuer for the Card.

Participants shall transfer funds by the Cardholder's order executed with the use of the Card.

Transaction performance shall be evidenced by documents executed in hard copies and/or electronically. A Transaction document shall be the basis for the Transaction settlement and/or evidence that it has been performed. A Transaction document shall be executed in accordance with the requirements of the Regulations, regulatory acts of the Bank of Russia and the laws applicable to the Participant.

The Transaction Performance in the System shall be as follows:

- Cardholders shall identify themselves with the use of the Card, undergo the authentication procedure and initiate a Card Transaction using the client interface of the Acquirer's device;
- The Acquirer shall generate an Authorization request and send it to the Operations Center. In the event of an Offline Transaction, the Authorization is provided by the Card Payment Application without submitting an Authorization Request to the Operations Center. The moment when the Card Payment Application generates an Authorization Response is the moment of irrevocability of the Offline Transaction funds transfer;
- The Operations Centre shall identify the Card Issuer that initiated the Transaction according to the System Table of BINs and route the Authorization Request to the Issuer;
- The Issuer shall carry out the Transaction Authorization, generate a Response to the Authorization Request and send it to the Operations Center. At this moment the irrevocability of the Transaction funds transfer commences. When performing an Electronic Money Transfer Transaction, the Issuer shall carry out the Transaction Authorization, debit the balance of electronic funds of the Cardholder, who is the payer, generate a Response to the Authorization Request and send it to the Operations Center.

The irrevocability of the Transaction electronic money transfer commences at this moment. The finality of the electronic money transfer occurs at the time when the Participant servicing the Customer (the payee) credits the latter's balance of electronic funds. If the Authorization is impossible, the Issuer shall generate a response with the Transaction Decline and send it to the Operations Center;

- upon receipt of the Issuer's Authorization, the Operations Center shall send an Authorization Request Response to the Acquirer;
- pursuant to the Authorization Response received from the Operations Center, the Acquirer shall either allow the Cardholder to complete the Transaction or forbid the Transaction;
- based on the Transaction results, the Cardholder shall be provided with a document containing mandatory details as set forth by the Regulations (primary document), the laws of the Russian Federation or the laws applicable to the Participant, which shall determine the time of occurrence of the funds transfer unconditionality;
- at the close of business on the Transaction day, the Payment Clearing Center shall process the results of the Transactions submitted for payment clearing and generate Reports for the Participants and the Net Position Log for the Settlement Center;
- based on the Net Position Log, the Settlement Center shall debit or credit funds to all the Participants' accounts. The time the funds are credited to the Participant's account shall be the moment of finality of the funds transfer within the Transaction submitted for payment by the Participant;
- based on the Net Position Log, the Central Payment Clearing Counterparty transfers funds to Non-RF Participants conducting settlement without the Participant's Account opening with the Settlement Center or receives funds from Non-RF Participants conducting settlement without the Participant's Account opening with the Settlement Center. The time the funds are credited to the Central Payment Clearing Counterparty's bank (correspondent) account shall be the moment of finality of the funds transfer within the Transaction submitted for payment by the Non-RF Participant conducting settlement without the Participant's Account opening with the Settlement Center.

9.5. System Payment Clearing Procedure

The payment clearing procedure shall include the following actions:

- receipt, processing and verification of transaction orders received from the Participants as part of Outgoing Clearing Files;

- processing of payment orders received from Participants in messages being both the Authorization Requests and Clearing messages with Participant's instructions regarding the Transaction;
- calculation of the Net positions and of the Operator's fees for the provision of payment clearing services, transaction services and other services;
- Net Position Logs generation and submission to the Settlement Center and/or the Central Payment Clearing Counterparty;
- generation of Reports and Incoming Clearing Files and sending them to the Participants based on the payment clearing results.

9.6. Processing and Verification of Payment Orders Received from the Participants

The Participant shall submit transaction payment orders as part of the Outgoing Clearing File to the Payment Clearing Center.

The Payment Clearing Center shall process and control the compliance of the Outgoing Clearing File with the requirements established in the System Standards, as a result of which:

- no errors found in the Outgoing Clearing File. In this case, a report on successful processing of the file shall be sent to the Participant who submitted the Outgoing Clearing File (the report format is provided in the System Standards), and all the payment orders that are part of the file shall be accepted for execution and included in the payment clearing;
- errors found in the Outgoing Clearing File resulted in the Payment Clearing Center inability to accept the file in whole. In this case a report containing the information on the errors found shall be sent to the Participant who submitted the Outgoing Clearing File;
- errors found in the Outgoing Clearing File resulted in the Payment Clearing Center inability to accept some of the payment orders included in the File. In this case, a report on partial acceptance of the Outgoing Clearing File containing the information on the errors found shall be sent to the Participant. Successfully verified Payment orders for transactions shall be accepted for execution and included in the payment clearing.

The Payment Clearing Center may refuse to accept payment orders sent by the Participant for the payment clearing for the following reasons:

- The Outgoing Clearing File is generated with violation of the format requirements;
- The Outgoing Clearing File (or individual payment orders as part of it) was re-submitted by the Participant and had been subject to the payment clearing earlier;

- Payment orders (the first request for payment) were submitted by the Participant in time exceeding 364 (three hundred sixty four) calendar days from the date of the Transaction performance.
- Payment orders for DC-based Purchase / DC-based Purchase Return Transactions were submitted by the Participant in time exceeding forty five (45) calendar days from the date of the Transaction performance.

Upon the receipt from the Payment Clearing Center of a message of refusal to accept payment orders for the above reasons, the Participant shall remedy the findings, generate and forward a new Outgoing Clearing File if required.

9.7. Calculation of Clearing Positions

Based on the payment orders accepted from the Participants for execution, the Payment Clearing Centre shall:

- calculate the total amount of payment orders on Transactions in which the Participant is the payer;
- calculate the total amount of payment orders on Transactions in which the Participant is the receiver of funds;
- calculate, for each Participant's transaction, an interchange fee in accordance with the procedure and fee rates set in the *Interchange Fees* Standard;
- calculate, for each Participant's DC-based Purchase / DC-based Purchase Return, a fee in accordance with the laws of the Russian Federation;
- calculate, for each Participant's transaction, the Operator's fee for the provision of clearing and operational services in accordance with the procedure and fee rates set in the System's Fees;
- calculate the Participants' Net Positions.

RF Participant's Net Positions are calculated in rubles. Non-RF Participant's Net Positions are calculated in currencies set by Non-RF Participants in the Application for Setting the Settlement Currency according to the form provided in the *Notification and Application Forms* Standard.

Direct Participant's Net Position is calculated with the account of the Transactions of the Indirect Participant for whom the Direct Participant is a Sponsor. The net position of a Participant Payment System shall be calculated with the account of Transactions of the Participant Payment System's participants.

9.8. Net Position Log Generation and Submission to the Settlement Center and/or the Central Payment Clearing Counterparty

The Payment Clearing Center shall generate a Net Position Log and send it to the Settlement Center and/or the Central Payment Clearing Counterparty for settlement on a daily basis following the payment clearing results, on business days before 3 p.m. Moscow time one log for one day, or several Net Position Logs for several days, if these days were a weekend and/or a public holiday in the Russian Federation.

9.9. Payment Clearing Reports Generation and Submission to the Participants Based on the Payment Clearing Results

Based on the payment clearing results, the Payment Clearing Center shall generate and send the following documents to each Participant:

- Incoming Clearing File;
- Reports.

Requirements to the Incoming Clearing File and Reports shall be set in the System Standards.

The Payment Clearing Center shall send the Incoming Clearing File and Reports to the Participants on the day of the payment clearing performance.

The set and contents of other reports to the Participants on Transactions made with other Participants' cards in the Participant's Card Acceptance Network or on Transactions made with the Participant's cards in the Card Acceptance Network of other Participants shall be agreed with the Operator.

The Payment Clearing Center shall not be held liable for the non-delivery of Reports and Incoming Clearing Files occurred due to a fault of the Participant or its Third Party Processor.

9.10. Settlements

9.10.1. Procedure for Settlement with the Use of the Participant's Account Opened with the Settlement Center

The Participant, by acceding to the Regulations shall:

- grant the Settlement Center the right to charge the Participant's account, without any additional instructions from the Participant, the amounts of the collection orders generated by the Settlement Center on the basis of the Net Position Log received;

- grant the Operator the right to charge fees to the Participant's account in accordance with the System's Regulations, Fees and the *Interchange Fees* Standard by including the amounts of these fees in the Net Position.

Based on the Net Position Log received from the Payment Clearing Center, the Settlement Center shall generate payment orders and carry out settlements with the Participants within the following time frames:

- the Bank of Russia – on the date of receipt of the Net Position Log before 4 p.m. Moscow time;
- VTB Bank (PJSC):
 - if settlement with the Participant is carried out in rubles - before 4 p.m. Moscow time on the date of receipt of the Net Position Log;
 - if settlement with the Participant is carried out in the currency other than rubles - not later 4:00 p.m. Moscow time of the business day following the date of receipt of the Net Position Log and being the business day in the Russian Federation, in the country where the Participant conducts its business, and the country whose currency is used to carry out settlement between the Participant and the Settlement Center.

In the event of a debit Net Position, the Settlement Center performing the functions of the Central Payment Clearing Counterparty shall debit funds as their recipient:

- from the Direct Participant's Account based on the collection order in the amount of the Direct Participant's debit net position;
- from the Participant Payment System's Account based on the collection order in the amount of the Participant Payment System's debit net position.

In the event of a credit Net Position, the Settlement Center performing the functions of the Central Payment Clearing Counterparty shall credit funds as their recipient:

- to the Direct Participant's Account based on the payment order in the amount of the Direct Participant's credit net position;
- to the Participant Payment System's Account based on the payment order in the amount of the Participant Payment System's credit net position.

The Settlement Center shall notify each Participant of debiting or crediting funds to their account in accordance with the bank account agreement.

In the event of insufficient funds on the Participant's Account, or inability to debit funds from the Participant's Account (due to the bank account seizure, suspension of transactions, revocation of a license for banking transactions, revocation of the Permit, etc.):

1. The Bank of Russia acting as the Settlement Center and the Central Payment Clearing Counterparty, on the date of receipt of the log from the Payment Clearing Center, shall:

- notify the Operator of the uncovered debit net position of the Participant in accordance with the procedure specified in the agreement between the Operator and Settlement Center;
- interact with the Participant in accordance with the procedure provided for in the bank account agreement executed between the Settlement Center and the Participant;
- if the Participant's Account still has insufficient funds needed for the fulfillment of the Participant's obligations at 10:00 p.m. Moscow time or it is still impossible to debit the Participant's account due to the reasons mentioned above at 10:00 p.m. Moscow time, the Settlement Center shall notify the Operator thereof and fulfill the Participant's obligations at the expense of the funds stored in the Guarantee Fund at the Guarantee Fund Account opened with the Bank of Russia.

2. VTB Bank (PJSC) acting as the Settlement Center and the Central Payment Clearing Counterparty, on the date of settlement, shall:

- interact with the Participant in accordance with the procedure provided for in the bank account agreement executed between the Settlement Center and the Participant;
- if the Participant's Account still has insufficient funds needed for the fulfillment of the Participant's obligations at 4:00 p.m. Moscow time or it is still impossible to debit the Participant's account due to the reasons mentioned above at 4:00 p.m. Moscow time, the Settlement Center shall notify the Operator thereof according to the notification procedure specified in the agreement between the Operator and the Settlement Center and fulfill the Participant's obligations at the expense of the funds stored in the Guarantee Fund at the Guarantee Fund Account opened with the VTB Bank (PJSC).

The procedure of settlement between the Direct Participant and Indirect Participants, as well as between the Participant Payment Systems and participants of the Participant Payment Systems shall be governed by separate agreements concluded between them.

9.10.2. Procedure for Settlement with the Non-RF Participant conducting settlement without the Participant's Account opening with the Settlement Center

If Non-RF Participant conducts settlement without the Participant's Account opening with the Settlement Center, VTB Bank (PJSC) acting as the Settlement Center and the Central Payment Clearing Counterparty shall transfer to or receive from the Non-RF Participant funds in the amount of the Non-RF Participant Net Position based on the Net Position Log received from the Payment Clearing Center.

Settlement shall be carried out in currencies set by Non-RF Participants in the Application for Setting the Settlement Currency according to the form provided in the *Notification and Application Forms Standard*.

The business day specified in the present section shall mean a business day being the business day in the Russian Federation, in the country where the Non-RF Participant conducts its business, and the country whose currency is used to carry out settlement between the Non-RF Participant and VTB Bank (PJSC).

In the event of the credit Net Position, VTB Bank (PJSC) acting as a payer shall transfer funds to the Non-RF Participant in the amount equal to the credit Net Position of the Non-RF Participant based on the Net Position Log before 4:00 p.m. Moscow time of the business day following the day of the Net Position Log receipt.

VTB Bank (PJSC) shall transfer funds to the Non-RF Participant with the use of the bank details provided by the Non-RF Participant to the Operator according to the form established in the System Standard *Notification and Application Forms*.

In the event of the debit Net Position, the Non-RF Participant shall transfer funds to VTB Bank (PJSC) acting as a payee in the amount equal to the debit Net Position of the Non-RF Participant based on the Reports not later than on the business day following the day of the Reports receipt by the Non-RF Participant.

The Non-RF Participant shall transfer funds with the use of the bank details of VTB Bank (PJSC) posted on the System's Information Resource.

Non-RF Participant's obligations are considered to be fulfilled as from the date of funds crediting to the bank (correspondent) account of VTB Bank (PJSC) in the amount of the Non-RF Participant's debit Net Position.

If the Non-RF Participant fails to fulfill its obligations within the time frame set above, the Operator shall have the right to suspend the Transactions performance within the Non-RF Participant's Card Acceptance Network until the Non-RF Participant fulfills all its obligations in full.

If funds in the amount of the debit Net Position of the Non-RF Participant are not credited to the bank (correspondent) account of VTB Bank (PJSC) within two business days including the business day on which the Non-RF Participant should have transferred funds to VTB Bank (PJSC), VTB Bank (PJSC) shall fulfill the Non-RF Participant's obligations before 4:00 p.m. Moscow time of the third business day at the expense of the funds stored in the Guarantee Fund at the Guarantee Fund Account opened with VTB Bank (PJSC) and notify the Operator thereof according to the notification procedure specified in the agreement between the Operator and VTB Bank (PJSC).

The procedure of settlement between the Direct Participant and Indirect Participants shall be governed by separate agreements concluded between them.

10. System Functioning Time Specifications

The Operations Center processes Authorization Requests within the System twenty-four hours a day, seven days a week (24/7).

Moscow time shall be recognized as a unified time scale for payment clearing and settlement within the System.

Payment clearing in the System shall be conducted on a daily basis.

The Outgoing Clearing Files shall be accepted by the Payment Clearing Center daily until 9:00 a.m. on the payment clearing day. The Outgoing Clearing Files accepted after 9:00 a.m. shall be processed by the Payment Clearing Center on the following payment clearing day.

Reports and Incoming Clearing Files shall be generated and sent by the Payment Clearing Center on the payment clearing day.

Net Position Logs shall be generated and sent to the Settlement Center by the Payment Clearing Center on business days:

- before 3:00 p.m. of the business day on which payment clearing is carried out;
- before 3:00 p.m. of the business day following the day on which payment clearing is carried out, if this day is a weekend and/or a holiday according to the laws of the Russian Federation.

Settlement on the Net Position Logs for Participants' Accounts opened with the Settlement Center shall be effected by the Settlement Center:

- by the Bank of Russia – before 4:00 p.m. on the day of receipt of the Net Position Logs from the Payment Clearing Center;
- by VTB Bank (PJSC):
 - if settlement with the Participant is carried out in rubles - before 4 p.m. Moscow time on the date of receipt of the Net Position Log;
 - if settlement with the Participant is carried out in the currency other than rubles - not later 4:00 p.m. Moscow time of the business day following the date of receipt of the Net Position Log and being the business day in the Russian Federation, in the country where the Participant conducts its business, and the country whose currency is used to carry out settlement between the Participant and the Settlement Center.

Settlement with the Non-RF Participants conducting settlement without the Participant Account opening:

- for credit Net Positions of the Non-RF Participant - by VTB Bank (PJSC) acting as the Settlement Center and the Central Payment Clearing Counterparty - not later 4:00 p.m. Moscow time of the business day following the date of receipt of the Net Position Log and being the business day in the Russian Federation, in the country where the Non-RF Participant conducts its business, and the country whose currency is used to carry out settlement between the Non-RF Participant and VTB Bank (PJSC).
- for debit Net Positions of the Non-RF Participant - by the Non-RF Participant and VTB Bank (PJSC) acting as the Settlement Center and the Central Payment Clearing Counterparty - - not later than on the business day following the date of receipt of the Reports by the Non-RF Participant and being the business day in the Russian Federation, in the country where the Non-RF Participant conducts its business, and the country whose currency is used to carry out settlement between the Non-RF Participant and VTB Bank (PJSC).

11. Collateral for Participants' Obligations

11.1. General Provisions

In order to ensure that the Participant fulfills its financial obligations to other Participants in respect of Card Transactions, as well as the obligations to the Operator (including for the performance of functions of the Operating Center and Payment Clearing Center), the System shall envisage the following:

- setting the limits of the Participant's obligations (the Participant's Limit);
- creating the System Guarantee Fund at the expense of the Participants' guarantee fees
- provision of independent bank guarantees by the Participants;
- other ways of ensuring the fulfillment of the Participants' obligations agreed with the Operator (guarantee, security deposit).

11.2. Participant's Limit

In order to minimize financial risks in the System, the Operator shall be entitled to set limits of the Participant's obligations (the Participant's Limit) depending on the level of risk.

When setting the Participant's Limit, the Operator shall send a notification to the Participant via SEDO not later than on the business day following the day on which such Limit is set.

The Direct Participant's limit shall be set in accordance with the Operator's internal procedures on the basis of the Participant's comprehensive assessment, as well as its financial strength rating with consideration of the investment rating set by rating agencies, and all types of securities provided by the Direct Participant for proper execution of its obligations and those of its Indirect Participants within the System, i.e. guarantee fee, independent guarantee and other ways of ensuring the fulfillment of the Participants' obligations, agreed with the Operator.

Participant Payment System's Limit shall be set based on the size of its guarantee fee.

The Operator shall continuously monitor the Participant's Card Transactions in the Card Acceptance Network of other Participants, and Card Transactions of other Participants in the Participant's Card Acceptance Network to make sure that the amount of the Participant's financial obligations does not exceed the Participant's Limit set for the Participant by the Operator.

The Operator shall block Participant's Card Transactions and (or) Card Transactions in the Participant's Card Acceptance Network, if the amount of the Participant's financial obligations exceeds the Participant's Limit.

11.3. Guarantee Fund

The System Guarantee Fund (hereinafter - the Guarantee Fund) shall be created by the Operator in order to ensure the fulfillment of the Participants' obligations.

The Guarantee Fund shall be created in rubles and (or) foreign currency.

The Guarantee Fund shall be held in separate bank accounts opened by the Operator with the Bank of Russia and credit organizations.

When opening the Guarantee Fund Account with the Bank of Russia, the Account shall be ruble-denominated.

The Guarantee Fund shall be formed from the guarantee fees of the Participants and the Participant Payment Systems the calculation method of which is set in Appendix 3.

The Operator, the Central Payment Clearing Counterparty and (or) the Settlement Center are entitled to deposit funds into the Guarantee Fund in order to ensure the fulfillment of the Participants' obligations.

In order to complete settlement with Non-RF Participants to ensure System's Business Continuity, the Operator is entitled to perform actions aimed at purchase of the currency set by the Non-RF Participant in the Application for Setting the Settlement Currency according to the form provided in the *Notification and Application Forms* Standard using funds deposited on the ruble Guarantee Fund Account, and crediting of purchased currency to the Guarantee Fund Account opened in the currency of settlement with Non-RF Participant, provided that:

- in case of occurrence of a negative difference between the amount in rubles debited from the Participant's Account opened with the Bank of Russia and the amount to be credited to the Non-RF Participant in the currency of settlement with such Non-RF Participant, the Operator ensures completion of settlements at its own expense in the amount of such a negative difference;
- In case of occurrence of a positive difference between the amount in rubles debited from the Participant's Account opened with the Bank of Russia and the amount to be credited to the Non-RF Participant in the currency of settlement with such Non-RF Participant, funds in the amount of positive difference shall be credited to the Operator's settlement account.

Amounts of negative/positive difference shall be put down to the Operator's financial performance.

If the Operator performed actions to purchase currency to complete settlements, obligations within the System to Non-RF Participants must be considered fulfilled from the moment of debiting of funds in

the amount to be credited to the Non-RF Participant from the Guarantee Fund Account opened in the currency of settlement with the Non-RF Participant.

In order to complete settlements with the Participants to ensure the System Business Continuity, the Operator's funds may be used in the amount necessary to fulfill the obligations of the Participant. At the same time, the Operator is entitled to recover funds in the amount allocated for Participant's obligations fulfillment (excluding the above-mentioned negative difference between the amount in rubles debited from the Participant's Account opened with the Bank of Russia and the amount to be credited to the Non-RF Participant in the currency of settlement with such Non-RF Participant), at the expense of the Participant's Guarantee Fee.

RF Participants (both Direct Participants and Participant Payment Systems) shall ensure depositing of the Guarantee Fee in rubles into the Guarantee Fund Account opened with the Settlement Center that renders settlement services to the Participant within the System.

Non-RF Participants being Direct Participants shall ensure that the Guarantee Fee is deposited into the Guarantee Fund Account opened with the Settlement Center that provides settlement services to the Participant within the System, and (or) to the Guarantee Fund Accounts opened by the Operator with other credit organizations, in the currency of the relevant Guarantee Fund Account.

The Operator shall make sure the Participants pay the guarantee fee in full and in a timely manner, and shall monitor the use of funds from the Guarantee Fund.

The Operator shall recalculate the amount of the Participant's guarantee fee at least one (1) time every three months.

The Operator shall have the right to recalculate the Participant's guarantee fee amount at any time.

If the Participant's guarantee fee amount has been recalculated, the Operator shall send to the Participant a notification thereof via SEDO. The specified notification is sent only if the guarantee fee amount has been changed (increased or decreased).

The Participant shall be obliged to ensure replenishment of the Guarantee Fund amount to reach the new guarantee fee amount set by the Operator no later than by the business day following the day of receipt of the notification from the Operator via SEDO, unless a later deadline is specified in the notification.

In the event of a reduction of the Participant's guarantee fee amount, the Operator shall order the Settlement Center to transfer the amount exceeding the required amount of the new guarantee fee to the Participant's account opened with the Settlement Center no later than on the business day following the date of notification of the Participant.

The Participants shall have the right to pay the guarantee fee amount exceeding the guarantee fee amount set by the Operator to the Guarantee Fund, and at that:

- when replenishing the Guarantee Fund Account, the Participant shall specify “Voluntary transfer of a guarantee fee by the Participant (Participant’s identifier XXXX) in the amount exceeding the guarantee fee amount calculated by the Operator. Without VAT” in the “purpose of payment” field;
- it will be considered that the Participant’s guarantee fee has remained the same, if, during the further Participant’s guarantee fee recalculation by the Operator, the new amount of the guarantee fee is less or equal to the guarantee fee paid;
- the Participant shall have the right to request the Operator to recalculate the guarantee fee amount at any time according to the procedure set in the Appendix 3. In this case, within three (3) business days following the date of the Participant’s request submitted via the System Information Resource, the Operator shall recalculate the guarantee fee amount and send a notification on the new guarantee fee amount to the Participant via SEDO.

If the new Participant’s guarantee fee amount is less than the guarantee fee paid by such Participant, the Operator shall order the Settlement Center to transfer the amount exceeding the new guarantee fee amount to the Participant’s account opened with the Settlement Center not later than on the business day following the date of notification of the Participant on the new guarantee fee amount.

If the new guarantee fee amount of the Participant exceeds the guarantee fee amount paid by such Participant, the Participant shall be obliged to ensure replenishment of the Guarantee Fund account to reach the new guarantee fee amount set by the Operator within the time frames specified in the Operator’s notification.

In the event of use of the Guarantee Fund for the fulfillment of the Participant’s obligations, the Operator shall have the right to suspend the Participant’s Card Transactions and Card Transactions in its Card Acceptance Network, resulting in debiting the Participant’s account, until the funds used for the fulfillment of the Participant’s obligation are returned to the Guarantee Fund Account.

The Operator shall notify the Participant on the use of the Guarantee Funds for the fulfillment of the Participant’s obligations via SEDO.

The Participant shall be obliged to reimburse the amount of the Guarantee Funds used for the fulfillment of its obligations no later than by the business day following the day of use of the Guarantee Fund, unless a later deadline is specified in the notification.

If the amount of the Guarantee Fund used for the fulfillment of the Participant’s obligations exceeds the amount of its guarantee fee, the Operator shall have the right to collect:

- a fine in the amount of fifty thousand rubles (RUB50,000) for the initial use of the Guarantee Fund;
- a fine in the amount of seventy five thousand rubles (RUB75,000) for the second use of the Guarantee Fund within 12 months from the date of the first use of the Guarantee Fund;
- a fine in the amount of one hundred thousand rubles (RUB100,000) for subsequent cases of the use of the Guarantee Fund within 12 months from the date of the first use;
- interest on the use of the Guarantee Fund in the amount exceeding the Participant's guarantee fee amount at the rate of ten (10) percent per annum for each day of use of the above funds.

If the Operator has decided to collect a fine and (or) interest for the Guarantee fund use, the Operator shall send to the Participant an electronic notice on recovery of a fine and/or accrual of interest via SEDO and shall mail the original hard copies.

After the notice on recovery of a fine and/or accrual of interest for the Guarantee fund use is sent to the Participant, the Operator shall collect all fines and/or interests due by inclusion of all fine and interests amounts in the Net Position not earlier than three (3) business days from the date of the notice submission to the Participant via SEDO.

If it is impossible to include the fine and interests amount in the Net Position, the Participant shall pay the fine and interests for the funds use within five (5) business days from the date of submission of the notice on recovery of a fine and/or accrual of interest by the Operator to the Participant via SEDO using the bank details specified in the notice.

Should the Participant fail to reimburse the funds of the Guarantee Fund used for the fulfillment of its obligations to other Participants and (or) the Operator in excess of the Participant's Guarantee Fee amount, the Guarantee Fund shall be credited by the Operator at its own expense. In this case, the Operator shall have the right to collect the money used for the fulfillment of the Participant's obligations in accordance with the procedure established in Section 25 hereof.

In the event of System participation termination, the guarantee fee amount shall be returned to the Participant by the Operator in accordance with the Subsection 6.4 hereof.

The provisions of this section establishing the right of the Operator to hold the Guarantee Fund in separate Guarantee Fund Accounts opened with credit organizations that are not Settlement Centers, the right of the Central Payment Clearing Counterparty and the Settlement Center to deposit funds into the Guarantee Fund in order to ensure the fulfillment of the Participants' obligations, the right of the Operator to recover funds from the Participant's Guarantee Fee in the amount allocated for Participant's obligations fulfillment at the expense of the Operator, the procedure for calculating and paying the Guarantee Fee by

Non-RF Participants in a currency other than the ruble, as well as the procedure for the currency purchase by the Operator in order to complete settlement with Non-RF Participants, shall be applicable from February 24, 2022.

11.4. Independent Guarantee

As may be agreed with the Operator, the Direct Participant shall be entitled to provide an independent guarantee (hereinafter – the Guarantee) in order to ensure the fulfillment of its obligations within the System.

The Participants shall obtain the Operator's approval of the Guarantee currency, the Guarantee amount, the Guarantee validity period and the organization (credit organization established in accordance with the laws of the Russian Federation or a bank (credit organization) established in accordance with the laws of a foreign country and located outside the Russian Federation) (hereinafter - the Guarantor) providing the Guarantee to the Operator. The Operator accepts Guarantees for consideration only from organizations that meet the requirements set in the System Standard *Requirements to Organizations the Independent Guarantees of which are Accepted for Consideration to Ensure the Participants' Obligations Fulfillment*. The Guarantee amount shall not be less than the amount calculated with the use of the procedure for the Participant's guarantee fee amount calculation set in Appendix 3.

The Guarantee shall be irrevocable and shall contain the following details:

- Participant obligations the due performance of which is secured by the Guarantee;
- Operator's right to repeatedly lodge claims to the extent of the amount of the paid Guarantee within its validity period;
- Guarantor's obligations to perform the Participant's obligations within five (5) business days from the date of receipt by the Guarantor of the Operator's written claim to pay the sum of money under the Guarantee;
- Operator's right to perform indisputable direct debiting from the Guarantor of the amount due in case of the Guarantor's failure to perform the obligations under the Guarantee;
- the Guarantor's obligation to pay the Operator a penalty in the amount of 0.1% (point one percent) of the sum due to be paid for each calendar day of delay in the performance of obligations under the Guarantee;
- condition according to which the Guarantor's performance of obligations under the Guarantee shall be the actual arrival of funds to the Operator's account;
- lack of the Guarantor's right to unilaterally revoke the Guarantee.

The Guarantee shall be issued for the period and in the amount agreed by the Participant with the Operator.

The Participants shall be obliged to provide the Guarantee to the Operator in writing in hard copy. The Guarantee shall be effective on the day of its provision. It is allowed to submit a Guarantee issued for the new period prior to its effective date provided that:

- such new Guarantee is submitted not later than thirty (30) calendar days prior to the expiration of the previously issued (effective) Guarantee;
- such new Guarantee enters into force not later than the day following the expiration of the previously issued (effective) Guarantee.

The Operator shall either accept the submitted Guarantee or refuse to accept it within the period not exceeding thirty (30) business days from the date of its receipt and shall notify the Participant in writing in hard copy about the Guarantee acceptance or rejection.

The Operator shall refuse to accept the Guarantee, if one of the following grounds is present:

- Noncompliance of Guarantee conditions with the requirements of the present section;
- Availability of the information that the Guarantor has not issued the Guarantee;
- Revocation of the banking license from the Guarantor (credit organization established in accordance with the laws of the Russian Federation) by the Bank of Russia;
- Suspension, revocation (cancellation) of a special permit (license) to perform the correspondent type of activity (operation) from the Guarantor (bank (credit organization) established in accordance with the laws of a foreign country and located outside the Russian Federation).

The Operator shall return the Participant the Guarantee executed in writing in hard copy in one of the following cases:

- The Operator's refusal to accept the Guarantee;
- The obligation secured by the Guarantee has been performed in full scope, terminated or has not occurred;
- The Participant has provided another surety bond;
- The Guarantee has expired.

The Guarantee amount shall ensure fulfillment of Participant's obligation within the System. The Operator shall calculate the amount of collateral to be provided by the Participant to ensure fulfillment of its obligations within the System in accordance with the procedure for the Participant's guarantee fee amount calculation set in Appendix 3 at least once every quarter. The Operator is entitled to calculate the

amount of the required Participant's collateral in accordance with the procedure for the Participant's guarantee fee amount calculation set in Appendix 3 at any time.

If the calculated amount of Participant's collateral exceeds the amount of the Guarantee, the Operator shall send a notification to the Participant via SEDO stating that the Participant has to credit the guarantee fee amount exceeding the Guarantee to the Guarantee Fund Account. Not later than on the business day following the day of submission of the specified notification by the Operator via SEDO, unless a later date is specified in such notification, the Participant shall credit the guarantee fee set by the Operator to the Guarantee Fund Account.

If the Guarantor's banking license has been revoked / the Guarantor's special permit (license) to conduct the correspondent type of activity (operations) has been revoked (cancelled) or if, for any other reason, the Guarantee has become invalid or otherwise ceased to ensure the proper performance of the Participant's obligations to the Operator, the latter shall be entitled to suspend Participant's Card Transactions or Transactions in the Participant's Card Acceptance Network until the Participant provides a new Guarantee to the Operator, and (or) transfers the Guarantee Fee to the Guarantee Fund account according to the procedure set by the present Regulations, and (or) provides another surety bond within the System.

If the Participant's funds on the Participant's account are not sufficient for the fulfillment of its obligations in the System, the guarantee funds shall be used according to the procedure envisaged by these Regulations.

If the Participant fails to reimburse the Guarantee Fund used for the fulfillment of its obligations to the other Participants and (or) the Operator according to the procedure set by the present Regulations, the Operator shall have the right to demand the Guarantor to pay the relevant amount under the Guarantee.

11.5. Other Means for Collateral of Participant's Obligations

As may be agreed with the Operator, the Direct Participants shall be entitled to other means of collateral for their obligations within the System on the terms and for the amount agreed with the Operator.

The amount of the Participant's collateral shall ensure fulfillment of its obligations within the System. The Operator shall calculate the amount of collateral to be provided by the Participant to ensure fulfillment of its obligations within the System in accordance with the procedure for the Participant's guarantee fee amount calculation set in Appendix 3 at least once every quarter. The Operator is entitled to calculate the amount of the required Participant's collateral in accordance with the procedure for the Participant's guarantee fee amount calculation set in Appendix 3 at any time.

If the calculated amount of Participant's collateral exceeds the amount of the provided guarantee or security deposit, the Operator shall send a notification to the Participant via SEDO stating that the Participant has to credit the guarantee fee amount exceeding the guarantee or security deposit to the Guarantee Fund Account. Not later than on the business day following the day of submission of the specified notification by the Operator via SEDO, unless a later date is specified in such notification, the Participant shall credit the guarantee fee set by the Operator to the Guarantee Fund Account.

If the Participant's funds on the Participant's account are not sufficient for the fulfillment of its obligations in the System, the guarantee funds shall be used in the order envisaged by Subsection 11.3 hereof.

If the Participant fails to reimburse the Guarantee Fund resources used for the fulfillment of its obligations to the other Participants and (or) the Operator according to the procedure set by the present Regulations, the Operator shall have the right to recover payment from the collateral object provided by the Participant.

If, for any reason, the collateral object provided by the Participant has become invalid or otherwise ceased to ensure the proper performance of the Participant's obligations to the Operator, the latter shall be entitled to suspend Participant's Card Transactions or Card Transactions in the Participant's Card Acceptance Network until the Participant ensures the availability of funds on the Guarantee Fund Account in the size of the Participant's guarantee fee amount as determined by the Operator, and (or) until the provision of a new bank method of collateral to ensure the fulfillment of its obligations within the System.

12. Funds Transfer and Payment Infrastructure Services Payment Procedure

The procedure and frequency of payment for funds transfer services and the services of the payment infrastructure providers (except for the Settlement Center) in the System shall be determined by the Operator and shall be uniform for all Participants.

The amount and types of fees collected from the Participants or credited to them shall be determined by the System Regulations, Fees and the *Interchange Fees* Standard.

The Operator's fees shall be included in the calculation of the Net position. The Operator shall be entitled to issue invoices to the Participant for the services provided within the System, if it is impossible to include the Operator's fees in the Net position, as well as when the Participant is being connected, and Net Positions have not been generated for it yet.

Payments for the services within the System shall be made by the Direct Participants both for themselves and for the Indirect Participants for which the Direct Participant is a Sponsor.

Upon the services completion, the Operator shall generate the following documents confirming the fact of services provision to Participants (hereinafter - the Documents) with breakdown by each Participant:

- Services Acceptance Certificate (hereinafter – the Certificate);
- Tax Invoice (schet-factura) in cases provided for in the laws of the Russian Federation;
- Invoice for the services rendered for the accounting period (if the Operator's Fee is not included in the Net position). The specified invoices are generated for Direct Participants and Participant Payment Systems.

Documents confirming the services rendering to RF Participants shall be sent by the Operator to the correspondent Participants. The Operator and RF Participants shall exceed Documents according to the procedure stipulated in subsection 12.3 of the Regulations.

Documents confirming the services rendering to Non-RF Participants shall be sent by the Operator according to the following procedure:

- Documents confirming the services rendering to Direct Participants shall be sent by the Operator to the correspondent Direct Participants;
- Documents confirming the services rendering to Indirect Participants shall be sent to Indirect Participants via their Sponsor Direct Participants. The Sponsor Direct Participant shall ensure documents submission to its Indirect Participants in accordance with the agreement establishing their interaction procedure.

The Operator and Non-RF Participants shall exceed Documents according to the procedure stipulated in subsections 12.1 or 12.2 of the Regulations.

12.1. Procedure for Documents Exchange via SEDO and Hard-Copy Documents Exchange

The Operator shall forward the Documents to the Participant via SEDO not later than on the tenth (10th) business day of the month following the accounting period according to the procedure established by the *Mir Payment System OPCC Operational Procedure Manual*.

The Documents shall be considered received by the Participant on the date they were sent by the Operator via SEDO.

The Participant shall do as follows within fifteen (15) business days from the date on which the Documents were received via SEDO:

- pay the invoice for the services rendered during the accounting period by transferring funds using the bank details indicated in the invoice with mandatory indication of the invoice reference details in the “purpose of payment” field (applicable to Direct Participants in case the Operator’s fee is not included in the Net position);

or

- send to the Operator via SEDO a substantiated refusal to sign the Certificate according to the procedure established by the *Mir Payment System OPCC Operational Procedure Manual*.

The originals of the Documents in hard copy shall be forwarded by the Operator to the Direct Participant by post or by courier to the relevant Participant’s address within five (5) business days after the Documents were sent via SEDO. At the same time, the originals of the hard-copy Documents for Indirect Participants for which the Direct Participant is a Sponsor shall be sent to such Direct Participant.

The Documents in hard copy shall be considered received by the Direct Participant:

- if sent by post, on the tenth (10th) business day from the date on which the originals of the hard-copy Documents were sent (the Participant shall be entitled to request the Operator to provide the mailed item’s identifier);
- if delivered by courier, on the date the Documents were delivered.

Within five (5) business days upon the receipt of the hard-copy original of the Certificate from the Operator, the Direct Participant shall have the Certificate signed by an authorized person and stamped with the official seal, and send one copy of the Certificate by post or have it delivered to the Operator by courier to the following address: Chief Accountant, NSPK JSC, 11, Bolshaya Tatarskaya Street, Moscow, 115184, the Russian Federation.

If the Direct Participant submits a substantiated refusal to sign the Certificate via SEDO, the Direct Participant shall send its original in hard copy by post or have it delivered to the Operator by courier to the following address: Chief Accountant, NSPK JSC, 11, Bolshaya Tatarskaya Street, Moscow, 115184, the Russian Federation, within five (5) business days from the date of submission of a substantiated refusal to sign the Certificate via SEDO.

In the event of non-receipt by the Operator of the Certificate signed by the Direct Participant or of the original of a substantiated refusal to sign the Certificate within fifteen (15) business days from the date of receipt by the Direct Participant of the hard-copy Documents from the Operator, the services rendered within the System shall be considered duly rendered and fully accepted by the Direct Participant.

The Sponsor Direct Participant shall submit the Documents of the Indirect Participant in hard copy to the Indirect Participant within five (5) business days from the date of their receipt from the Operator.

The Documents of the Indirect Participant in hard copy shall be considered received by the Indirect Participant on the fifteenth (15th) business day from the date of their receipt by the Sponsor Direct Participant from the Operator.

Within five (5) business days upon the receipt of the hard-copy original of the Certificate the Indirect Participant shall have the Certificate signed by an authorized person and stamped with the official seal, and send one copy of the Certificate to the Sponsor Direct Participant. Within five (5) business days upon the receipt of the hard-copy original of the Certificate from the Indirect Participant, the Sponsor Direct Participant shall send this Certificate by post or have it delivered to the Operator by courier to the following address: Chief Accountant, NSPK JSC, 11, Bolshaya Tatarskaya Street, Moscow, 115184, the Russian Federation.

If the Indirect Participant submits a substantiated refusal to sign the Certificate via SEDO, it shall send the original of this Certificate to the Sponsor Direct Participant within five (5) business days from the date of submission of the substantiated refusal to sign the Certificate via SEDO. The Sponsor Direct Participant shall ensure the sending of the Indirect Participant's substantiated refusal to sign the Certificate in hard copy by post or by courier to the Operator to the following address: Chief Accountant, NSPK JSC, 11, Bolshaya Tatarskaya Street, Moscow, 115184, the Russian Federation, within five (5) business days from the date of receipt of such substantiated refusal.

In the event of non-receipt by the Operator of the Certificate signed by the Indirect Participant or of the original of a substantiated refusal to sign the Certificate within thirty (30) business days from the date of receipt by the Indirect Participant of the hard-copy Documents, the services rendered within the System shall be considered duly rendered and fully accepted by the Indirect Participant.

12.2. Procedure for Exchange of Hard-Copy Documents Only

If it is not possible to send the Documents via SEDO, the Operator shall send the original Documents in hard copy to the Direct Participant by registered mail to the Participant's address not later than the tenth (10th) business day of the month following the accounting period. At the same time, the originals of the hard-copy Documents for Indirect Participants for which the Direct Participant is a Sponsor shall be sent to such Direct Participant.

The Documents in hard copy shall be considered received by the Direct Participant:

- if sent by post, on the tenth (10th) business day from the date on which the registered mail was sent (the Participant shall be entitled to request the Operator to provide the mailed item's identifier);
- if delivered by courier, on the date the Documents were delivered.

Within fifteen (15) business days from the date of the hard-copy Documents receipt the Direct Participant shall:

- pay the invoice for services rendered during the accounting period by transferring funds using the bank details indicated in the invoice with mandatory indication of the invoice reference details in the "purpose of payment" field, and have one copy of the Certificate signed by the Participant's authorized person and stamped with the official seal delivered to the Operator by post or by courier to the following address: Chief Accountant, NSPK JSC, 11, Bolshaya Tatarskaya Street, Moscow, 115184, the Russian Federation;

or

- send a substantiated refusal to sign the Certificate to the Operator. The original of the substantiated refusal to sign the Certificate in hard copy shall be submitted by the Direct Participant to the Operator by post or by courier to the following address: Chief Accountant, NSPK JSC, 11, Bolshaya Tatarskaya Street, Moscow, 115184, the Russian Federation.

In the event of non-receipt by the Operator of the Certificate signed by the Direct Participant or of the original of a substantiated refusal to sign the Certificate within twenty-five (25) business days from the date of receipt by the Direct Participant of the hard-copy Documents from the Operator, the services rendered within the System shall be considered duly rendered and fully accepted by the Direct Participant.

The Sponsor Direct Participant shall submit the Documents of the Indirect Participant in hard copy to the Indirect Participant within five (5) business days from the date of their receipt from the Operator.

The Documents of the Indirect Participant are considered to be received by the Indirect Participant on the fifteenth business day from the date of their receipt by the Sponsor Direct Participant from the Operator.

Within fifteen (15) business days from the date of the hard-copy Documents receipt the Indirect Participant shall:

- have the Certificate signed by an authorized person of the Indirect Participant and stamped with the official seal, and send one copy of the Certificate to the Sponsor Direct Participant.

or

- send a substantiated refusal to sign the Certificate to the Sponsor Direct Participant. The original of the substantiated refusal to sign the Certificate in hard copy shall be submitted to the Sponsor Direct Participant.

The Sponsor Direct Participant shall ensure the sending of the Indirect Participant's Certificate or the substantiated refusal to sign the Certificate to the Operator by post or by courier to the following address: Chief Accountant, NSPK JSC, 11, Bolshaya Tatarskaya Street, Moscow, 115184, the Russian Federation, within five (5) business days from the date of receipt of the Documents from the Indirect Participant.

In the event of non-receipt by the Operator of the Certificate signed by the Indirect Participant or of the original of a substantiated refusal to sign the Certificate within forty (40) business days from the date of receipt by the Indirect Participant of the hard-copy Documents, the services rendered within the System shall be considered duly rendered and fully accepted by the Indirect Participant.

12.3. Electronic Documents Exchange Procedure

Electronic document flow (EDF) is a process of exchange of electronic documents, signed with a Qualified digital signature, between the Operator and the Participant.

Digital Signature (DS) is the information in the electronic form that is attached to the other information in the electronic form (information to be signed) or otherwise connected to such information and that is used for identification of the person who signs the information.

Qualified Digital Signature (QDS) is a type of the enhanced digital signature, the verification key of which is provided in the qualification certificate issued by an accredited Certification Authority.

EDF Operator is an organization ensuring the exchange of public and confidential information via telecommunication channels between the Parties in EDF system.

The Certification Authority is an organization whose function is creation and issuance of digital signature verification key certificates and other functions stipulated by the laws of the Russian Federation.

Electronic document flow envisages an electronic exchange of the following Documents (hereinafter - EED) by the Parties: Documents, Participant's substantiated refusal to sign the Certificate. When exchanging Documents, the Parties shall use the document formats approved by the Federal Tax Service or in the format provided by the Operator. A substantiated refusal to sign the Certificate may be forwarded by the Participant in any format.

In order to participate in EED signed by QDS via the EDF telecommunication lines, the Participant shall submit an application to the Operator in the form provided in the *Document Forms* Standard. Indirect Participants shall submit the specified application via their Sponsor Direct Participant.

For the purpose of checking the operability and(or) the interface of technical means of the Parties and (or) EDF Operators, the Parties shall conduct a test EED. The result of the test EED via EDF system shall be considered positive, if EED has been performed without errors and Parties' comments to EDF.

Following the test results, the Operator shall send to the Participant's address provided in the Application a confirmation of possibility/impossibility to conduct EDF and the date of the Electronic Document exchange commencement.

EED signed using a valid QDS shall be recognized equivalent to a hard-copy document signed by hand and shall cause legal consequences for the Parties in the form of determination, amendment and termination of mutual rights and obligations. Subject to these conditions, EED signed using QDS shall be recognized by the Parties as a source document, shall be used as an evidence in court proceedings, and shall be submitted to state authorities at their request.

QDS shall be acknowledged valid if all of the following conditions are observed:

- qualification certificate has been executed and issued by the Certification Authority whose accreditation is valid on the day of the issuance of the certificate;
- qualification certificate is valid on the moment of EED signing (provided that there is true information on the moment of signing) or on the day of validation of the said certificate, if the moment of EED signing is not determined;
- the ownership of QDS used for EED signing has been verified and the absence of changes made to this EED after its signing has been confirmed;
- QDS is used with due regard for the restrictions (if any) contained in the Qualification certificate of the person who signs EED.

The Parties shall inform each other about the following:

- QDS restrictions. Until the receipt of such notification, the Party is entitled to consider the other Party's QDS not encumbered with any restrictions, and EED signed by such QDS legally valid;
- impossibility to exchange EED signed using QDS in the event of a technical failure of the Parties' internal systems or EDF Operators. During such failure, the Parties shall exchange EED in accordance with subsection 12.1 hereof.

The Parties shall update their digital key certificates in advance. If they fail to observe this obligation, they shall immediately inform the other Party thereof.

The Confirmation of EED receipt by the Party (hereinafter – the Receiving Party) from the Party who sent them (hereinafter – the Sending Party) shall be electronic messages/confirmations of EED receipt from the Sending Party's EDF Operator. If the Sending Party does not receive such confirmations within one (1) business day following the day of EED sending, it shall contact its EDF Operator to find out the reason for non-receipt and, if necessary, shall send EED again.

If the Receiving Party is not able to accept EED (due to the impossibility to decipher EED, or if the Receiving Party's QDS is invalid and (or) EED intactness is violated), the Receiving Party shall send a notice of EED non-acceptance for processing to the Sending Party not later than one (1) business day following the date on which EED were sent and explain the reason for non-acceptance.

EED shall be considered not received by the Receiving Party until the moment of receipt by the Sending Party of a relevant confirmation.

The Operator shall forward EED signed using the Operator's QDS via EDF system to the Direct Participant or the Participant Payment System not later than the tenth (10th) business day of the month following the accounting period of services rendering.

The Participant shall do as follows within fifteen (15) business days from the date on which EED from the Operator were received via EDF system:

- forward the Certificate signed using the Participant's QDS to the Operator via EDF system;
- pay the invoice for the services rendered during the accounting period by transferring funds using the bank details indicated in the invoice with mandatory indication of the invoice reference details in the "purpose of payment" field;
- send a substantiated refusal signed using the Participant's QDS to sign the Certificate via EDF system.

In the event of non-receipt by the Operator of the Certificate signed using the Participant's QDS or a substantiated refusal signed using the Participant's QDS to sign the Certificate within fifteen (15) business

days from the date of EED receipt by the Participant via EDF system, the services rendered within the System shall be considered duly rendered and fully accepted by the Participant Payment System, the Direct Participant and the Indirect Participant.

If it is not possible to arrange EED according to the procedure set in this section due to the lack of the document exchange between EDF Operators of the Parties, the Operator and the Participant shall exchange EED in accordance with subsection 12.1 of the Regulations.

12.4. Fees and Procedure of Payment for the Settlement Center's Services

Fees and the payment procedure for the Settlement Center's services (other than the Bank of Russia) shall be determined by the Settlement Center and shall be uniform for all Participants.

The Payment for the services of the Settlement Center whose functions are performed by the Bank of Russia shall be uniform for all Participants and shall be executed in accordance with the regulatory acts of the Bank of Russia.

Fees of the Settlement Center whose functions are performed by the Bank of Russia shall be determined and put into effect according to the procedure set out by the Bank of Russia in accordance with the laws of the Russian Federation.

13. System Services

Value Added Service and Stand-In Service

Additional Verification (Value Added Service) and Stand-In Services are supported by the System to ensure its continuous operation.

The Stand-In Service allows to provide an Authorization response for and on behalf of the Issuer in such instances when:

- the Issuer is unavailable;
- No Issuer's response to the Authorization request was received within the set time frame (the maximum timeout for the Issuer's response is established in the System Standards);
- The Issuer's response to the Authorization request has the code indicating the necessity to use the Stand-in Service (Response Codes are listed in the System Standards);
- The Issuer's response to the Authorization request does not meet the requirements of the System Standards and cannot be interpreted by the System.

The Issuer shall have the right to independently determine the quantity and (or) cost parameters (Card and/or Card number range floor limits, in particular, per a transaction limit, Transaction amounts accumulative limit, accumulative limit for the number of Transactions for a certain number of days) for Stand-in of its Cards, and such parameters shall not be lower than the parameters provided for in the System by default.

The Issuer shall be responsible for the Transactions authorized via the Stand-in Service.

The exception file used during the Stand-In shall be generated by the Operations Center on the basis of the Issuers' respective requests.

The Issuer shall be responsible for the timely submission of the information to the Operations Center about Cards for which a negative response must be given in the Stand-In mode, as well as about Cards for which special exceptions are envisaged. A Card shall be included into the exception file by the Issuer with a corresponding attribute and accompanying parameters, if:

- the Card has been lost/stolen;
- the Card has been compromised;
- the Card Transaction must always be declined for any other reason;
- the Card must be captured;
- a positive Authorization response must always be given for the Card's transactions;
- an individual spending limit has been set for the Card.

As part of the Stand-In Service, Cards shall be automatically included in the exception file for ten (10) days if the Issuer's Authorization response contains the information that:

- the Card must be captured;
- the Card has been lost;
- the Card has been stolen.

Before the Card inclusion in the exception file, the Issuer shall bear full financial responsibility for the Card Transactions performed with the Card.

More information on the procedure for the Value Added Service and Stand-In Service rendering, as well as conditions for the services provision within those Services are specified in the System Standards.

Mobile Payments Services

In order to enable the Participants to perform Transactions via mobile devices within the System, there are mobile payment services that allow for the transaction performance via mobile devices with the use of a depersonalized alternative PAN (Token) in the Acquirer's Card Acceptance Network supporting payment via Card microprocessor contactless interface or from Merchants' mobile applications.

A separate BIN is used for Token generation. To obtain such BIN, the Issuer shall file an appropriate application to the Operator according to the form provided in the *Notification and Application Forms* Standard.

Procedure for the mobile payments services provision is described in the System Standards.

Other services may be provided within the System. Their procedures and terms of rendering shall be determined in accordance with the System Standards, Regulations and Fees.

14. Stop List

The use of the Stop List minimizes the Issuer's risks related to Offline Transactions.

The Operations Center shall generate Stop Lists on the basis of the Exception File comprising details of Cards for which the requirement to block Transactions and/or to capture the Card has been set.

The Operations Center shall send up-to-date Stop Lists to Issuers (on their Cards) and to Acquirers (on all Participants' Cards) via SEDO on a daily basis.

Before 00:00 a.m. MSK of the calendar day following the date on which the Operator provides the Stop List to the Acquirer, the financial responsibility for Offline Transactions made with Cards included in the Stop List shall be borne by the Issuer.

Starting from 00:00 a.m. MSK of the calendar day following the date on which the Operator provides the Stop List to the Acquirer, the financial responsibility for Offline Transactions made with Cards included in the Stop List shall be borne by the Acquirer.

The procedure for generation, distribution and use of the Stop List shall be determined in the System Standard.

15. Card Fraudulent Transaction Information

In order to counteract Fraudulent transactions with Cards/Card details or data compromise, each Participant shall inform the Operator about all fraudulent transactions with Cards.

The Operator's requirements to the provision of information on fraudulent activity shall be as follows:

- The Participant shall send a Fraudulent transaction message to the Operations Center not later than thirty (30) calendar days after the Participant becomes aware of the Transaction fraudulent nature;
- The Participant shall send a message informing the Operations Center about an event of possible compromise of Cards in the Acquirer's Card Acceptance Network within 5 (five) business days upon becoming aware of the fact of such compromise.

The procedure for submission of information and the message formats is provided in the System Standards.

The Information received from Participants shall be posted on the System Information Resource.

The Operator shall have the right to initiate assessment of compliance with the Regulations by the Participants associated with incidents of revealed fraudulent Card/Card details Transactions.

16. Participant Compliance

The Operator shall monitor the Participants' and Payment Infrastructure Service Providers' compliance with the Regulations.

16.1. Procedure for Monitoring the Participants' Compliance with the Regulations

Monitoring of Compliance with the Regulations may be preliminary (preventive) or conducted upon a violation detected.

The procedure for preliminary (preventive) monitoring of Participants' compliance with Regulations shall not require any grounds, such as suspicions or detection of a violation of any provisions of the Regulations. Within the procedure for preliminary (preventive) monitoring of Participants' compliance with Regulations, the Operator shall regularly monitor the Participants' activities within the System in accordance with the procedure and under the terms specified in the System Standards and Regulations including:

- collection, processing and systematization of Transaction information;
- collection and analysis of Participants' reports;
- check and analysis of data on an alleged breach of System Standards and Regulations by the Participant (if such data was received from System Subjects and(or) a third party);
- collection, processing and analysis of information about activities of organizations contracted by the Participant for the fulfillment of its obligations within the System and (or) related to the Participant's activities within the System;
- use of the test purchase method ('mystery shopper');
- inspections (audits) performance, etc.

For the implementation of the preliminary (preventive) monitoring of compliance with Regulations, the Operator is entitled to request from the Participant the information about its activities within the System including about its compliance/noncompliance with the requirements of the System Standards and Regulations. The Participant is obliged to provide the information required by the Operator within the timeframes set by the Operator in the request. Participant's failure to provide the required information and (or) respond to the Operator's request shall be considered a violation of the System Standards and Regulations.

Any System Subject may inform the Operator about an alleged violation of System Standards and Regulations by the Participant. A written notice on an alleged violation shall be delivered to the Operator, listing specific incidents that gave grounds to suspect a violation of the System Regulation by the System

Subject. The Operator may also use the information about the alleged violation of System Standards and Regulations by the Participant, that was received from a third party.

If the Operator reasonably believes that the information about the reported violation of the System Standards and Regulations has grounds, the Operator may send a written request describing the reported violation of the System Standards and Regulations to the Participant in respect of which the information about noncompliance with System Standards and Regulations was received within fifteen (15) calendar days from the date of receipt of such information. The Participant is obliged to provide the Operator with its explanations within the timeframes set in the Operator's request. Participant's failure to provide the required information and (or) respond to the Operator's request shall be considered a violation of the Regulations.

After establishing a fact of Participant's violation of System Standards and Regulations, the Operator shall send to the Participant a notification on the detected violation with the request to remedy this violation within the timeframes set by the Operator.

The Participant shall remedy all the violations revealed within the timeframes set by the Operator in the notification. The Operator may request the Participant to provide a remedy plan. Upon the detection of violations of the System Regulations and Standards, as well as in case of failure to remedy the detected findings within the timeframes established by the Operator, the Operator shall have the right to apply penalties to the Participant, including suspension of its participation in the System until the Participant remedies all the findings and (or) termination of its participation in the System.

The Operator is entitled to audit the Participant (check of premises, documents, procedure for carrying out procedures, etc.). The assessment (audit) may be conducted by a third party experienced in such audits. The Operator shall have the right to determine the frequency of assessments (audit) at its own discretion.

The Operator shall notify the Participant in writing of the offsite assessment (audit) procedure initiation at least thirty (30) calendar days prior to the offsite assessment (audit) date. The notification shall contain a plan of assessment (audit) with the list of System Standards and Regulations sections compliance with which will be assessed, as well as the timeframes of such assessment (audit) set by the Operator depending on the character of violation and expected consequences of such violations. The Operator shall have the right to extend the scope of assessment (audit), if facts of violations of the System Regulations and Standards, not originally determined in the assessment (audit) plan, are revealed during the assessment.

Within the period set forth in of the Operator's and/or of the engaged third party's request, the Participant being assessed shall provide the information requested by the Operator and/or the engaged third party in connection with the assessment (audit) and provide access to all the premises and documents related to the assessment (audit). The Participant shall ensure the completeness, accuracy, reliability, and integrity

of the information being verified. The Participant shall fully and promptly cooperate with the Operator in carrying out the assessment and, in the event the Operator involves a third party for the assessment (audit), entitle the Operator to communicate (disclose) such information and documents to such a third party.

In case of offsite assessment (audit) conducted upon a detected violation of System Standards and Regulations or a violation detected during the offsite assessment (audit), the Operator shall be entitled to require that the Participant reimburse expenses related to the offsite assessment (audit) by sending a relevant notification and a receipt to the Participant. The Participant shall pay the specified expenses within thirty (30) calendar days from the date of the invoice receipt.

Following the assessment (audit) results, within fifteen (15) calendar days from the assessment (audit) completion date, the Operator shall generate a report containing the detected violations and send a written notification about the detected violations and the report containing assessment (audit) results to the Participant. The Participant shall remedy all the violations of System Standards and Regulations revealed during the assessment (audit) within the period specified in the Operator's notice. The Operator shall have the right to request the Participant to provide a remedy plan. Upon the detection of violations of the System Regulations and Standards, as well as in case of failure to remedy the violations detected during the assessment (audit) within the timeframe established by the Operator, the Operator shall have the right to apply penalties to the Participant including suspension of its participation in the System until the Participant remedies all the violations, or until the termination of its participation in the System.

16.2. Procedure for Monitoring the Payment Infrastructure Service Providers' compliance with the Regulations

To implement control over the compliance of Payment Infrastructure Service Providers (excluding the Bank of Russia) with the Regulations, the Operator monitors the Payment Infrastructure Service Providers' activity within the System in accordance with the procedure set forth in Section 18 hereof.

Within the procedure for monitoring of Payment Infrastructure Service Providers' compliance with the Regulations, the Operator is entitled to:

- require the information about the Payment Infrastructure Service Providers' activity within the System including about the Payment Infrastructure Service Providers' activity compliance/noncompliance with the Regulations' requirements;
- initiate the procedure for assessment (audit) of the Payment Infrastructure Service Provider.

The Payment Infrastructure Service Provider shall be obliged to provide the information about its activity within the System required by the Operator within the timeframes set in the Operator's request.

In case of assessment (audit), the Operator shall notify the Payment Infrastructure Service Provider in writing of the onsite assessment (audit) procedure initiation at least fifteen (15) calendar days prior to such assessment (audit), and of the offsite assessment (audit) procedure initiation at least thirty (30) calendar days prior to such assessment (audit). Such notification shall contain the assessment (audit) plan with a list of the System Regulations sections the compliance with which will be checked, and the assessment (audit) timing.

The procedure for assessment (audit) of Payment Infrastructure Service Providers by the Operator may be specified in the relevant agreement entered into by and between the Operator and the Payment Infrastructure Service Provider.

17. Liability for Non-Compliance

The System Subjects shall be responsible for non-fulfillment/improper fulfillment of their obligations in accordance with the System Regulations, Standards, agreements and the laws of the Russian Federation.

The Participants' responsibility for compliance with the Regulations shall commence from the moment of their accession to the Regulations.

The System Subjects' liabilities for breach of their obligations shall be allocated in the following way:

- The Operations Center shall:
 - shall be liable to the Participants and other Payment Infrastructure Service Providers for failure to provide/inadequate provision of operational services;
 - shall be obliged to compensate the Participants and other Payment Infrastructure Service Providers for the actual damage inflicted as a result of non-provision (inadequate provision) of operational services;
- The Payment Clearing Center shall:
 - shall be liable for damages caused to the Participants and the Settlement Center by failure to provide/improper provision of payment clearing services;
 - shall be obliged to compensate the Participants and the Settlement Center for damage caused in the amount evidenced by documents;
- The Settlement Center:
 - shall be liable to the Participants for failure to provide/inadequate provision of settlement services under the bank account agreement;
- The Operator:
 - shall be liable to the Participants for failure to fulfill/improper fulfillment of its obligations;
 - shall be obliged to compensate the Participants for the damage caused in the amount evidenced by documents;
 - shall not be liable for violation by the Participant and/or persons affiliated with it of the laws applicable to such Participant and/or persons affiliated with it. The Operator shall not reimburse the Participant and/or persons affiliated with it for fines and other losses incurred by the Participant and/or persons affiliated with it due to their incompliance with the applicable laws. An affiliate person of a Participant shall mean any individual or legal entity that directly or indirectly controls the Party, is controlled by the Party or is under the common control with

- such Participant as well as any individual or legal entity that may be deemed an affiliate with the Participant in accordance with the applicable laws. Control shall mean (with regard to a legal entity) legal or actual rights to directly or indirectly (via one or several intermediaries) manage or handle the policy of such legal entity or make decisions on appointment of the majority of its directors or the chief executive officer;
- shall not be liable for violation by the Participant and/or third parties involved by the Participant for the performance of activities within the System of the laws applicable to such Participant and/or third parties, including if the country of registration of the Participant and/or third parties involved by it differs from the country where such Participant and/or third parties involved by it conduct their business.
- Participants:
 - shall be liable to the System Subjects for their actions/inaction within the System, as well as for the actions/inaction (including fraud) of third parties engaged by the Participant to carry out activities in the System, including any violation of the System Regulations and Standards caused through the Participant's fault;
 - shall be liable for violation by the Participant and/or third parties involved by the Participant for the performance of activities within the System of the laws applicable to such Participant and/or third parties, including if the country of registration of the Participant and/or third parties involved by it differs from the country where such Participant and/or third parties involved by it conduct their business;
 - shall be obliged to compensate the Operator at its request for damages caused by inaccuracy of warranties and/or representations provided by the Participant in accordance with Section 23 hereof, should such warranties and representations be violated or should such warranties and representations be inaccurate;
 - shall be obliged to compensate the System Subjects for the documented damage caused by actions/inaction of the Participant, as well as for actions/inaction of third parties engaged by the Participants to carry out activities within the System.

The Participants shall be responsible for failure to fulfill/improper fulfillment of the conditions of positioning and use of the System trademark, service marks and logos, determined by the Regulations, as well as for misrepresentation of the System trademark and service mark.

If the Participant violates the System Regulations and Standards and if it fails to remedy the violations revealed by the Operator within the timeframe established by the Operator, the Operator shall be entitled to charge penalties and apply other sanctions, including the suspension of Participant's Card Transactions and Card Transactions in the Participant's Card Acceptance Network, and suspension or termination of its participation in the System in accordance with the procedure set by the Regulations. Determining the relevant corrective action shall be acknowledged an absolute and sole right of the Operator.

The following fines shall be envisaged in the System:

Violation	Fine amount
a) violation of any provision of the Regulations and System Standards except for those specified in clause b) and c):	
• first violation of any provision of the System Regulations and Standards	RUB 50,000
• second violation of the same provision of the System Regulations and Standards within twelve (12) months after the first violation	RUB 250,000
• third violation of the same provision of the System Regulations and Standards within twelve (12) months after the first violation	RUB 500,000
• fourth and further violations of the same provision of the System Regulations and Standards within twelve (12) months after the first violation	RUB 1,000,000
b) violation of the procedure for the System trademarks (service marks) and logos placement and use:	
• for each violation	RUB 500,000
c) violation of requirements of the System Standard. Requirements to High-risk Activities at the Acquirer in term of violation by the Participant of obligations to control prohibited Merchant business activities:	
• for each violation	RUB 500,000

When making a decision on the exaction of a fine or taking another corrective action, the Operator shall take into account the type and frequency of the violation occurrence, the nature of damage (including financial) incurred by the System Subjects, the Participant's ability to remedy the violation, and the violation consequences for the security and business continuity of the System.

Should a corrective action be taken in respect of a Participant, the Operator shall send a notice containing the following information to the Participant:

- corrective action;
- reasons for corrective action;
- fine to be collected;

- bank details for fine payment (in case of inability to include the amount of fine in the Net Position);
- remedy deadlines.

The Operator shall send a notice to the Participant via SEDO with further mailing of the notice original in hard copy.

Should a corrective action be taken in respect of an Indirect Participant, the Operator shall send a notice both to the Indirect Participant and the Direct Participant (the Sponsor of such Indirect Participant) via SEDO with further mailing of the notice original in hard copy.

Not earlier than three (3) business days from the date of the notice submission to the Participant via SEDO, the Operator shall collect all fines due by inclusion of the fine amount in the Net Position within the settlement with the Participant. The amount of fines to be collected from the Indirect Participant is included in the Net Position of the Direct Participant that is the Sponsor of this Indirect Participant.

If it is impossible to include the fine amount in the Net Position, the Participant shall pay the fine within five (5) business days from the date of the notice submission by the Operator via SEDO. The Direct Participant shall pay the fine both for itself and for the Indirect Participant sponsored by it.

Should the Participant disagree with the findings, it shall have the right to send a written objection to the Operator containing a substantiation of the Participant's standpoint within thirty (30) calendar days from the date of the violation notice receipt from the Operator.

No objection sent by the Participant shall release it from the liability to pay the fine.

The Operator shall review the Participant's objection within fifteen (15) business days from the date of its receipt by the Operator.

If the Operator makes a positive decision based on the results of the review of the Participant's objection, the amount of the fine collected shall be returned to the Participant within ten (10) business days.

The System Subjects shall be exempt from the liability for partial or complete non-fulfillment/improper fulfillment of their obligations as defined in the System Regulations and Standards, if such non-fulfillment/improper fulfillment is a result of occurrence of force majeure circumstances (force majeure), i.e. emergency circumstances, unforeseen circumstances, and unavoidable circumstances that could not have been reasonably anticipated or prevented via reasonable measures and means.

Force majeure events shall include flood, fire, earthquake and other acts of God, as mass diseases (pandemics, epidemics), strikes, warfare, hostilities, acts of terrorism, acts or actions of government and(or) local authorities, and any other circumstances that prevent the System Subjects from duly fulfilling their obligations hereunder and are beyond the System Subjects' control.

In the event of force majeure circumstances specified in this section, System Subjects shall immediately, but not later than five (5) calendar days from the date of their occurrence, notify the Operator thereof in writing using any available means letting to identify the fact of notification sending and receipt. The notice shall contain the information on the nature of the circumstances and, where possible, the information allowing to assess their impact on the possibility of fulfillment by the System Subjects of their obligations within the System.

At the Operator's request, the System Subject affected by force majeure events shall provide an official document issued by the relevant authorized organization responsible for certification (averment) of such circumstances. This document is deemed to be a reliable confirmation of the force majeure events if their occurrence and effect cannot be established by the Operator as a commonly-known fact (e.g., from the mass media at the Operator's location).

Should the System Subject fail to send or untimely send the notice, it shall compensate the other System Subjects for the losses incurred by them and shall not be entitled to refer to force majeure circumstances.

Upon the termination of the above circumstances the System Subject that was not able to fulfill its obligations due to force majeure shall notify the Operator in writing thereof within five (5) business days after their termination. The notice shall indicate the period during which the System Subject intends to fulfill its obligations within the System.

The System Subject that refers to force majeure events pursuant to this Section shall take all reasonable measures to mitigate losses caused by force majeure events and to fulfill its obligations according to System Standards and Regulations whose fulfillment was breached or became impossible due to such events.

In the event of force majeure circumstances hampering the fulfillment of the System Subjects' obligations, the period of fulfillment of such obligations by the System Subjects shall be extended for the duration of such circumstances, as well as the time required for the elimination of their consequences.

18. System Business Continuity (BC) Procedure

18.1. General Provisions

The Operator shall ensure the System Business Continuity (hereinafter referred to as SBC) by complying with the requirements of Federal Law No.161-FZ dd. 27.06.2011 *On the National Payment System* and regulatory acts accepted pursuant thereto, the System Regulations and Standards (hereinafter referred to as the requirements to the services rendering) and(or) recovery of the payment infrastructure services rendering in case of their suspension within the timeframe set by the Operator.

The System operation is considered to be continuous when the System ensures the operational, payment clearing, and settlement services rendering to the Participants without violation of the services rendering recovery timeframe in case of their suspension, as well as without violation of the timeframe of recovery of services rendering prior to services rendering compliant with the requirements to services rendering.

The System operation suspension (termination) shall be considered the failure to render at least one payment infrastructure service and (or) the failure to transfer funds to all Participants within more than two (2) hours.

The timeframe within which the payment infrastructure services rendering (if suspended) shall be recovered shall not exceed two (2) hours from the moment of the services suspension (termination).

The timeframe within which the payment infrastructure services rendering according to requirements to the services rendering (in case of violation of the specified requirements) shall be recovered shall not exceed twenty-four (24) hours from the moment of detection of the specified requirements violation.

The Operations Center shall process at least 80% of Authorization Requests within 2 seconds during a calendar month when rendering payment infrastructure services;

- this threshold parameter is considered to be the reference standard of the Operations Center's payment infrastructure services.

The Payment Clearing Center shall generate and submit Net Position Logs based on the payment clearing results to the Settlement Center on business days before 3:00 p.m. Moscow time on a daily basis;

- this threshold parameter is considered to be the reference standard of the Payment Clearing Center's payment infrastructure services.

The time of deviation from the Settlement Center's set timeframes for settlements on the Net Position Logs shall not exceed twenty-four (24) hours for the one-time violation of the Settlement Center's set timeframes;

- this threshold parameter is considered to be the reference standard of the Settlement Center's payment infrastructure services.

Suspension (termination) of payment infrastructure services rendering to one or several Participants and (or) information exchange between the Operator and the Payment Infrastructure Service Provider occurred during Transactions processing during the period of maintenance works by the Payment Infrastructure Service Provider shall not be considered an Incident provided that the Payment Infrastructure Service Provider provides System Subjects with information about timeframes for the specified maintenance works in advance.

Maintenance works shall mean activities carried out by the Payment Infrastructure Service Provider to support the operation of automated systems ensuring functioning of the Operational and Payment Clearing Center for the purpose of their proper use, as well as activities comprising corrective actions (necessary or desirable) taken to eliminate Incidents and operational problems, preventive measures, as well as modernization of hardware and(or) software.

To mitigate adverse effects on SBC, the Operator shall establish the System Business Continuity (SBC) Procedure comprising:

- System Risk management;
- System Business Continuity management;
- Organization of the Operator's communication with the Payment Infrastructure Service Providers and Participants;
- Control over the Payment Infrastructure Service Providers' and Participant's adherence to the SBC Procedure.

Requirements listed in Section 18 hereof are not applicable to the Bank of Russia acting as the Settlement Center.

18.2. System Risk Management

The System Risk Management is set out in the *NSPK JSC Risk Management and Internal Control Policy*, *NSPK JSC Business Continuity Policy*, *Mir Payment System Risk Management Committee Regulations* and *the Method for NSPK JSC Non-financial Risks Evaluation and Assessment* posted on the System Information Resource.

18.2.1. System Risk Management Model

In the System risk management model, the risk assessment and risk management functions shall be allocated among the Operator and the System Subjects. The Operator shall determine its own risk management structure and functional duties of risk management employees, as well as set risk management requirements to the System Subjects.

In order to ensure SBC, the System Subjects shall independently manage the risks inherent to the type of their activity and status in the System. The risk management system of each System Subject shall include, without limitation, the appointment of responsible employees and/or vesting the units responsible for the risk management and development of internal risk management regulations. It shall also evaluate the activities of the System Subjects as a whole, including the activities not associated with participation in the System, if such activities may become a source of risks affecting the ability of the System Subject to comply with these Regulations or meet the System participation criteria. The System Subjects shall be responsible for the risks occurrence in their activities in accordance with the Regulations, the laws of the Russian Federation and the laws applicable to the Participant.

18.2.2. Operator's Risk Management Organizational Structure

The Operator's risk management structure consists of:

- Supervisory Board;
- Chief Executive Officer;
- Management Board;
- Managers and employees of the Risk Management Division;
- other units within their functional duties;
- Mir Payment System Risk Management Committee.

Risk management shall be carried out by the Operator's employees and structural units within their authorities. The functional duties of units responsible for the System risk management shall be as follows:

- development and approval of internal risk management documents;
- continuous risk detection, analysis, and assessment;
- control over the adherence to the Operator's Regulations, methods and policies establishing the risk management procedure;
- amendment of the Operator's Regulations, methods and policies establishing the risk management procedure to improve the risk management system;
- drawing up recommendations regarding risk management;

- other duties for the purpose of risk management.

The risk management responsibilities of the Operator's units within the System shall be set forth in the Operator's regulations, orders, job descriptions and other internal documents.

The information about risks shall be brought to the attention of the Operator's CEO, Mir Payment System Risk Management Committee, Managing Board and the Supervisory Board by the correspondent Operator's units in accordance with the procedure and within the timeframes specified in the Operator's internal regulatory documents.

The System Subjects shall independently determine their own organizational risk management structure within the System in accordance with the regulatory acts of the Bank of Russia or the laws applicable to the Participant.

18.2.3. Risk Management Collective Body

A collective risk management body (Mir Payment System Risk Management Committee (hereinafter referred to as the Committee)) is established within the System. The Committee is composed of the Operator's, the Payment Infrastructure Service Providers' and the Participants' representatives responsible for the System risk management. The representatives of the Bank of Russia with a consultative vote may also be the Committee members. The main tasks of the Committee are the proposals examination and drawing up of recommendations for the System risk management improvement. The Committee's functional duties and competencies are as follows:

- establishing the risk management system assessment criteria, including the systemic risk;
- conducting the assessment;
- drawing up proposals and recommendations based on the risk management assessment findings.

18.2.4. Types of Risks in the System

The Operator shall identify the following main types of risks in the System:

- The System Credit Risk is a Participant's risk of failure to fulfill contractual obligations to the Settlement Center and the Central Payment Clearing Counterparty within the set timeframes or in the future, and, as a consequence of this, the risk of improper payment infrastructure services rendering. The System Credit Risk occurrence is related to the Participant's inability to perform its financial obligations in time and in full scope within the System. The occurrence of such risk may lead to the Operator's financial losses.

The Operator's Risk Management Division employees regularly (at least quarterly) assess the Participants' and Payment Infrastructure Service Providers' financial status and, if required, use various risk management measures according to the Regulations requirements including as they relate to the Participant's Guarantee Fee generation, the Participant's Limit setting, Operator's blocking of Participants' Card Transactions and Card Transactions in the Participants' Card Acceptance Network, Participant's System participation suspension, etc.;

- The System Liquidity Risk is a risk of the Central Payment Clearing Counterparty's and/or Participants' lack of funds sufficient for the timely fulfillment of their obligations to other System Subjects and resulting in the SBC violation and improper payment infrastructure services rendering.

The management of this risk is performed by regular monitoring of the Operator's, Participants', and Payment Infrastructure Service Providers' financial status by the authorized Operator's units. The System Liquidity Risk management methods are used in accordance with the System Regulations and internal risk management documents of the System Subjects;

- The Overall System Commercial Risk is a risk of loss occurrence (default risk) and deterioration in the Operator's and (or) Payment Infrastructure Service Providers' financial state resulting from the reduction in revenue and (or) increase in expenses of the Operator and (or) the Payment Infrastructure Service Providers, that will lead to the SBC violation. The Overall System Commercial Risk is not related to the occurrence of the System Credit Risk and System Liquidity Risk;
- The System Operational Risk is a risk of SBC violation resulting from the System Subjects' IT faults, malfunctions, and failures, errors in arrangement and performance of technological and management processes, errors or wrongful acts of System Subjects' employees, or resulting from the events the occurrence of which is not related to the System Subjects' activities including emergency situations, erroneous or illegal acts of third parties.

To manage the System Operational Risk, the Operator shall:

- apply the principles of separation and limitation of functions, powers and responsibilities of the Operator's employees, collective decision-making, and shall use the dual control mechanisms when performing its activities;
- organize the backup of hardware and software suites and information resources, backup of technically important communication channels and media;

- ensure the continuity of information and telecommunication systems used in the System, improve their reliability via the backup of hardware and software suites, information resources and communication channels;
 - develop, check (test) and review action plans aimed at the provision of the Operator's business continuity and disaster recovery at least once in two years;
 - use fault-tolerant equipment and data backup servers;
 - apply procedures protecting data from loss, damaging or accidental destruction, as well as enabling data recovery after software failures;
 - perform daily monitoring of Incidents (including the Information Security Incidents) that may affect SBC;
 - monitor key risk indicators;
 - use licensed software, stable communication channels and data copying systems;
 - set the requirements governing the basic and most important aspects of activities within the System in the System Regulations and Standards, as well as the requirements to the System Subjects aimed at ensuring that their functional, technological and other capabilities are in line with the Regulations. The Payment Infrastructure Service Providers shall be responsible for the management of Operational Risks related to their payment infrastructure services rendering within the System;
- The System Legal Risk is a risk of SBC violation and improper payment infrastructure services rendering resulted from the System Subjects' incompliance with the current laws of the Russian Federation, regulatory acts of the Bank of Russia, the System Regulations and Standards, agreements entered into by and between System Subjects, Operator's documents, and documents of the Payment Infrastructure Service Providers, or resulted from conflicts of laws and(or) lack of legal clarity in the laws of the Russian Federation, regulatory acts of the Bank of Russia, the System Regulations and Standards, agreements entered into by and between System Subjects, as well as resulted from the Payment Infrastructure Service Providers' being under the jurisdiction of different countries.

All System Subjects shall ensure the System Legal Risk management within their activity in the System. To manage the System Legal Risk, the Operator develops the System Regulations and Standards enabling the Participants to uniformly determine their rights and obligations and sets a transparent structure of contractual relations within the System.

18.2.5. SBC Parameters

The Operator determines and controls the compliance with the following SBC parameters:

- A parameter (hereinafter referred to as P1) of the payment infrastructure services recovery time within which the payment infrastructure services shall be recovered, if suspended including as a result of violation of requirements to data protection when transferring funds, established in Statement No.382-P dd. 09.06.2012 of the Bank of Russia *On Requirements to Data Protection when Transferring Funds and the Procedure for Monitoring by the Bank of Russia of Compliance with the Requirements to Data Protection When Transferring Funds*. The P1 threshold value for the operational, payment clearing, and settlement services is two (2) hours. P1 value for each Payment Infrastructure Service Provider and each Incident resulted in the payment infrastructure services suspension shall not exceed the threshold value;
- A parameter (hereinafter referred to as P2) of the payment infrastructure services continuity. This parameter is used to describe a period of time between two consecutive System events that led to violation of payment infrastructure services rendering (compliant with services rendering requirements) including due to the violation of requirements to data protection when processing Transactions, that resulted in the payment infrastructure services rendering suspension. The P2 threshold value for the operational and payment clearing services is twenty-four (24) hours, and the P2 threshold value for the settlement services is thirteen (13) hours. Such P2 value for each Payment Infrastructure Service Provider shall not be less than the set threshold value;
- A parameter (hereinafter referred to as P3) of the Operations Center's compliance with the operational services requirements (a parameter of compliance with the rule). This parameter describes the ratio of the number of Transactions for which operational services were rendered without violations to the total number of Transactions for which the operational services were rendered. P3 threshold value is 99,8%. P3 value shall not be less than the set threshold value. The rule for the procedures performance is processing of authorization messages by the Operations Center (with message code identifiers 0100, 0110, 0200, 0210, 0400, 0410) within two (2) seconds. Time of an authorization message processing by the Operations Center is defined as total time of the authorization message presence at the Operations Center with consideration of milliseconds;
- A parameter (hereinafter referred to as P3) of the Payment Clearing Center's compliance with requirements to the payment clearing services rendering (a parameter of compliance with the rule). This parameter describes the ratio of the number of Transactions for which

payment clearing services were rendered without violations to the total number of Transactions for which the payment clearing services were rendered. P3 threshold value is 99,8%. P3 value shall not be less than the set threshold value. The rule for the procedures performance is sending of Incoming Clearing Files by the Payment Clearing Center to the Participants within six (6) hours starting from 7:30 p.m. Moscow time of the day during which payment clearing procedures were performed, as well as sending of the Net Position Log to the Settlement Center before 3:00 p.m. Moscow time of each business day;

- A parameter (hereinafter referred to as P3) of the Settlement Center's compliance with requirements to the settlement services rendering to the Participant (a parameter of compliance with the rule). This parameter describes the ratio of the number of Transactions for which settlement services were rendered without violations to the total number of Transactions for which the settlement services were rendered. P3 threshold value is 99,0%. P3 value shall not be less than the set threshold value;
- A parameter (hereinafter referred to as P4) of availability of the Operations Center's operational services. This parameter describes the ratio of the total duration of all operational services suspensions to the total duration of the operational services set in accordance with the System working hours. P4 threshold value is 99,95%. P4 value shall not be less than the set threshold value;
- A parameter of the Incident frequency change. This parameter describes the rate of increase of the average daily number of Incidents occurred within the assessed calendar month with respect to the average daily number of Incidents occurred within the last twelve (12) calendar months including the assessed calendar month. The threshold value of this parameters is 10%. This parameter value within the System in general and for each Payment Infrastructure Service Provider in particular shall be less than the set threshold value.

18.2.6. Risk Analysis Methods

The risk analysis and assessment procedure is aimed at the System risks detection and analysis including the detection of Risk Events the occurrence of which may lead to the occurrence of Incidents affecting SBC. Risk evaluation and assessment is performed with consideration of the following criteria: compliance with SBC parameters, compliance with the service requirements, financial obligations fulfillment, System technical services availability.

The risk evaluation and assessment methods comprise:

- analysis and assessment of external and internal factors affecting the System functioning;
- generation and keeping up-to-date of the System business processes list;
- development and keeping up-to-date of the System risk, Risk Events, Risk Event causes classifiers;
- analysis of all System business-processes and generation of a list of potential risk-events for each business process with indication of causes and consequences of such Risk Events;
- identification of the inherent risk level for each detected System risk and setting of the allowable risk level;
- comparison of the identified inherent risk level and the set allowable risk level for each detected System risk to determine the significant System risks;
- application of risk management methods for each significant System risk and further identification of the level of the residual risk for each significant System risk;
- comparison of levels of the residual risk and allowable risk for each significant System risk and making a decision to apply other System risk management methods in addition to the previously applied risk management methods;
- monitoring of System risks including the levels of residual System risks and their compliance with the allowable risk level;
- assessment of measures of response to the detected risks;
- generation and keeping up-to-date profiles of each identified System risk including the profile of SBC violation risk (hereinafter referred to as risk profiles) based on results of the System risk assessment and analysis of effectiveness of the proper payment infrastructure services recovery measures.

The Operator creates risk profiles for all System risk types. Risk profiles contain detailed risk descriptions comprising:

- Risk Event description;
- Risk Event cause description;
- description of System business-processes in which Risk Events may occur;
- Risk Event occurrence probability;
- description and assessment of potential adverse consequences of a Risk Event;
- description of business-processes and a list of System Subjects that may be affected by a Risk Event;
- risk level (inherent, allowable, residual);
- list of System risk management methods reducing inherent and residual risk levels.

The SBC violation risk profile is created with respect to significant System risks.

Methods used within the risk management system are determined following the risk profiles development.

The Operator reviews risk profiles at least once a year. If the Incident (not specified in the risk profiles as a Risk Event) occurs and leads to the payment infrastructure services suspension, the risk profiles shall be reviewed within three months from the date of such Incident.

The Operator stores data contained in risk profiles during two (2) years from the date of risk profiles review (update).

The Operator monitors the System Subjects' compliance with the Regulations with respect to the regular System risk assessment and evaluation based on the requested data on the System Subjects' risk assessment and evaluation results.

In terms of the risk assessment and evaluation, the Payment Infrastructure Service Providers shall:

- regularly arrange monitoring of System risks that may affect SBC, including the risks for which the need for real-time monitoring was identified;
- regularly identify and analyze the risks arising in the normal course of activities, develop and implement measures to eliminate them;
- collect, process and systematize Transaction information;
- immediately inform the Operator of the occurrence of Incidents, disputable, emergency and nonstandard situations, and events that caused operational failures, of their causes and consequences in accordance with the procedure set forth in the Regulations, agreements entered into by and between the Operator and the Payment Infrastructure Service Providers;
- comply with the information protection requirements;
- provide the Operator with the information about risk assessment and evaluation results at the Operator's request.

In terms of the risk assessment and evaluation, the Participants shall:

- take measures to maintain the account balance sufficient for uninterrupted Transaction settlements;
- identify and analyze the risks arising in the normal course of activities, develop and implement measures to eliminate them;

- immediately inform the Operator of the occurrence of disputable, emergency and nonstandard situations and events that caused operational failures, of their causes and consequences in accordance with the procedure set forth in the Regulations;
- provide the Operator with the information about risk assessment and evaluation results at the Operator's request.

System Subjects perform the integrated System risk monitoring comprising the real-time control and the regular assessment. The System risk monitoring is performed based on the following criteria:

- System Subjects' compliance with SBC parameters;
- Payment Infrastructure Service Providers' compliance with the payment infrastructure service levels;
- fulfillment of financial obligations to all System Subjects by the Participants;
- availability of System technical services;
- System Subjects' compliance with IS Risk parameter values.

When performing risk assessment, the Operator uses quantitative, analytical, statistical, and expert evaluation methods.

The Operator determines the risk level following the risk assessment and evaluation results based on the probability of Risk Event occurrence and the Risk Event consequence.

The System risk management stages are as follows:

- Risk detection. Risk detection means identification of a risk, its causes and preconditions;
- Risk assessment. Risk assessment means analysis of data obtained from the risk identification, assessment of the likelihood of adverse effects;
- Risk response. Risk response means development and implementation of measures to limit, mitigate, and prevent risks;
- Risk monitoring. Risk monitoring means analysis of the risk and its evolution dynamic;
- Risk report preparation.

The Operator manages non-financial and financial System risks.

Non-financial risks are identified via self-assessment of the Operator's structural divisions in terms of assessment of risks to business processes run by them, identification of key risk indicators (KRI), preparation of risk profiles, analysis and assessment of Risk Events and Information Security Incidents, continuity of business-processes ensuring System's business continuity, analysis of System Subjects' reports on compliance with requirements to data protection when performing Card Transactions and on System Subjects' IS Risks management. Scales on the basis of which non-financial risks are assessed and decisions on their management are made were developed to manage non-financial risks.

The following assessment scales are used for the non-financial risks assessment:

- Scale of assessment of impact of risks affecting the System's business continuity:

Types of adverse effects Impact level / Risk Event criticality level	Impossibility to process Authorization Requests by the Operations Center within the CPD <i>(CPD is a calendar day from 00.00.00 a.m. to 11.59.59 p.m.)</i>	Impossibility to process Authorization Requests by the Participant (with a breakdown by issuing and (or) acquiring traffic) due to the Participant's fault within the CPD <i>(CPD is a calendar day from 00.00.00 a.m. to 11.59.59 p.m.)</i>	Delay in clearing information provision by the Payment Clearing Center to Participants after the set period	Delay in settlement data provision by the Payment Clearing Center to the Settlement Center or a delay in settlement performance by the Settlement Center
5 - extreme impact / maximum criticality level	Total down-time of Authorization Requests processing for more than 1 hour from the time of the Risk Event occurrence	Total down-time of Authorization Requests processing (issuing and (or) acquiring traffic) for more than 1 hour from the time of the Risk Event occurrence	More than 13 hours after the set period for submission of clearing data on all Participants	More than 13 hours after the set period for settlement data submission to the Settlement Center / after the set period for settlement by the Settlement Center
4 - high impact / high criticality level	Total down-time of Authorization Requests processing from 15 minutes to 1 hour (inclusive) from the time of the Risk Event occurrence	Total down-time of Authorization Requests processing (issuing and (or) acquiring traffic) from 15 minutes to 1 hour (inclusive) from the time of the Risk Event occurrence	From 6 to 13 hours after the set period for submission of clearing data on all Participants	From 6 to 13 hours after the set period for settlement data submission to the Settlement Center / after the set period for settlement by the Settlement Center
3 - medium impact / medium criticality level	Over 10,000 Authorization Requests for one Participant or over 30,000 Authorization Requests for two and more Participants from the moment of the Risk Event occurrence	Over 10,000 Authorization Requests (issuing and (or) acquiring traffic) from the time of the Risk Event occurrence	From 2 to 6 hours after the set period for submission of clearing data on all Participants	From 2 to 6 hours after the set period for settlement data submission to the Settlement Center / after the set period for settlement by the Settlement Center
2 - low impact / low criticality level	From 1,000 to 10,000 Authorization Requests for one Participant or from 3,000 to 30,000 Authorization Requests for two and more Participants from the moment of the Risk Event occurrence	From 1,000 to 10,000 Authorization Requests (issuing and (or) acquiring traffic) from the moment of the Risk Event occurrence	From 30 minutes to 2 hours after the set period for submission of clearing data on all Participants	From 30 minutes to 2 hours after the set period for settlement data submission to the Settlement Center / after the set period for settlement by the Settlement Center
1 - insignificant impact / low criticality level	Less than 1,000 Authorization Requests for one Participant or less than 3,000 Authorization Requests for two and more Participants from the moment of the Risk Event occurrence	Less than 1,000 Authorization Requests (issuing and (or) acquiring traffic) from the time of the Risk Event occurrence	Less than 30 minutes after the set period for submission of clearing data on all Participants	Less than 30 minutes after the set period for settlement data submission to the Settlement Center / after the set period for settlement by the Settlement Center

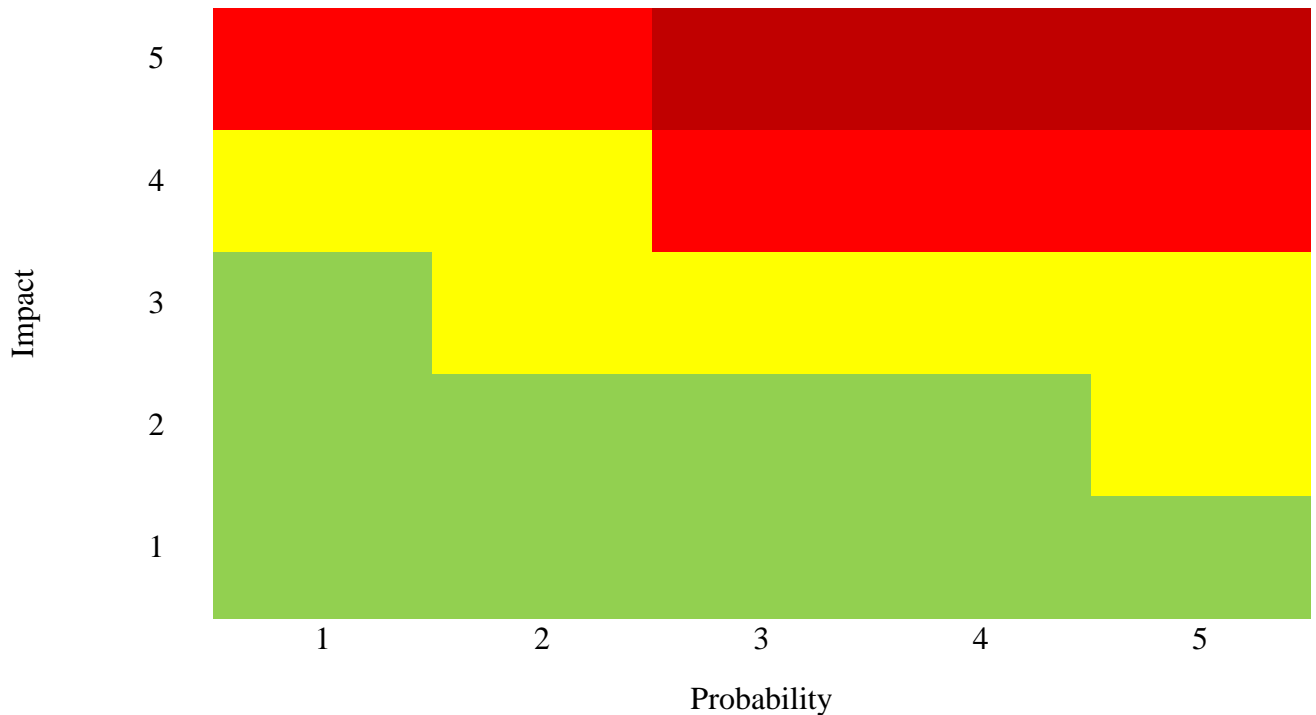
- Scale of assessment of impact of IS Risk in the System:

Types of adverse effects Impact Level / IS Incident criticality level	Any IS Event caused by a violation of security requirements in the Operations Center and (or) the Payment Clearing Center as a result of the actions of third parties, which led to the theft or compromise of any materials or records containing Card data	Unauthorized transfer of funds initiated by the Operational Center and (or) the Payment Clearing Center as a result of violation by third parties of security requirements in the Operational Center and (or) the Payment Clearing Center	Unauthorized access to Card data on the Participant's side	Unauthorized funds transfer on the Participant's side
5 - extreme impact / maximum criticality level	2 IS Incidents that happened within 3 months	From RUB 2,000,000	Data of over 100,000 Cards	Over RUB 30,000,000
4 - high impact / high criticality level	2 IS Incidents that happened within 6 months	From RUB 1,000,000 to RUB 1,999,999	Data from 10,000 to 99,999 Cards	From RUB 10,000,000 to RUB 29,999,999
3 - medium impact / medium criticality level	1 IS Incident during a calendar year	From RUB 0.01 to RUB 999,999	Data from 500 to 9,999 Cards	From RUB 1,000,000 to RUB 9,999,999
2 - low impact / low criticality level	–	–	Data from 10 to 499 Cards	From RUB 500,000 to RUB 999,999
1 - insignificant impact / low criticality level	–	–	Data from less than 10 Cards	Less than RUB 499,999

- Scale of risk probability assessment:

Probability	1 - extremely unlikely	2 - unlikely	3 - possible	4 - very likely	5 - almost surely
Risk occurrence frequency	Less often than once every 5 years	Once every 3-5 years	Once every 1-3 years	Once every 3-11 months	Once every 1-2 months

- Risk assessment heat map



Following the risk assessment, a decision on risk response and management is being taken or data on decisions taken to respond to and manage risks is being requested from System Subjects, if a System Subject is responsible for the risk occurrence.

A system of business continuity was introduced to support the Operator’s business continuity. Within this system, regular trainings including relocation to back-up offices are held.

NSPK JSC Business Continuity Policy was developed. This policy covers the support of the Operator's business continuity, and developed action plans aimed at business continuity maintenance and disaster recovery.

From a technical perspective, actions were taken to protect computer and technical infrastructure from disruption to power supplies (power supply channels were duplicated, backup power sources are introduced), secure information channels were also duplicated, Internet communication channels were also duplicated, devices ensuring continuous operation were also duplicated and warranty contracts were signed with service providers to ensure prompt replacement of failed equipment.

A system of assessment of Participants' financial status was developed within the financial risks management. An internal financial strength rating is assigned to each Participant.

When assessing the financial strength, the following criteria are taken into consideration:

- Financial state;
- Rating (international/Russian);
- Presence of systemically important credit institutions in the list;
- Acquiring network size;
- Card Issuance volume;
- Transaction activity level;
- Business model quality;
- Presence of fraudulent transactions;
- Compliance with the requirements of the laws applicable to the Participant on anti-money laundering and counter-terrorism financing;
- Other criteria.

Based on the Participant's rating, a decision on the Participant's guarantee fee amount payable to the Guarantee fund is made.

The Operator set the following methods of financial risks management:

- Transaction performance within the Participants' Floor Limits with consideration of the risk level;
- creation of the System Guarantee Fund;
- regular monitoring of Participants' compliance with the System Regulations and Standards;
- Operator's blocking of Participants' Card Transactions and Card Transactions in the Participants' Card Acceptance Network;
- System participation suspension or termination.

The Operator prepares the System risk assessment and evaluation report and submits it to the Committee members for review at least once a year.

18.2.7. Operational and Technological Means and Procedures Change Procedure

The Operator may change the operational and technological means and procedures at its own discretion in the following cases:

- a change in the Transaction processing procedure or in the list of System Transactions;

- in cases provided for by the laws of the Russian Federation or at the request of the Bank of Russia;
- changes to the risk management system functioning;
- as a result of a quality assessment of the functioning of the operational and technological means and information systems, conducted by an independent organization in accordance with the Procedure set forth in the Regulations.

If a change in the operational and technological means and procedures made by the Operator requires changes in the Regulations, the Operator shall make the appropriate changes in accordance with the procedure set forth in the Regulations.

If a change in the operational and technological means and procedures, made by the Operator, does not require changes in the Regulations, the Operator shall notify the Participants of the change of the operational and technological means and procedures with a description of such changes not later than thirty (30) calendar days before the effective date of the respective changes.

The Participants are not entitled to change the operational and technological means and procedures related to the interaction with the System without the Operator's approval of the expected changes and their implementation terms.

18.3. System Business Continuity Management

The System Subjects shall organize their SBC maintenance activities within their internal risk management systems.

SBC maintenance activities are performed by System Subjects and controlled by the Operator.

The Operator shall be obliged to:

- coordinate the Payment Infrastructure Service Providers' and Participants' SBC maintenance activities;
- control the Payment Infrastructure Service Providers' compliance with the procedure for the SBC maintenance by way of regular Incidents monitoring and SBC parameter values analysis.
- inform the Bank of Russia and Participants of cases and reasons for the payment infrastructure services suspension.

The Payment Infrastructure Service Providers shall be obliged to:

- manage risks of SBC violation in accordance with their internal documents;

- in the event the Operator reveals facts indicative of the System risk levels increase, provide clarifications and take measures to minimize level(s) of identified risks;
- collect and process data on Incidents, calculate and analyze SBC parameters and provide the obtained results to the Operator;
- independently collect the following data on Incidents and involve Participants, if required:
 - Incident time and date (if it is not possible to identify the Incident occurrence time, the time of its detection shall be specified);
 - brief description of the Incident (description of the occurred Incident and its consequences);
 - names of related consecutive technological procedures performed when rendering payment infrastructure services (hereinafter referred to as business-process) during which the Incident occurred;
 - name of the business-process affected by the Incident;
 - presence (absence) of the fact of payment infrastructure services suspension (termination) resulted from the Incident;
 - Incident's influence on SBC determined with consideration of requirements provided for by Statement No.607-P dd.03.10.2017 of the Bank of Russia *On Requirements to the Procedure for Uninterrupted Functioning of the Payment System, Parameters of Uninterrupted Functioning of the Payment System, and Payment System Risk Analysis Methods Including Risk Profiles*;
 - the degree of Incident's influence on SBC depending on the number of Payment Infrastructure Service Providers, and (or) the number and significance of Participants directly affected by the Incident, and (or) the number and amount of unpaid, and (or) untimely paid, and (or) erroneously paid Participant's payment orders, and other factors;
 - time and date of proper payment infrastructure services recovery in case of their suspension;
 - measures to eliminate the Incident and its adverse consequences with indication of the planned and actual duration of such measures;
 - date of proper payment infrastructure services recovery;
 - adverse consequences of the Incident including:
 - the amount of money paid by the System Operator and (or) collected from the System Operator;

- the amount of money paid by the Payment Infrastructure Service Provider and (or) collected from the Payment Infrastructure Service Provider;
 - the number and the amount of unpaid, and (or) untimely paid, and (or) erroneously paid Participant's payment orders, the payment of which was affected by the Incident;
 - duration of the payment infrastructure services suspension;
- analyze the way each System Incident affects SBC within twenty-four (24) hours from the moment of its occurrence (detection), as well as within twenty-four (24) hours from the moment of its elimination (proper payment infrastructure services recovery) in accordance with the internal documents;
 - determine the Incident's influence on SBC and assess the impact of all System Incidents occurred within a calendar month on SBC in accordance with the internal documents;
 - ensure the Incident data storage during three years from the date of receipt of this data.

The System Subjects shall develop action plans aimed at the SBC maintenance and disaster recovery in case of the operation termination (suspension).

The Payment Infrastructure Service Providers and Participants shall provide the action plans aimed at the SBC maintenance and disaster recovery to the Operator at its request.

The System Subjects shall review the action plans aimed at the SBC maintenance and disaster recovery at least once every two years.

The action plans aimed at the SBC maintenance and disaster recovery, or any other System Subjects' documents including the documents regulating the SBC maintenance process shall contain the analysis of effectiveness of the proper payment infrastructure services recovery measures.

18.4. Organization of Interaction with Payment Infrastructure Service Providers and Participants to Ensure SBC

In order to ensure the System business continuity and risk management, the Operator shall carry out information exchange with the System Subjects.

The Operator shall have the right to request and receive from the Participants and Payment Infrastructure Service Providers the information necessary for the System risk management, as well as to classify, process, collect and store such information. The Operator shall be informed of failure (improper fulfillment) of the Participants' obligations by the Settlement Center, and the exchange of information

between the Operator and the Settlement Center shall be performed, in accordance with the procedure and within the time period specified in the agreement signed between the Operator and the Settlement Center.

The Participants shall provide the requested information to the Operator in accordance with the procedure and within the time period specified in the Operator's request and in the manner set forth by other provisions herein. Should the requested information contain data that constitutes the Participant's commercial or other secret protected by law, the Operator shall ensure the preservation of such information in accordance with the laws of the Russian Federation or the laws applicable to the Participant.

The Participants shall not be entitled to unreasonably deny the Operator the provision of the above information. If provision of certain information to the Operator by the System Subjects is prohibited by the laws of the Russian Federation or by the laws applicable to the Participant, the Participant or the Payment Infrastructure Service Provider shall refuse to provide such information, indicating the reasons for the refusal and giving reference to the provisions of the relevant regulatory acts of the Russian Federation or the laws applicable to the Participant.

The procedure for informing the Operator of the events that caused controversial, non-standard and emergency situations, including cases of system failures, as well as of the results of the investigation of such events and the analysis of their causes and consequences shall be provided in Section 22 hereof.

The System Subjects shall collect, record and process primary information about the System functioning as follows:

The Operations Center shall:

- record the time of failure and restoring of the transactional services provision to the Participants, including those resulting from failures in the communication channels;
- include into the summary reports on risk events the information on the quantity and total duration of failures, including those in the communication channels, indicating the cause and location of a failure: on the Participant's side, on the Operations Center's side.

The Payment Clearing Center shall:

- record the timing of:
 - receipt of the Outgoing Clearing Files;
 - sending of the Reports and Incoming Clearing Files to the Participants;
 - sending of the Net Positions Logs to the Settlement Center;
- include into the summary reports on risk events the information on the quantity and periods of failures in provision of the reports and registers to the Participants and the Settlement Center;

- on a monthly basis, provide information to the Operator pertaining to each Participant, i.e. on the amounts of the net positions;
- the total amount of Transactions for which the Participant was the payer.

The Settlement Center shall:

- record the timing of receipt of the Net Positions Logs from the Payment Clearing Center;
- inform the Operator, in the manner and within the time specified in the agreements signed with the Operator, of the results of the execution of orders issued by the Settlement Center based on the Net Positions Logs;
- in the manner and within the time specified in the agreements signed with the Operator inform the Operator of the Participants, for the fulfillment of whose obligations the funds from the Guarantee Fund were used, as well as of the amount of funds used.

The Operator shall organize collection of primary information about the System functioning, perform systematizing, statistical processing and analysis of the primary information collected for the purpose of managing the risks associated with ensuring the System business continuity, as well as for the System improvement.

The Operator shall ensure the coordination of System Subjects within the System in various forms, including:

- in the form of regular meetings of the Committee, as well as other regular meetings and conferences with the Participants' and the Payment Infrastructure Service Providers' representatives;
- in the form of an ongoing working interaction with the Participants' and the Payment Infrastructure Service Providers' representatives.

The Committee shall hold the meeting at least once a year. Other meetings and conferences shall be held as needed.

Methodological recommendations, amendments to these Regulations and risk management documents, Committees' minutes of meetings shall be posted by the Operator as issued and/or as necessary on the System's Information Resource.

Within the risk management, the Operator shall have the right to develop documents to be used by the Payment Infrastructure Service Providers and Participants to ensure SBC.

18.5. Control over the Payment Infrastructure Service Providers' and Participants' Adherence to the SBC Procedure

The Operator monitors the Payment Infrastructure Service Providers' and Participants' adherence to the SBC procedure as follows:

- collects and stores information about the System failures and malfunctions;
- analyzes and assesses risks based on the information received;
- develops recommendations on the risk level minimization and submits them to the Payment Infrastructure Service Providers and Participants.

To control the adherence to the SBC procedure, the Operator shall have the right to request the Payment Infrastructure Service Providers' and Participants' internal documents related to the Payment Infrastructure Service Providers' and Participants' risks management including risk profiles, reports describing risk management procedures (identification, analysis, monitoring), reports describing incident management procedures (identification, analysis, monitoring), action plans aimed at the SBC maintenance and disaster recovery, results (protocols) of testing action plans aimed at the SBC maintenance and disaster recovery.

The Regulations and agreements signed by the Operator and Payment Infrastructure Service Providers envisage the Payment Infrastructure Service Providers' and Participants' liability for the failure to comply with the SBC procedure.

18.6. Risk Management System Assessment Procedure

Within their System activity, the System Subjects shall independently perform the assessment of the risk management system including the used risk evaluation and assessment methods, and results of risk management methods application at least once every two years in accordance with the current laws of the Russian Federation, regulatory acts of the Bank of Russia and the Regulations.

The Operator's report on the risk management system assessment shall be prepared in writing and reviewed by the Operator's Management Board; it shall comprise the description of used risk assessment and evaluation methods, risk monitoring results, used risk minimization measures, risk management methods application results.

The basic performance criteria of the System risk management system are as follows:

- Operations risk level criterion. Within this criterion, the Operations Center's accessibility at the level of 99.95% and IS Risk parameter values are assessed. The operations risk management

within the System is considered effective, if, as of the report date, the Operations Center's accessibility is 99.95% and IS Risk parameter values do not exceed the set threshold values;

- Legal risk level criterion. The number of lost Operator's lawsuits initiated by the Participants and indicative of conflicts of laws and/or legal uncertainties in certain provisions of the Regulations is assessed within the legal risk level criterion. If this criterion equals to zero (0), risk level management is considered effective;
- Liquidity risk level criterion. Guarantee fund sufficiency is assessed within the liquidity risk level criterion; i.e. the Operator shall ensure that the Guarantee fund level is higher than the overall level of financial obligations of Participants with high risk level as of the report date or is higher than the two-day turnover between the Participant and the largest Card Acceptance Network as of the report date. Liquidity risk management is considered effective, if the Operator complies with the set assessment parameters as of the report date;
- Credit risk level benchmark. System credit risk management is considered effective, if the scope of Participant's financial obligations after the License (Permit) revocation (cancellation) does not exceed 100% of its guarantee fee and/or other collateral.

If the risk management system is determined to be effective, the risk minimization measures are also considered effective.

If during the period under review the risk management system is found ineffective, the Operator shall develop new measures to achieve and maintain the residual risks level not higher than the allowable risk level or new allowable risk levels shall be set.

18.7. Procedure for Assessment of Quality and Reliability of Information Systems and Operational and Technological Means by the Third Party Organization

The assessment of quality and reliability of information systems and operational and technological means shall be performed in accordance with assessment standards and practices with involvement of the third party organization at least once a year.

Assessment results of third party organizations that performed the Operational and Payment Clearing Centers audit may be taken into consideration within the assessment of quality and reliability of information systems and operational and technological means.

Based on the third party organization's report on the assessment performed, the Operator shall make a decision to upgrade or replace the used information systems, operational and technological means in accordance with the recommendations of the independent third party organization.

19. Data Security Requirements

The responsibilities for determining the System data security procedures pertinent to Card Transactions shall be shared by the Operator, the Payment infrastructure service providers and the Participants.

The RF System Subjects undertake to ensure the Transaction data protection in accordance with the System Regulations, Standards, the laws of the Russian Federation and regulatory acts of the Bank of Russia on data protection when transferring funds.

The Non-RF System Subjects undertake to ensure the Transaction data protection in accordance with the System Regulations, Standards, and applicable laws.

These requirements are applied to ensure the protection of data specified in the *Security Program Standard*.

Each System Subject shall independently determine its data protection procedures in accordance with the applicable laws, the System Regulations and Standards within its areas of responsibility stipulated in the Regulations.

When involving organizations, the Participants shall:

- inform the Operator of the involvement of such organizations within the timeframes and in accordance with procedures specified in the *Security Program Standard*;
- ensure compliance of these organizations with the requirements specified in the *Security Program Standard*, as well as control (monitor) implementation of the specified requirements;
- inform the Operator of compliance of the involved organizations with the requirements specified in the *Security Program Standard* within the timeframes and in accordance with procedures specified in this Standard;

In order to manage the information security risk in the System, the System Subjects, within their information security risk management system, are obliged to:

- define IS Risk parameters;
- implement IS Risk detection and identification processes in respect to information infrastructure objects;
- detect and analyze IS Risk;
- control IS Risk level.

The said measures shall be taken by the System Subjects in accordance with requirements of the System Standard *Requirements to IS Risks Management System of Mir Subjects*.

Participants are entitled to limit the performance of Transactions, if it is detected that IS Risk parameter values set by the Participant in accordance with the System Standard *Requirements to IS Risks Management System of Mir Subjects* are exceeded. Participants individually determine conditions for removal of such limitations.

If it is detected that IS Risk parameter values set by the Payment Infrastructure Service Provider are exceeded, the Payment Infrastructure Service Provider is entitled to limit rendering of payment infrastructure services.

Payment Infrastructure Service Providers (excluding the Bank of Russia) shall obtain the Operator's approval of IS Risk parameter values, as well as parameters for limitation of payment infrastructure services rendering and conditions for removal of such limitations.

Within their area of responsibility, the System Subjects ensure detection of IS Incidents, response to the detected IS Incidents, elimination the IS Incident causes, taking of all measures to minimize adverse consequences of IS Incidents and measures to prevent their reappearance in accordance with the applicable laws, the System Regulations and Standards.

The Participants and Settlement Centers (excluding the Bank of Russia) shall inform the Operator of the detected IS Incidents within the timeframes and in accordance with procedures specified in the *Security Program Standard*.

For the purpose of the analysis and control (monitoring) of the Transaction data security within the System, the Participants and Settlement Centers (excluding the Bank of Russia) shall inform the Operator of the Transaction data protection measures within the timeframes and in accordance with procedures specified in the *Security Program Standard*.

20. Electronic Document Management System (SEDO)

To ensure the confidentiality and integrity of information pertinent to their activities in the System, the System Subjects shall use the System's electronic document management system (SEDO) and secure communication channels ensuring transmission of documents during the information exchange between the System Subjects in an encrypted form signed by the digital signature of the party that generated the document. Documents under subclause 12.3 herein shall not be transmitted via SEDO.

The electronic document flow between the Participants, the Operations Center and the Payment Clearing Center shall be performed in accordance with the procedure and under the terms specified in the System Standards.

Electronic information, transmitted by a System Subject via SEDO, signed by the digital signature generated according to the procedure set forth by the System Standards, shall be acknowledged an electronic document equivalent to a paper-based document sign by hand.

The electronic document flow between the System Subjects and the Settlement Center shall be performed in accordance with the procedure and under the terms specified by the Settlement Center.

The Subjects may agree on other forms of information exchange as a backup data exchange channel.

21. Personal Data

For the purpose of compliance with the System Regulations and Standards, the Participants shall transfer to the Operator personal data of Cardholders, their representatives, and third-party representatives, data on which is required to fulfill the System Regulations and Standards requirements (hereinafter referred to as the PD Subjects). In this regard, each Party shall undertake to comply with the requirements of the applicable personal data security and processing laws, as well as laws maintaining personal data confidentiality and protection during their processing, and shall not consider PD Subjects' personal data transfer as a request.

For the purpose of compliance with the System Regulations and Standards, as well as agreements on payment systems interaction signed with PPS operators, the Operator shall transfer personal data of Cardholders data on which is required to Participants, PPS operators, and PPS Participants for compliance with the System Regulations, Standards, and agreements on payment systems interaction signed with PPS operators.

For the purpose of improvement of the quality of services rendered within the System, as well as improvement of the services usability and development of new System products and services, the Operator is entitled to transfer or subcontract Participant representatives' personal data processing to third parties the list of which is posted on the Operator's official website (www.nspk.ru) on the Internet.

The Operator shall process PD Subjects' personal data in accordance with the NSPK JSC Policy of Personal Data Processing and Protection.

The Participants shall be obliged to:

- ensure compliance with the requirements of the applicable personal data security and processing laws;
- at the Operator's request, within fifteen (15) business days provide proofs of legal grounds for the PD Subjects' personal data processing, collection, and transfer to the Operator and third parties (including cross-border transfer) for the purposes of compliance with the System Regulations and Standards.

Participants shall guarantee that they have legal rights to perform PD Subjects' personal data processing, collection, and transfer to the Operator and third parties (including cross-border transfer) for the purposes of compliance with the System Regulations and Standards.

22. Interaction Procedure in Exceptional Situations

In case of an emergency that may affect the Payment Infrastructure Service Providers' capabilities to perform their functions in time, the Payment Infrastructure Service Providers shall notify the Operator and the Participants concerned thereof.

In case of an emergency falling within the responsibility area of the Operator or the Operational Center and the Payment Clearing Center, that may result in the SBC violation including the payment infrastructure services termination (suspension), the Operator shall immediately inform the Settlement Center and the Participants concerned of the occurred incident, its potential cause and the planned time of the payment infrastructure services level recovery. Participants shall be informed via the System's Information Resource.

In case of an emergency falling within the responsibility area of the Settlement Center (other than the Bank of Russia), that may result in the SBC violation including the payment infrastructure services termination (suspension), the Settlement Center shall immediately inform the Operator and the Participants concerned of the occurred incident, its potential cause and the planned time of the payment infrastructure services level recovery.

The procedure for interaction between the Bank of Russia acting as the Settlement Center and the Operator in the event of disputes, exceptions and emergencies, including cases of systemic failures, shall be determined by the procedure for interaction between the Settlement Center and the Operator.

Within the dates specified in the System Standards, the Participants shall inform the Operator and the Payment Infrastructure Service Providers of the events that caused disputes, exceptions and contingencies including cases of systemic and operation failures, and of the results of investigation of such events, and of the analysis of their causes and effects.

The Participants shall inform the Operator via the System's Information Resource. The Subjects' procedure for informing and interacting in the above extraordinary events shall be provided in the System Standards.

Upon the receipt of a notification of the occurrence of extraordinary events and situations, the Operator shall determine, in conjunction with the relevant Participant, an action plan individually for each event in order to remedy the faults, including their effects, and to prevent the occurrence of the new ones.

The Operator shall inform the Participants about events of and reasons for suspension (termination) of payment infrastructure services on the date of such suspension (termination) by posting the relevant information on the System's Information Resource.

23. Warranties and Representations

Each Party (a Party in this section shall be understood as the Operator, the Operations Center, the Payment Clearing Center, and the Participant) represents and warrants to the other Party that:

- it is a duly established and registered legal entity (organization) conducting its business in compliance with the laws of the Russian Federation and/or the law applicable to the Party;
- it has a valid special permission (license) to conduct the corresponding type of activity (operations), if such permission (license) is required in accordance with the laws applicable to the legal entity (organization);
- its actions are not aimed at self-liquidation, it is not in the process of reorganization or liquidation, it has not been declared bankrupt by a court, a bankruptcy petition has not been accepted by court, a bankruptcy procedure has not been initiated, and there is no risk of the Party's bankruptcy at present;
- it is not a participant in (party to) executive, administrative, civil, criminal, tax or other proceedings that could influence the Party's ability to fulfill its obligations set forth by the Regulations;
- its accession to the Regulations (agreement conclusion) and/or the fulfillment by the Party of the conditions set forth by the Regulations does not contradict, directly or indirectly, all and any law, decree, directive, other regulatory acts, acts of state administration or local public authorities, the Party's internal regulatory documents, court's decision applicable to the Party;
- the Party has obtained all permissions, agreements and approvals required for accession to the Regulations (agreement conclusion) and/or execution of the Regulations and System Standards, including those set forth by the applicable laws, regulatory acts, statutory and/or internal Party's documents, including, but not limited to approval of interested party deals and approval of major transactions;
- the person who signs the Application for Accession to the Regulations, as on the day it is signed, has all the required powers and holds the position indicated in the Application for Accession to the Regulations;
- it has all the necessary resources, personnel and experience to conduct activity in the System;
- it has and will have during the term of participation in the System sufficient technical and financial means for timely and full (due) execution of its obligations set forth by the Regulations and the System Standards.

The Participant represents and warrants to the Operator and other Participants that the Participant and third parties involved by such Participant for the performance of activities within the System perform their activities in accordance with the laws applicable to the Participant and (or) third parties involved by it, including if the country of registration of the Participant and/or third parties involved by it differs from the country where such Participant and/or third parties involved by it conduct their business.

The warranties and representations by legal entities (organizations) that accedes to the Regulations are essential to the Operator. The Operator has made a decision on the accedence of such legal entities (organizations) to the Regulations with the account of the above warranties and representations.

24. Anti-Corruption Undertaking

Each Party (a Party in this paragraph shall be understood as the Operator, the Operations Center, the Payment Clearing Center, and the Participant), when fulfilling its obligations under the Regulations, shall not have and shall cause its affiliated persons, employees and/or agents not to have any right, directly or indirectly, to offer and/or pay money and/or other valuables to the employees and representatives of the other Party with the purpose of gaining any advantages related to the activity in the System.

For the purpose of executing the Regulations each Party undertakes not to engage in an action that can be qualified as giving or getting a bribe, commercial bribery, misfeasance in office, as well as in actions violating the law applicable to the Party and the international anti-money laundering acts.

If a Party has a reason to suspect that another Party has violated these requirements, it shall notify such a Party in writing. In its written notice the Party shall refer to the facts or submit materials evidencing, or giving the ground to believe, that a violation of requirements hereunder by the other Party has taken or will take place.

If the risk of a corruption violation under the Regulations has been revealed, the corresponding Party shall, within seven (7) business days from the moment of receipt of the above notification, notify the other Party on the measures taken to exclude such risks, and provide the relevant evidence.

25. Governing Law. Dispute Resolution

The present Regulations are subject to the laws of the Russian Federation.

All disputes, controversies, and claims (hereinafter referred to as Disputes) arising out of or in connection with the present Regulations alongside with their violation, suspension, repudiation, or invalidation shall be settled as per the procedure established by the present section.

When setting Disputes, the Party whose rights were violated may require the Party in breach to remunerate the actual loss in the full scope.

The Disputes between the System Subjects shall be resolved by pre-court settlement:

- Disputes related to the performance (refusal to perform) of the Transaction (hereinafter – the Dispute) including the cases of the unauthorized Card use occurring both between the Participants and the parties participating in the Transaction shall be settled in accordance with the *Dispute Resolution Guide*. In accordance with the *Dispute Resolution Guide* the pre-court dispute settlement procedure shall not be applicable from the day of termination of the system participation of at least one of the Dispute Participants. The terms and conditions for the termination of participation are established in subsection 6.4 of the Regulations;
- Disputes related to the conclusion, interpretation, execution, and termination of the Regulations shall be settled by the Parties through negotiations. In case of failure to reach an agreement during the negotiations mentioned above, the party concerned shall send a written claim signed by the authorized person to the other party. The claim shall be sent via the communication media ensuring the recording of its mailing (by post, by cable, etc.) and receipt, or it shall be handed out to the other party against receipt. The documents justifying the claims submitted by the party concerned, as well as the documents confirming the powers of the person who signed them, shall be attached to the claim. The specified documents shall be submitted in the form of duly notarized copies. The claim sent without documents confirming the powers of the person who signed it shall be considered unsubmitted and shall not be subject to examination. The Party to which the claim is sent shall examine the received claim and notify the party concerned in writing on the results within twenty (20) business days from the date of the claim receipt.

If the dispute is not settled under the pre-court settlement procedure, as well as in case of non-receipt of the response to the claim within the period set above, the dispute shall be submitted to:

State of Registration of the Participant being the disputing party	Place of settlement of a dispute
The Russian Federation, the Republic of Belarus, the Republic of Kazakhstan, the Kyrgyz Republic, the Republic of Tajikistan, the Republic of Uzbekistan, the Azerbaijani Republic, the Republic of Moldova	Moscow City Arbitration Court
Germany, Greece, Georgia, Israel, the Republic of Italy, the Kingdom of Spain, the Kingdom of Morocco, the Republic of Latvia, the Netherlands, the Portuguese Republic, the Republic of Cyprus, the Republic of Bulgaria, the United Kingdom of Great Britain and Northern Ireland, the Republic of Tunisia, the Republic of Turkey, the Czech Republic, Finland, the French Republic, Hong Kong, the People's Republic of China, Vietnam, the Kingdom of Thailand, Malaysia, the United Arab Emirates, the Republic of Korea, the Republic of India, Singapore	<p>Arbitration clause:</p> <p>Any disputes arising out of these Regulations or in connection herewith including in relation to its existence, performance, validity, violation, or termination, shall be tried in the International Commercial Arbitration Court at the Chamber of Commerce and Industry of the Russian Federation under the International Commercial Arbitration Court applicable rules and regulations which are deemed to be incorporated by reference into this section hereof.</p> <p>The Arbitration award is final for the parties.</p> <p>The number of arbitrators shall be three.</p> <p>The seat, or legal place, of arbitration shall be Moscow.</p> <p>The language to be used in the arbitration shall be English.</p> <p>The laws regulating the present Regulations and the arbitration clause are the laws of the Russian Federation.</p> <p>Documents related to arbitration shall be drawn up in paper form and sent by expedited delivery (DHL or other) return receipt requested. Documents shall be sent:</p> <ol style="list-style-type: none"> 1) at the actual address (operational headquarters) of the Participant specified in the Application for accession to the Mir Payment System Regulations; 2) at the Operator's address: 11 Bolshaya Tatarskaya Street, Moscow, Russian Federation, 115184
Other countries	Judicial authority at the defendant's location

The results of legal proceedings on disputes between the Participants and/or the payment infrastructure service providers shall be communicated in writing to the Operator by the party that initiated the legal proceedings within ten (10) business days from the legal decision's date.

The terms of the present section shall not be applicable to the Settlement Centers and the Central Payment Clearing Counterparties.

26. Participants' Reporting Procedure

The Participants shall submit reports to the Operator on their activities within the System in accordance with the procedure and within the terms set forth in the System Standard - *Participants' Reports* - or in accordance with the Operator's individual requests. Direct Participants shall also provide reports on all their Indirect Participants. Indirect Participants shall submit their reports via Direct Participants. Participant Payment Systems shall generate a summary report based on the results of their activities. Participants shall be liable for the timely submission to the Operator and for the completeness and accuracy of data on their activities within the System.

27. Interaction with Partner Payment Systems

NSPK JSC being the System Operator shall have the right to conclude agreements with the Partner Payment System operators on the interaction between payment systems for the purposes of the Cross-system Transactions performance.

Procedure for interaction between the System and PPS.

Payment clearing and settlement between the System and PPS shall be carried out in accordance with the procedure set in the agreement signed by the Operator and the operator of the relevant PPS, and the following provisions:

- NSPK JSC shall carry out the payment clearing and generate settlement data for the System and PPS for all Cross-system Transactions processed within the cross-system interaction;
- The System shall provide payment clearing and settlement services for Participants for Cross-system Transactions in accordance with the Regulations, System Fees and Standards;
- PPS shall provide payment clearing and settlement services for PPS Participants for Cross-system Transactions in accordance with the PPS rules and fees.

Cross-system Transactions Performance Procedure

The servicing of PPS Cards by the Participants within the Participants' Card Acceptance Network and Participants' Cards within the PPS Participants' Card Acceptance Network (Cross-system Transactions) shall be performed in accordance with the procedure established by the System Regulations, Fees and Standards.

28. Procedure of interaction with the payment system of the Bank of Russia for the purposes of funds transfer using the Faster Payment System of the payment system of the Bank of Russia

According to the agreement on payment systems interaction signed by and between the Bank of Russia (the operator of the payment system of the Bank of Russia) and NSPK JSC (the System Operator), the payment system of the Bank of Russia and the System interacts to ensure the use of the Instant Payment Service of the payment system of the Bank of Russia by RF Participants simultaneously being participants of the payment system of the Bank of Russia and System Participants (Direct or Indirect Participants).

Within the specified interaction of the payment system of the Bank of Russia and the System:

- NSPK JSC provides operating and payment clearing services;
- The Bank of Russia provides payment clearing services related to the funds sufficiency check and settlement services.

Procedure for funds transfer using the Instant Payment Service, procedure for operational, payment clearing, and settlement services rendering to Participants, as well as procedure for pre-trial settlement of disputes related to funds transfer using the Instant Payment Service are regulated by:

- Rules of the payment system of the Bank of Russia (regulations of the Bank of Russia the list of which is posted on the official website of the bank of Russia at http://www.cbr.ru/psystem/system_p/rules/);
- Rules of operational and payment clearing services rendering within the Instant Payment Service posted on the System's Information Resource.