Appendix No. 2
to the Mosnarbank
Terms of Bank Cards Issue and Servicing

Procedure for issuing and using the Token

1. Terms and Definitions

Payment System: a combination of institutions interacting according to the payment system rules for the purposes of transfer of funds. All cards related to one Payment System shall have features identifying their relation to such Payment System. For the purposes of these Terms, the Payment System means the MIR payment system, in which the Bank is a participant, and NSPK JSC (OGRN (Primary State Registration Number) 1147746831352) is the operator.

Processing center: AO AB ROSSIYA (OGRN 1027800000084), located at 191124, Russian Federation, St. Petersburg, Rastrelli Sq. 2 lit. A, which collects, processes, and sends information on Card transactions to payment system participants, sends SMS messages to Bank Clients/Bank Card Holders with information on Card transactions, SMS codes, one-time passwords to make secure transactions/payments over the Internet using the 3D Secure Card Technology.

Mobile Payment System (MPS): a service *(Mir Pay Application)* provided by the Payment System operator, which helps Card Holders perform transactions using the Card details, information about which has been stored by the Cardholder in a mobile device (smartphone, tablet, watch, cell phone, etc.) equipped with NFC technology,[1] Android operating system and Internet access.

Token (TAN - Token Account Number): an identifier of the Card, including the Card number, expiration date and Security Code (PPK2), using which the Holder carries out transactions through MPS; the Token is generated by the Payment System operator upon registration of the Card in the MPS by the Holder. Token details can be generated by the Holder in a mobile device with MPS in the form of Consumer-Presented QR code (hereinafter, the QR code). The Token / QR code with token details are stored in encrypted form in the mobile device (smartphone, tablet, watch, cell phone, etc.) with MPS, which the Holder used to register the Card in the MPS. The Token helps uniquely identify the Card used in a transaction.

SMS notifications: a service providing real-time notifications about all bank card_authorizations, as well as receiving SMS codes, one-time passwords for transactions using the 3D Secure Technology.

SMS code: a unique digital code generated by the Payment System operator, which the Holder needs to register the Card and activate the Token in the MPS. SMS code is transmitted to the Holder by the Processing Center in the form of a short text message if technically possible.

The terms specified in this Appendix No. 2 shall apply in accordance with the terms defined in the Mosnarbank Terms of Bank Cards Issue and Servicing and are given above for convenience of work with this Appendix No. 2, which becomes an integral part of the Terms of Bank Cards Issue and Servicing.

[1] Near-field wireless communication technology

2. Procedure for issuing and using the Token

2.1. The Holder has the right to install MPS on the mobile device owned by the Holder, or use the built-in MPS application on the mobile device.
The Holder is notified and agrees that the use of MPS is possible if the Payment System Operator/Processing Center/Bank has technical ability to use MPS and Token by the Holder.

2.2. To carry out transactions via MPS, the Holder must register a valid Card issued in his name, following the instructions of the Payment System operator as specified at the MPS website page.

2.3. Upon successful registration of the Card details, a Token is generated and activated by the Holder by entering the SMS code. The Token is transferred via the Internet to the permanent storage of the mobile device with the Holder's copy of MPS application.

To be able to generate a Token, the Card Holder must have Internet access on his/her mobile device and to activate the SMS notification service using the Card Holder's telephone number, which is specified in the Client's application for SMS notification service and used by the Processing Center to send SMS codes for generating the Token for the Card.

2.4. Multiple Tokens can be generated for a single Card, for each of the Holder's mobile devices. The MPS/Payment System may set limits on the maximum number of Tokens, as well as refuse to generate a Token without explanation.

Token generation is possible for any Card that has not expired or has not been blocked. Termination of the Card disables the transactions using all of the Tokens generated for that Card.

2.5. Documents on transactions involving the Cards, executed with the use of the Tokens, can be signed (certified) by authenticating with the mobile device (biometric confirmation on the mobile device (photo, fingerprints) and/or entering the password of the mobile device in which the Token is saved and/or entering the password of the MPS application). The documents on the Card transactions executed and signed (certified) in this way shall be the proper confirmation of the fact that the order to conduct the Card transactions was drawn up and signed (certified) by the Holder, establishing the rights and obligations of the Holder and the Bank similar to the documents in hard copy, and can serve as evidence in settling disputes between the Holder and the Bank, including in court. Transactions with the use of the Token can be carried out without entering the PIN or the Holder's signature on the receipt.

2.6. The Holder is notified that transactions with the use of the Token can be performed without authentication on the mobile device and/or entering the password of the mobile device, in which the Token is saved and/or entering the MPS password, PIN, PPK2, one-time password, in which case they are also considered to be performed by the Holder.

2.7. The Holder is notified, understands and agrees that not all Trade (Service) Organizations and/or Banking Institutions (acquirers) can accept the Token for transactions, and that the Bank, the Payment System and/or credit organizations (acquirers) can impose restrictions, including on the amounts of transactions.

2.8. When using the Token, the service terms of the Card to which the respective Token is generated (tariff rates, established limits and restrictions, informing on transactions, participation in advertising campaigns and other conditions) shall not change. Transactions performed using the Token shall be equated to those performed using the details of the Card for which such Token has been generated.

2.9. Blocking the Token or removing it from the mobile device memory does not terminate the validity of the Card for which the respective Token was generated, and does not technically limit its use (does not block the Card). If multiple Tokens have been generated for the Card, blocking any one of them does not invalidate any other Tokens.

From the moment a Token is blocked and until it is unblocked, no transactions can be performed by the Holder using the respective Token.

2.10. The Holder shall ensure privacy and safekeeping of the mobile device containing the Token, SMS codes, passwords and other credentials necessary to activate and log into the mobile device and carry out transactions using the Cards via the MPS, in a way that excludes third-party access to them.

If such credentials are disclosed to the third parties, the Holder shall be fully liable for such third parties obtaining access to the Holder's personal information, to the Holder's mobile device and MPS, as well as the possibility to make transactions using the Cards, including via the MPS.

2.11. Before installing MPS, the Holder shall make sure that he/she specified only his/her credentials for access to the mobile device, including the fingerprint and/or photo scanner data built into the mobile device, as the specified data can be used as authorization in the MPS for transactions with the Holder's Card.

In case the credentials for access to the Holder's mobile device, including the fingerprint data and photo scanner built into the mobile device, belong to a third party, transactions performed via SMS with the use of this data are considered to have been performed by the Holder. The Holder will be responsible for all transactions made using their mobile device, regardless of whether the credentials used belonged to them or to another person.

2.12. If the Holder loses the mobile device containing the Token, or if the mobile device is used by third parties, or if the password and other credentials necessary to activate and log into the mobile device with the Token and to the MPS became available to third parties, the Holder must immediately contact the Bank/Processing Center by phone with the password specified by the Client in the relevant application for the Card or Additional Card, to block the Card/cancel the Token, with the subsequent actions as stipulated in Clause 6.3 of the Terms.

When blocking the Card in cases stipulated by the Terms, the Bank blocks and cancels all Tokens for this Card held by the Holder, in order to prevent further transactions in the MPS, and the Token cannot be unblocked.

If the Token is blocked, the Bank blocks and cancels the Token in order to prevent further transactions in the MPS, and the Token cannot be unblocked.

When the Card servicing is suspended in cases stipulated by the Terms, the

Token transactions are also suspended. If the Card is reactivate, the Token transactions will resume as well.

2.13. The Bank may at any time, at its sole discretion, change the type of Cards that can be used in the MPS, and to suspend the ability to use the Card/Token for transactions via MPS.

2.14. The Holder may at any time remove a previously activated Token from the MPS.

The Client has the right to terminate (invalidate) the Token generated by the Additional Card Holder, in the manner stipulated by paragraph 2.12 of this Appendix No. 2.

2.15. By activating the Token in the MPS, the Holder agrees that the Bank may collect, use and transfer information about the Holder, including information relating to his/her Card/Token and the use of MPS, information about transactions made with the use of Cards/Tokens via MPS, and to exchange this information with the subjects of MPS, the Payment system and the Bank of Russia.

2.16. The Bank does not charge a fee for using the Token.

2.17. The Holder cannot use the Token for transactions related to business activities.

2.18. Cash deposits to the Card's banc account via ATMs or other technical devices using the Token are not processed.

2.19. By performing the actions specified in points 2.1 - 2.3 of this Appendix No. 2, the Holder confirms he/she has been introduced to this Appendix No. 2 (its changes) and consents to its terms.

2.20. The Bank may modify this Appendix No. 2 in accordance with the procedure stipulated by Section 11 of the Terms. At the same time the Holder agrees to all changes if he/she continues to use the Card/Tokens in the MPS. If the Holder does not agree to accept the changes of this Appendix No. 2, he/she must remove all Cards/Tokens from the MPS.

3. Liability of the Parties[2]

3.1. The Holder is liable for all transactions with the Card using the Token, performed until the Bank has been notified in accordance with paragraph 2.12 of this Appendix No. 2.

3.2. In case of a Card transaction using the Token without the consent of the Client/Holder, the Client/Holder shall perform the actions stipulated by the Terms for the cases of transactions with the Card (Card details) without the consent of the Client/Holder in accordance with Section 6 of the Terms.

3.3. The Bank does not support the software installed on the mobile device with MPS in which the Token is stored; it is not responsible for supporting the operating system of the mobile device with MPS, for the operation of the mobile device and MPS, for the security of information collected, stored and sent in connection with the use of MPS, for the unavailability of transactions using MPS, as well as for the privacy of information stored on the mobile device with MPS.

[2] This Section 3 shall survive termination of the Terms.

The Bank is not liable for any losses that may be incurred by the Holder as a result of the refusal of the Trade (Services) Organization to carry out transactions with the Card via MPS.

3.4. The Bank does not provide any assistance to the Holder at his/her request (verbal or written) as part of the installation of MPS by the Holder, in particular, for the Holder ascending to the terms of MPS (registration/termination of use of MPS), registration (exclusion) of Cards/Tokens of the Holder in the MPS; the Bank also does not provide advice or notification for the Holder on the terms of MPS and the order of their execution, and the Holder is not entitled to make any claims against the Bank in this connection.

3.5. The Bank is not liable (directly or indirectly) to the Holders for any circumstances in which the MPS operations are interrupted or disrupted, such as unavailability of the MPS or wireless services, communication services, network delays, outages or interruption of the wireless connection. The Bank is not liable for MPS or any wireless services used to access, use or maintain such services.

3.6. The Bank is not responsible for the MPS availability for transactions with the Card/Token, the availability of transactions in a particular Trade (Service) Organization or the continuous or error-free use of MPS.

3.7. Unless otherwise stipulated by law, the Bank shall in no event be liable for any losses incurred in connection with the use or inability to use the MPS, regardless of the causes and grounds of liability.

3.8. The Parties agree that all transactions performed using the Token cannot be claimed by the Client/Holder as having been performed without his/her knowledge and consent and challenged by him/her as unlawful, since the performance of transactions in this manner by the unauthorized Client/Holder is the result of the Client/Holder's violation of this Appendix No. 2 and the Terms.

3.9. Information from hardware and software systems of the Payment System, the Bank, or the manufacturer of the operating system and/or mobile device that provides information and technological assistance in generating, maintaining and using the Token can be used as evidence in disputes, including in court.

3.10. Relationships arising between Clients/Holders and wireless service providers, the manufacturer of the operating system and/or mobile device that provide information and technological assistance in generating, maintaining and using the Token, as well as other persons providing services via MPS, are regulated by separate and independent agreements, for which the Bank shall not be liable.