

Appendix No. 2 to the Public Offer on the Issuance and Servicing of Bank Cards for Individuals

TERMS AND CONDITIONS for the tokenization and use of JSC “Octobank” bank cards in digital wallets and payment services

1. GENERAL PROVISIONS AND DEFINITIONS

- 1.1. These Terms and Conditions form an integral part of the Public Offer on the Issuance and Servicing of Bank Cards for Individuals of JSC “Octobank” (the “Offer”) and govern the addition of the Bank’s Cards to digital wallets and payment services, the Tokenization of Cards, the servicing of Tokens, and transactions carried out using them.
- 1.2. Any matter not regulated by these Terms and Conditions is governed by the Offer, the banking services agreement, the Bank’s Tariffs, the rules of payment systems, the requirements of the relevant Service Provider, and the laws of the Republic of Uzbekistan.
- 1.3. The Service Provider is neither the Bank nor the issuer of the Card and does not service the Card Account unless expressly provided otherwise in a separate agreement. The Bank is not the provider of the digital wallet, the Device, or its operating system.
- 1.4. For the purposes of these Terms and Conditions, the following terms and definitions apply. Terms not expressly defined below have the meanings given to them in the Offer:
 - 1.4.1. **Bank** — Joint Stock Company “Octobank”, the issuer of the Card.
 - 1.4.2. **Client** (Cardholder) — an individual in whose name the Bank has issued a Card.
 - 1.4.3. **Digital Wallet / Payment Service** — a third-party software service that enables the storage of a digital representation of the Card (Token) and its use for payments.
 - 1.4.4. **Service Provider** — a legal entity that develops, owns, and operates the relevant Digital Wallet, and/or such entity’s authorized affiliates.
 - 1.4.5. **Token** — a unique digital identifier generated by the tokenization platform of the relevant payment system, securely linked to a specific Device, and used in place of the Card number when transactions are carried out.
 - 1.4.6. **Device** — the Client’s electronic device (smartphone, smartwatch, tablet, personal computer, or other supported wearable device) certified by the Service Provider for secure Token storage and payments (including via NFC technology).
 - 1.4.7. **Device Access Code** — a personal code for unlocking the Device (password, PIN, or unlock pattern), as well as the Cardholder’s biometric data (Touch ID fingerprint, Face ID facial scan, etc.) registered in the Device settings and used to confirm Transactions in Digital Wallets.
 - 1.4.8. **Provisioning (Adding a Card)** — the process of linking a Card to a Digital Wallet on the Cardholder’s Device and generating a unique Token, carried out through the Bank’s Mobile Application or directly through the Digital Wallet application.

2. ADDING A CARD AND ACCEPTING THE TERMS AND CONDITIONS

- 2.1. The Client independently initiates the addition of a Card through the Bank’s mobile application, the Digital Wallet application, or another channel supported by the Bank.
- 2.2. Before the addition of a Card is completed, the Client reviews these Terms and Conditions. Pressing the “Accept”, “Agree”, “Continue”, or “Add” button on the Device screen or confirming the transaction in the Bank’s mobile application constitutes acceptance by conduct and signifies full and unconditional acceptance of these Terms and Conditions.
- 2.3. To confirm the addition of a Card and activation of a Token, the Bank may use authorization in the mobile application, an OTP/SMS code, push confirmation, the contact center, verification of Client data, or another method.

- 2.4. The Bank may approve or refuse to add a Card, or require additional verification. Only a valid, unblocked Card may be added, subject to compliance with security requirements, the Service Provider's and payment system's requirements, and applicable law.
- 2.5. Separate Tokens may be created for a single Card on multiple Devices. Adding a Card does not constitute the issuance of a new card or the opening of a new account.

3. CARD USE, TARIFFS AND LIMITS

- 3.1. Transactions made through a Digital Wallet or Payment Service are treated as transactions made with the relevant Card and recorded in the Card Account. Successful authentication on the Device (using the Device Access Code or the Cardholder's biometric data) is deemed a valid instruction from the Client.
- 3.2. Once a transaction has been confirmed, the Client may not cancel it unilaterally. Refunds, cancellations, and disputes are handled in accordance with the payment system rules, the Card service terms, the merchant's rules, and applicable law.
- 3.3. The addition of a Card, servicing of a Token, and transactions are subject to the Bank's Tariffs and established limits. Third-party fees are not fees charged by the Bank and are not reimbursed by the Bank.
- 3.4. The Bank does not guarantee uninterrupted operation of a Digital Wallet or Payment Service or their acceptance by all merchants.

4. PERSONAL DATA AND TRANSFER OF INFORMATION

- 4.1. The Client consents to the Bank processing and transferring information about the Client, Card, Card Account, Token, Device, and transactions to the extent necessary for adding the Card, Tokenization, servicing the Token, fraud prevention, support, dispute resolution, and compliance with law.
- 4.2. This information may be transferred to the Digital Wallet or Payment Service provider, payment systems, tokenization service providers, processing centers, providers of fraud prevention and information technology services, and other parties involved in processing, including outside the Republic of Uzbekistan.
- 4.3. The information transferred may include certain Card details and its status, Card and Token identifiers, information about the Device and user account, Device settings, attempts to add the Card, and, if the relevant feature is enabled, approximate location when the Card is added.
- 4.4. Information entered by the Client directly in the Digital Wallet or on the Device may be processed by the Service Provider in accordance with its terms and privacy policy. The Bank neither receives nor stores the biometric templates used for local authentication on the Device.

5. SECURITY, TOKEN BLOCKING AND REMOVAL

- 5.1. The Client must safeguard the Card, Token, Device, user account, and authentication data; must not disclose them to third parties; must not register another person's biometric data on a Device used for payments; and must not use a Device with a hacked or modified operating system.
- 5.2. If the Card, Token, Device, user account, or authentication data is lost, stolen, brought under a third party's control, or compromised, the Client must notify the Bank immediately and use the Service Provider's available measures to remotely block the Device or remove the Card.
- 5.3. The Bank may suspend, block, or remove a Token if the Card is blocked, closed, reissued, or expires; if there are signs of fraud or compromise; if these Terms and Conditions are breached; or if required by the Service Provider, a payment system, a competent authority, or law.

- 5.4. When a Card is reissued, the Token may be updated automatically or the Client may need to add the Card again. When the Card Account is closed and/or the Card is cancelled, the Bank unilaterally initiates the deactivation and removal of all active Tokens issued for that Card.

6. LIABILITY AND DISPUTED TRANSACTIONS

- 6.1. The Client is liable for transactions confirmed on their Device or using their authentication data, including transactions carried out by a person whose biometric data is registered on the Device, unless fault on the part of the Bank is proven.
- 6.2. The Bank is responsible only for actions it performs as the Card issuer: verifying the Card and Client, sending a Tokenization request, processing authorization, servicing the Token, and handling inquiries.
- 6.3. The Bank is not responsible for the operation, availability, or security of the Digital Wallet, Payment Service, Device, operating system, user account, payment system, communications, the Internet, merchants, or other third parties, or for goods and services paid for using the Token.
- 6.4. The Client must review transaction history regularly and notify the Bank of an unauthorized transaction within the period specified in the main Offer. Investigation, refunds, and Chargeback are carried out in accordance with payment system rules and applicable law.

7. AMENDMENTS TO AND AVAILABILITY OF THE TERMS AND CONDITIONS

- 7.1. The current version of these Terms and Conditions is posted on the Bank's official website and may also be available in the Bank's mobile application, the Digital Wallet, or another supported channel. These Terms and Conditions must be available to the Client before the addition of the Card is completed.
- 7.2. The Bank may amend these Terms and Conditions by giving notice in the manner provided for in the Card Offer. Continued use of the Card through a Digital Wallet or Payment Service after the amendments take effect constitutes acceptance of them.