PUBLIC OFFER

On Issuing and Servicing Individual Bank Cards

This Public Offer on issuing and servicing individual bank cards (the **Offer**) defines the terms of the Agreement on Issuing and Servicing Bank Cards (the **Agreement**) concluded between Octobank JSC (the **Bank**) and an individual who complies with the terms of this Offer.
This Offer is an official public offer of the Bank in accordance with Article 369 of the Civil Code of the Republic of Uzbekistan and is addressed to individuals intending to open an account and receive services using bank cards on or without physical media (virtual cards) in national and international payment systems in national and foreign currencies.

Procedure for concluding the Agreement (Acceptance):
Personal bank contact: The Agreement is considered concluded from the moment the Client signs and the Bank accepts a written Application for issuing the card.
Remote bank contact: (via the Bank's mobile application, self-service systems, or other remote banking channels). The Agreement is considered concluded after the Client has successfully completed the identification procedure (including remote identification in accordance with the laws of the Republic of Uzbekistan) after the Client commits the Implicative Actions.
The above actions are recognized as a full-fledged Acceptance of the terms of the Offer, which means the unconditional acceptance by an individual of all the terms of the Agreement without any exceptions or restrictions.
The terms of this Offer apply to all Bank Cards issued before the effective date.
The Bank notifies Clients who have concluded contracts prior to the publication of this Offer about the update of the terms via SMS message, Push notification in the Mobile Application or other channels provided for in the Section of **Error! Reference source not found.**this Offer.
The execution of a transaction by the Client upon a notification or publication of the Offer on the Bank's website is recognized as a full and unconditional Acceptance of this Offer. From the moment of making such a transaction, all previous agreements between the Bank and the Client are considered valid in the wording of this Offer.

1. SUBJECT MATTER OF THE AGREEMENT

1.1. This Offer defines the conditions for opening and maintaining the Client's special card account (Cart Account) in the Bank, determines the procedure for issuing and servicing bank cards (both national and international payment systems), the procedure for their tokenization and use in third-party services and digital wallets, and also regulates the related relations between the Bank and the Client.

2. TERMS AND DEFINITIONS

For the purposes of this Offer, the following basic terms and definitions apply:

2.1. **Authorization** – a procedure for obtaining permission from the Issuer or Processing Center to perform Transactions on the Card, confirming the presence of a sufficient Active Balance and the absence of restrictions.

2.2. **Automatic token renewal** – a payment system technology that allows third–party services (subscriptions) to receive data about a client's new card when the old one is reissued without the client's participation.

2.3. **Active balance** – the amount of funds in the Client's Card Account available for Transactions using the Card or its details at the current time.

2.4. **Client's questionnaire** – a document in the form of the Bank (including KYC questionnaires, compliance questionnaires, applications for tax residence, etc.) containing information about the Client, his activities, financial situation and purposes of transactions, to be completed by the Client at the request of the Bank.

2.5. **Blocking** – a temporary authorization of the transaction amount in the Card Account until the transaction is confirmed by the Processing Center or the transaction is canceled.

2.6. **Currency transactions** – transactions related to the transfer of ownership of currency valuables, their use as a means of payment, as well as cross–border transfers in accordance with the laws of the Republic of Uzbekistan.

2.7. **Refund** – a transaction to refund funds to the Client's Card Account upon refusal of a product or service, approved by the RSO. The refund is made exclusively in non-cash form to the Card Account from which the payment was made.

2.8. **Cardholder** – a Client (individual) or a person authorized thereby, in whose name the Card was issued and who has the right to dispose of funds in the Card Account within the established limits.

2.9. **Additional card** – a Card attached to the Client's Card Account, issued after the Card was issued to the Client, and having the details of the Client or the Cardholder, who is a close relative, in the details.

2.10. **Pre–defined acceptance** – the Client's unconditional consent for the Bank to debit funds from the account in cases stipulated by the Agreement, without receiving a separate order from the Client for each such transaction.

2.11. **Application** – a Client's order submitted to the Bank in writing or via Remote Service Systems for issuing/reissuing a Card, opening an account, or other actions.

2.12. **Bank's instructions** – the internal rules and local documents of Octobank JSC, including AML/CFT/FRM rules, payment system rules, security rules and tariff plans. The Bank's instructions are posted on the website www.octobank.uz The Bank has the right to unilaterally change the Bank's Instructions by notifying the Client via the Bank's website.

2.13. **Card (Bank Card)** – a payment tool that provides its holder with the opportunity to make payments through payment infrastructures or receive cash, or to exchange currency and perform other transactions established by the bank card issuer. The card can be issued both on a physical medium (plastic) and without it (Virtual card).

2.14. **IPS card** – a bank card of international payment systems (VISA, MASTERCARD, etc.) issued by a Bank.

2.15. **Card account** – a special bank account of an individual opened at a Bank and attached to the Card details to account for transactions using the Cards.

2.16. **Client (Cardholder) –** an individual (Resident or Non-Resident) in whose name the Bank has issued the Card.

2.17. **Code word** – a confidential alphanumeric sequence specified by the Client in the Card opening application. It is used to identify the Client during remote service (through the Contact Center and other communication channels) in order to provide information about the Card, Account and Transactions performed.

2.18. **Device access code -** the personal unlock code of the Device (password, PIN code, pattern), as well as the Holder's biometric data (Touch ID fingerprint, Face ID face scan, etc.), registered in the Device settings and used to confirm the completion of Operations in Digital Wallets.

2.19. **Implicative actions** – the actions of the Client performed in the RSS (pressing on-screen buttons, entering OTP (one-time passwords), passing Face-ID, etc.), which unequivocally confirm the Client's will to conclude the Agreement, order a new Card, or perform a Transaction. They have the legal force of a handwritten signature.

2.20. **Bank's mobile application** – a specialized software of Octobank JSC that allows the Client to remotely order a Card issue (including a Virtual One), undergo Remote identification and receive full banking services.

2.21. **International Payment Systems (IPS)** – payment systems (Visa, MasterCard, etc.) that provide technological interaction between IPS participants around the world.

2.22. **National Payment Systems (NPS)** – UZCARD and HUMO payment systems operating in accordance with the laws of the Republic of Uzbekistan.

2.23. **Non–resident** – a person who does not fall under the concept of a Resident in accordance with the laws of the Republic of Uzbekistan.

2.24. **Non–deductible balance** – the amount of funds in the Card Account, which is determined by the Bank's Tariffs, which is not available for use on the Card, that is, it is not included in the amount of the Active Balance. The Non-Deductible Balance is used by the bank to pay off the debt incurred as a result of Card Transactions in excess of the amount of the Active Balance. In the case of using the funds of the Non-Deductible Balance, it is recoevered at the expense of funds deposited to the Client's Card Account at the next replenishment of the Card Account.

2.25. **One–time password (OTP)** – a unique alphanumeric or digital code generated by the Bank and sent to the Client via SMS, Push notification, or other agreed-upon method, intended for confirming a specific Operation, authorization in the SDO, verification during Card tokenization, or document acceptance. OTP is an analogue of the Client's own handwritten signature in the digital environment.

2.26. **Partner** – Agents of the Bank and its Partners who have contractual relations with the Bank to provide banking services to Clients.

2.27. **PIN code** – a personal identification number designed to identify the Holder during Transactions and provide protection against unauthorized access to funds and Card data.

2.28. **AML/CFT/FPWMD** – a number of measures aimed at countering the legalization (laundering) of proceeds from criminal activities, the financing of terrorism and the financing of the proliferation of weapons of mass destruction.

2.29. **Service Provider** – a legal entity that is the developer, owner, and operator of the relevant Digital Wallet.

2.30. **Processing center** – an organization or its division that provides information and technological interaction between settlement participants, including authorization of Transactions, collection, processing and storage of data on them, as well as formation and provision of reports for final settlements on Card Accounts.

2.31. **Resident** – a citizen of the Republic of Uzbekistan, including a foreign citizen who has a residence permit in the Republic of Uzbekistan, a stateless person who has a residence permit in the Republic of Uzbekistan.

2.32. **Card details** – information contained on the card (last name, first name, number, expiration date, CVV2/CVC2 code on the card, etc.) and/or stored in it, allowing to establish the card's affiliation to its holder, issuer and payment system.

2.33. **Self–service system** – an automated software and hardware system (information kiosks, ATMs, card machines, etc.) designed for ordering, issuing Cards and performing Transactions without the participation of Bank staff.

2.34. **Slip** – a document (paper or electronic) confirming the fact of the Transaction and containing its mandatory details.

2.35. **Stop list** – a database of cards for which Transactions have been temporarily suspended (blocked) due to loss or suspicion of fraud.

2.36. **Third–party applications** – mobile applications and other digital platforms of other banks and payment organizations in which the Client has the right to register (add) the Card issued by Octobank JSC for performing Transactions (balance viewing, transfers, payment for services) in accordance with the rules of such systems.

2.37. **RSS (Remote Service System)** – a set of software and hardware tools that ensure remote interaction between the Client and the Bank. It includes both the Bank's own systems (Mobile application, Self-Service Systems, etc.) and systems of Third-Party payment service providers (mobile applications of other banks and payment organizations).

2.38. **Bank's tariffs** – the list and amount of the Bank's fees, which are an integral part of the Agreement.

2.39. **Technical overdraft** – the debt incurred on the Card Account in excess of the Active Balance.

2.40. **Token** – a digital representation of bank card details, which is formed upon the Client's completion of necessary actions through tokenization platforms of payment systems.

The token contains payment information in encrypted form. The card can be digitized/tokenized.

2.41. **Tokenization** – a system for protecting Card details by replacing these details with a Token.

2.42. **Transaction/Operation** – a payment, transfer, withdrawal of funds, or information request initiated by the Client through the Bank's infrastructure, Self–Service Systems, and through Mobile Applications of other banks and payment organizations that support the Issuer's Card services.

2.43. **RSO (retail and service outlet)** – a legal entity, an individual who carries out business activities without forming a legal entity, a self–employed person who sells goods (works, services), as well as recipients of payments to the state budget and state trust funds.

2.44. **Remote identification (Identification)** – a number of measures taken by the Bank to establish, verify and confirm Client data without his physical presence in the Bank using biometric data.

2.45. **Device** – a compatible electronic device (smartphone, smartwatch, tablet, or other wearable gadget) supported by the relevant Service Provider and certified for the secure storage of Tokens and the execution of Operations through Digital Wallets.

2.46. **Digital Wallet (Third-Party Payment Service / Wallet) -** specialized software and/or mobile payment services of third-party providers (including, but not limited to: Apple Pay, Google Pay, etc.), which allows for storing Bank Card Tokens on compatible Devices and using them to make payments.

2.47. **Issuer** – Octobank JSC who issues Cards and owns the right to them and assumes obligations to the Holder and Acquirer for making payments and fulfilling other conditions related to the use of the Cards issued thereby.

2.48. **Acquirer** – an organization (bank, etc.) that provides settlements with RSOs on transactions, as well as the issuance of cash to Cardholders through its structural divisions or RSS.

2.49. **CVV2/ CVC2** – a secret three–digit authentication code used for Online Transactions without physically presenting a Card.

2.50. **KYC (Know Your Client)** – a procedure for identifying and assessing a Client's risks.

2.51. **POS terminal** – a device in the RSO for reading Card data and making payments in real time.

2.52. **Provisioning (Adding a Card)** — the process of linking the Card to the Digital Wallet on the Holder's Device with the formation of a unique Token, carried out through the Bank's Mobile application or directly through the Digital Wallet application.

2.53. **QR code** – a means of accepting and making non-cash payments, which is a static code with permanent RSO/Card details or a dynamic code generated by an RSO/RSS device at the time of the transaction is linked to a specific amount, transaction parameters, and has a set deadline for making the payment.

3. GENERAL

3.1. The Bank, based on the Application to issue the Card and subject to the successful completion of the identification procedure by the Client (including remote identification for remote channels), opens a Card Account within 10 (ten) business days and ensures the issuance of the Card.

3.2. The Card on a physical medium is transferred in the following ways:

a. in person at a Bank branch;

b. by courier delivery to the address specified by the Client in the Application;

c. through the Bank's Self-Service Systems.

3.3. The Virtual Card is issued by the Bank based on an Application submitted through the RSS. The Card is considered transferred to the Client from the moment its full details are displayed in the interface of the Bank's Mobile Application.

3.4. The currency of the Card and the Card Account (sum or foreign currency) is determined by the Client independently at the stage of submitting the Application from the list of currencies available for the corresponding type of card product in accordance with the Tariffs.

3.5. The bank card (including its details) is the property of the Bank and is transferred to the Holder for temporary use for the period of its validity. The Client is solely responsible for the safety of the Card, as well as for ensuring the strict confidentiality of the PIN code, CVV2/CVC2 code and/or one-time confirmation codes (OTP).

3.6. Additional cards:

3.6.1. Based on the Application of the Client who has a Card Account, the Bank has the right to issue Additional Cards (physical or virtual) in the name of the Client or in the name of a third party designated thereby (the Holder of the additional card).

3.6.2. The Holder of the additional card (a third party) is required to complete the identification procedure at the Bank.

3.6.3. The Client bears full material and legal responsibility for all Operations performed using Additional Cards (including their tokenization in Digital Wallets), as well as for familiarizing Additional Cardholders with the terms of this Agreement and the Bank's Instructions.

3.6.4. Remuneration is charged for issuance and maintenance of Additional Cards according to the Bank's Tariffs.

3.7. Blocking and termination:

3.7.1. The Client has the right to terminate the validity of the main or Additional Card at any time based on an Application submitted in writing to the Bank or sent via the Mobile Application.

3.7.2. When submitting an Application through the Mobile Application, the Card is blocked by the Bank immediately and automatically.

3.7.3. Upon termination of the validity of the Card on a physical medium, the Client/ Holder is obliged, at the request of the Bank, to return it to the Bank or destroy it in a way that precludes its further use.

3.8. The Card Account is closed by the Bank at the Request of the Client (provided that there is no debt owed to the Bank) or at the initiative of the Bank in cases stipulated by law and this Agreement.

4. RULES FOR CARD AND CARD ACCOUNT TRANSACTIONS

4.1. The Card and the Card Account are intended exclusively for Transactions that are not related to the Client's business activities. The Client is fully responsible for the legality of Card Account Transactions.

4.2. All Transactions on the main and Additional Cards are recorded, and settlements with the Bank are carried out using the Client's single Card Account.

4.3. All Transactions performed on the Additional Card are considered to have been performed on behalf of the Client. The Client bears full responsibility for the consequences of such Transactions.

4.4. The Card Account is topped up in cash through the Bank's cash departments and/or Self-Service Systems, as well as in a non-cash form.

4.5. The Card can be used to perform the following Transactions:

4.5.1. Conducting cashless settlements for goods and services at trade and service points within the territory of the Republic of Uzbekistan and worldwide (within the framework of Card acceptance infrastructure), including operations using tokenized Cards in Digital Wallets in accordance with Appendix № 2 to this Offer, as well as remote payment on the Internet by entering Card details (number, expiration date, and CVV2/CVC2 code) or by selecting the appropriate Digital Wallet as the payment method.

4.5.2. Registration and use of the Card (both on physical media and in virtual form) in the RSS, as well as its tokenization (linking) in Digital Wallets by any means not prohibited by the legislation of the Republic of Uzbekistan.

4.5.3. Non-cash payments and cash withdrawals, when using virtual cards or tokenized physical cards, these operations are possible exclusively at service points (terminals) and devices (ATMs) with the appropriate technical infrastructure.

4.5.4. Crediting funds to a Card Account through Bank cash departments, Self-Service Systems, or by wire transfer.

4.5.5. Obtaining background information on the Card Account (balance, statement, transaction history) through the RSS.

4.5.6. Receiving cash at the Bank's cash desks, cash departments of other banks (Acquirers) and through Self-Service Systems. At the same time, cash is issued using virtual cards (including cards tokenized in mobile devices) exclusively at service points and devices with the appropriate technical infrastructure.

4.6. QR payments:

4.6.1. Acceptance of the transaction and/or scanning of the QR code through the RSS or the Bank's Mobile Application is considered an appropriate and sufficient order for the Client to debit funds.

4.7. The Client expresses its unconditional consent to transfer to the Card Account any funds received thereby, including social benefits, wages, cross-border transfers, Refunds, Cashback, etc.

4.8. The Bank has the right to suspend the transfer of funds to the Client's Card Account or block the amount received (without the possibility of using it by the Client) in the following cases:

4.8.1. If there is a suspicion that the operation is of a dubious nature or is carried out for the purpose of legalizing (laundering) proceeds from crime.

4.8.2. If the payment details are found to be inconsistent with the Client's data.

4.8.3. Upon receiving a request from the originating bank or payment system about the possible erroneous or fraudulent nature of the transfer.

4.8.4. If it is necessary to comply with international or national sanctions restrictions.

4.8.5. In other cases stipulated by the laws of the Republic of Uzbekistan.

4.9. In case of blocking of an incoming transfer, suspension of an outgoing Transaction, or if there is a need to update data as part of compliance control procedures, the Bank notifies the Client about this through available communication channels. The Client undertakes to provide, within 3 (three) business days after receiving the request (unless another deadline is specified in the request itself):

4.9.1. Documents confirming the origin of the funds.

4.9.2. Documents that are the basis for the Transaction (contracts, invoices, certificates, etc.).

4.9.3. A completed and signed Client Questionnaire in accordance with the Bank's form, as well as explanations about the economic meaning of the Transaction.

4.9.4. Other information required by the Bank to comply with internal rules and legal requirements.

4.10. The Bank undertakes to review the submitted documents within the time period specified in the Bank's Instructions. Based on the results of the review, the Bank makes one of the following decisions:

4.10.1. Unblocking, crediting funds to an account with granting the Client the right to dispose of them.

4.10.2. Refusal to transfer, refund of funds to the sending bank (with possible deduction of the refund fee, if this is provided for by the tariffs).

4.10.3. Further blocking until appropriate orders are received from government regulators or judicial authorities.

4.11. The Bank is not responsible for any losses (including lost profits), fines or penalties incurred by the Client or third parties in connection with the lawful suspension of

operations for verification in accordance with the terms of the Agreement and legal requirements.

4.12. The Client gives the Bank a pre-accepted consent (grants the right) to debit from the account, without additional instruction from the Client, the amounts that were credited by the Bank in error (as a result of a technical malfunction or operator error).

4.13. Entering Card data on a third-party resource (marketplaces, taxis, subscriptions, etc.) is recognized by the Bank as a Client's order to conduct all subsequent operations. At the same time:

4.13.1. The Bank is not responsible for the legality, frequency and amount of debits initiated by such services.

4.13.2. The risk of unauthorized debiting when transferring card data to third parties lies with the Client.

4.13.3. Reissue or blocking of the card does not guarantee the termination of debits if the IPS technology allows updating the card token automatically.

4.13.4. To stop debiting, the Client must independently unlink the card in the interface of a third-party service.

4.14. The Client acknowledges that any actions performed in the Bank's Self-Service Systems (entering a PIN code, using biometric data, scanning a QR code on the device screen) are a complete and sufficient order for operations.

4.15. The Client gives a given acceptance in advance for debiting funds, including the Bank's fees according to the Tariffs, when performing cash withdrawal operations, transferring funds or paying for services through self-service terminals.

4.16. The use of the Card or its details (including tokenized data on smartphones and other supported Devices) abroad is recognized by the Bank as an action performed personally by the Client.

4.17. In order to ensure security, the Bank informs that when sending any notifications, Bank employees never request the provision of full card details (number, expiration date, CVV2/CVC2), as well as RSS passwords or one-time passwords (OTP). The Client shall be vigilant and not transfer the specified data to third parties in order to avoid phishing attacks.

4.18. The risk of unauthorized debiting in the event that the Client transfers card details, access to their account in a third-party service, Apple / Google accounts, and/or the Mobile App is entirely borne by the Client.

4.19. Client's responsibilities for managing third-party subscriptions and linked services:

4.19.1. The Client is fully and solely responsible for managing all active subscriptions and linked third-party services (marketplaces, mobile applications, etc.) of the Card.

4.19.2. In case of termination of use of a third-party service or intention to abandon automatic debits, the Client shall independently perform actions to delete Card data (unlink) in the interface of the corresponding third-party service.

4.20. The reissue of the Card does not guarantee the automatic termination of debits in third-party services that support the technology of Automatic token renewal.

4.21. The Bank does not monitor the Client's activity in third-party services and is not entitled, on its own initiative, to terminate debits initiated by third parties based on an acceptance previously provided by the Client.

4.22. The blocking of the Card or the expiration of its validity period does not guarantee the automatic termination of the Client's obligations to third-party services. If a new card is issued to replace a lost/expired one (reissue), some payment systems may support automatic token renewal, which will lead to continued debits.

4.23. It is not possible to use the Card for Transactions (it is suspended or terminated) in the following cases:

4.23.1. Expiration of the Card.

4.23.2. Card blocking:

a. at the initiative of the Cardholder (in case of loss, theft or suspected compromise of banking details);
b. at the initiative of the Bank in case of breach by the Client of the terms of the Agreement, the Instructions of the Bank or the identification of suspicious transactions under the AML/CFT/FPWMD;
c. at the request of authorized state bodies in accordance with the laws of the Republic of Uzbekistan (including the seizure of the Card Account).

4.23.3. Incorrect PIN code entry three times (for Cards on physical media and during transactions at terminals/ATMs).

4.23.4. Mechanical or other damage to the Card on the physical medium (demagnetization of the chip/tape, plastic breakage), precluding its technical reading by devices.

4.23.5. Lack of technical Authorization capability (failures in communication channels, routine work in the Processing Center or payment system).

4.24. In cases specified in clause 4.23.3 and 4.23.4, the Client has the right to apply to the Bank for reissue of the Card with payment of the commission according to the Tariffs.

4.25. The procedure for issuing, using, suspending, and deleting Tokens in third-party payment services and Digital Wallets, requirements for the security of compatible Devices, as well as the distribution of risks between the Bank and the Client when performing tokenized operations, are regulated by Appendix №2 to this Offer.

4.26. Confirmation of the Operation using the Token via the Device Access Code or biometric data registered on the Device (Face ID, Touch ID, and similar) is recognized by the parties as proper strict authentication of the Holder, has the legal force of entering the Card PIN code / analogue of the Holder's own handwritten signature, and creates unconditional obligations for the Bank to execute the order and debit funds from the Card Account.

5. TARIFFS, FEES, AND SETTLEMENT PROCEDURES

5.1. The Bank charges a fee for issuing and reissuing the Card, as well as for opening a Card Account in accordance with the Tariffs in force on the date of submitting the relevant Application or making a banking transaction.

5.2. The Bank does not charge or pay interest on the remaining funds in the Client's Card Account, unless otherwise stipulated by the terms of a specific Tariff Plan.

5.3. Commission fee:

5.3.1. For conducting Operations (transactions) and providing additional services via the Card, the Bank shall charge the Client a commission fee in accordance with the Bank's Tariffs. For the issuance of Tokens and their use in Digital Wallets, no additional commission is charged by the Bank, unless otherwise expressly established by the Bank's Tariffs; operations using Tokens are charged in accordance with the Tariffs for the corresponding Card.

5.3.2. The Client grants the Bank the right to debit fees without acceptance (automatically) at the time of the Transaction or within other time limits determined by the Bank.

5.4. All settlements under the Agreement, including the withdrawal of commissions and fees, with the exception of cross-border transactions, are made in the currency of the Card Account.

5.5. Rules for conversion and cross-border payments:

5.5.1. When making Transactions in a currency other than the currency of the Card Account, the amounts are automatically converted at the exchange rate of the IPS/NPS or the Bank.

5.5.2. When exchanging foreign currency for Uzbek soums through the RSS, the exchange rate set by the Bank or the rate of the relevant credit institution in effect at the time of confirmation of the Transaction is applied.

5.5.3. The Client confirms its agreement with the applicable exchange rate and the rules for the conversion of IPS/NPS at the time of the Transaction/its confirmation.

5.5.4. The Client agrees to debit the fees of third-party acquiring banks incurred during Transactions abroad or on the devices of other credit institutions.

5.6. In case of early termination of the Card at the initiative of the Client or on the grounds stipulated by the Agreement, the fees previously paid by the Client for issuing, servicing the Card and for Transactions already performed will not be refunded.

5.7. The Bank has the right to make changes and additions to the Tariffs unilaterally. The Client is notified of the changes at least 10 (ten) calendar days before the effective date in the following ways:

5.7.1. By posting an updated version of the Tariffs on the Bank's official website www.octobank.uz;

5.7.2. By placing information on stands in the Bank's operating areas.

5.8. If, prior to the effective date of the changes, the Client has not submitted a written notice of termination to the Bank and continues to use the Card, such changes are considered fully accepted by the Client.

6. INFORMATION INTERACTION AND NOTIFICATION

6.1. The Bank has the right to send notifications, notices, as well as information about changes in Tariffs or terms of the Offer to the Client in the following ways (at the Bank's choice):

6.1.1. Personally on paper.

6.1.2. In writing by means of postal communication or e-mail specified in the Application.

6.1.3. By sending Push notifications through the Bank's Mobile App.

6.1.4. By sending SMS messages to the Client's mobile phone number.

6.1.5. Through the Bank's official accounts in verified messengers.

6.1.6. By publishing information on the Bank's official website www.octobank.uz

6.2. The Parties agree that the Client is considered to have been duly notified:

6.2.1. When sending a Push notification or SMS — at the moment when the sending is recorded by the Bank's software and hardware system (regardless of the moment when the Client actually reads it).

6.2.2. When sending by E-mail — after 24 hours from the date of sending the letter by the Bank.

6.2.3. When published on the website — from the effective date of the changes specified in the publication.

6.3. Disabling the function of receiving SMS messages or Push notifications by the Client in the settings of the mobile device, as well as no access to the Internet or cellular communications, does not constitute grounds for recognizing the notification as undelivered.

6.4. Any notification sent using the contact information provided by the Client is considered a legally significant message. The risk of consequences of not receiving or not knowing the information in full is borne by the Client.

6.5. The Client shall ensure the operability of their devices and access to the Internet in order to receive timely notifications. The Bank is not responsible for delays or non-delivery of notifications caused by:

6.5.1. the Client's lack of an Internet connection or mobile connection;

6.5.2. malfunction of the Client's device;

6.5.3. the Client's software settings that restrict reception of notifications.

6.6. The Client undertakes to independently check for updates of the Offer and Tariffs on the Bank's official website at least once a week.

6.7. The Client shall notify the Bank within 3 (three) business days of a change in the phone number, e-mail address, place of residence or other personal data.

6.8. In case of non-fulfillment of the obligation to update the data, the notification sent using the old details is considered delivered and entails appropriate legal consequences.

6.9. The Parties acknowledge that electronic documents and notifications sent through remote channels (Mobile application, SMS, e-mail) are equivalent to paper documents signed by hand and can be used as evidence in court.

7. RIGHTS AND OBLIGATIONS OF THE PARTIES

7.1. The Bank may:

7.1.1. Unilaterally change the terms of this Offer, Tariffs and Instructions of the Bank.

7.1.2. If necessary, require the physical carrier of the Card to be presented, as well as to withdraw it from the Cardholder, having previously notified the Client at least 3 (three) calendar days before the expected withdrawal date.

7.1.3. Temporarily block the Card and/or suspend Card Account Transactions in the following cases:

a) upon receiving the relevant order (Application) from the Client in the form prescribed by the Bank;

b) if a breach by the Client or the Cardholder of the terms of this Offer, the Agreement or the Instructions of the Bank are discovered;

c) when the Client knowingly provides false information/documents, or fails to provide documents requested by the Bank for the purpose of due diligence (KYC) or when the Client performs questionable and suspicious transactions as part of AML/CFT/FML legislation;

d) if the Client fails to provide documents confirming the source of the funds or the economic meaning of the Transaction;

e) during the third attempt to enter an incorrect PIN code. In this case, the Bank blocks the Card and notifies the acquiring bank (a member of the IPS/NPS), in whose device the Transaction is performed, about the need to withdraw or detain the Card;

f) if the Bank receives mandatory requirements (orders) of state bodies in accordance with the applicable laws of the Republic of Uzbekistan;

g) upon termination of the relationship with a Partner, if this makes it impossible to continue servicing the Card;

h) when identifying the risks of breaching international or national sanctions regimes;

i) upon receiving information about possible unauthorized use of the Card (compromise of banking details), as well as if there are other grounds that may cause material damage to the Bank and/or the Client.

j) in respect of individual Card Tokens (without blocking the physical bearer of the Card or Card Account) - in case of suspicion of compromising the Device or the Service Provider's account (Apple Account, Google Account, etc.), detection of signs of registration of third-party biometric data on the Device, or at the request of the Service Provider or payment system in accordance with Appendix № 2 to this Offer.

7.1.4. Demand from the Client immediate payment of Card Account arrears (including unauthorized overdraft), as well as reimbursement of expenses and losses incurred by the Bank in connection with the Client's breach of the terms of the Offer or the Bank's Instructions.

7.1.5. Verify the accuracy and completeness of the information provided by the Client in the documents upon receiving the Card and during the fulfillment of the Agreement. If discrepancies are found, the Bank has the right to refuse to issue/reissue the Card or to satisfy other Client requirements.

7.1.6. Without acceptance (without obtaining additional consent) to debit funds from the Client's Bank Account in cases stipulated by this Offer and the laws of the Republic of Uzbekistan.

7.1.7. If erroneous records are found for crediting to the Card Account or debiting funds, make corrections by making reverse transactions (crediting / debiting) in due manner without the Client's prior consent.

7.1.8. In case of disputed Transactions/Operations performed with IPS Cards, require the Client to provide the documents necessary for reviewing applications for these

operations and make copies of them. In order to obtain objective data, contact the IPS with a request for supporting documents from the acquiring bank. If the acquiring bank documents the validity of the disputed Transaction, the costs of obtaining supporting documents will be charged to the Client's account.

7.1.9. Destroy the Card on a physical medium that is not in demand by the Client within 3 (three) months from the date of its release.

7.1.10. Request additional information, set individual Transaction limits, refuse to conduct Transactions, or terminate the Agreement unilaterally if the Client refuses to provide documents or fill out Client Questionnaires provided for in the Bank's Instructions.

7.1.11. In accordance with the Bank's Instructions, periodically update Client data, requiring re-identification or the provision of supporting documents for previously completed transactions.

7.1.12. Terminate this Agreement unilaterally in the cases established by this Agreement.

7.2. The Client may:

7.2.1. Dispose of funds on the Card Account within the limits of the Active Balance by performing Transactions provided for in the Section 4 of the Offer, subject to compliance with the laws of the Republic of Uzbekistan and the terms of the Agreement.

7.2.2. Top up the Card Account in cash and non-cash form using available methods.

7.2.3. When receiving a Card or in the process of using it, you can independently change the PIN code through the available RSS.

7.2.4. Receive statements about completed Transactions and the status of the Card Account. When contacting the Bank in person, the Client must present an identity document. The holder of an Additional Card may not request information about the Client's Card Account from the Bank.

7.2.5. Apply to the Bank for an investigation of the Transaction with which it does not agree. The Client undertakes to reimburse the Bank for all actual expenses incurred in connection with such an investigation and the refund procedure.

7.2.6. Upon expiration, in case of loss, theft, mechanical damage to the Card or change of personal data (full name), contact the Bank to reissue the Card. The old Card (if it is not lost) must be returned to the Bank for blocking and destruction.

7.2.7. Unilaterally cancel the Agreement by submitting an Application no later than 30 calendar days before the termination date, subject to the return of all Cards to the Bank and the full completion of mutual settlements.

7.2.8. Know about the availability of the personal data by the Bank and receive information about their processing.

7.2.9. Request temporary suspension of processing or destruction of data if it is incomplete, outdated, inaccurate or illegally obtained;

7.2.10. The Cardholder does not have the right to demand a refund from the Bank until it receives information from the RSO about the transactions made.

7.2.11. Receive cash and top up the Card Account through cash departments and Self-Service Systems in accordance with their technical capabilities.

7.2.12. Add the Card to the Digital Wallet on supported Devices and remove the Tokens in the manner prescribed by Appendix № 2 to this Offer.

7.3. Under this Agreement, the Holder of the Additional Card may:

7.3.1. Use the Card to perform the transactions specified in this Agreement.

7.3.2. Receive cash through RSS or bank cash departments.

7.3.3. Top up the Card Account with cash through the RSS or the Bank's cash department.

7.3.4. Receive background information about the Active Balance, as well as brief information about the Transactions carried out in the RSS.

7.4. The Bank shall:

7.4.1. Make the Client familiar with the Bank's Tariffs and Offer, including by publishing them on the Bank's website (including using Digital Wallets).

7.4.2. Issue the Card and ensure its transfer to the Client (or display the details for Virtual Cards) in accordance with the rules of the Offer.

7.4.3. Promptly debit the Card Account for the amounts of Transactions and commissions, as well as credit incoming funds and refunds to the account.
7.4.4. Provide the Client with Card Account statements in accordance with the Bank's Tariffs.
7.4.5. Upon receiving a message about the loss of the Card, immediately (within 24 hours in case of technical obstacles) stop servicing the Card and add it to the Stop List.
7.4.6. Provide consulting support to the Client regarding the use of Cards and payment technologies.
7.4.7. Upon termination of the Agreement, return the remaining funds in the Card Account to the Client in a legal manner after completing all mutual settlements for previously completed Transactions.
7.4.8. Reissue the Card within 10 (ten) banking days from the date the Client submits to the Bank a written application for reissue of the Card.
7.4.9. Based on the Client's Application on the IPS Cards and in accordance with the IPS rules, conduct an investigation (in particular, obtain copies of receipts and, if possible, details of the Transaction from the acquiring bank) on disputed Transactions. Take all reasonable and affordable measures for refund.
7.4.10. Inform the Client about detected signs of fraud, information security, cybersecurity, and fraud incidents through available communication channels.

7.5. The Client shall:

7.5.1. Bring the terms of the Agreement and the Bank's Instructions to the attention of the Holders of additional Cards and require them to strictly comply with them.
7.5.2. Comply with the terms of the Offer and the Instructions of the Bank, and when making Currency Transactions, comply with the requirements of the applicable laws of the Republic of Uzbekistan.
7.5.3. Pay fees according to the Tariffs, reimburse the amounts of funds credited in error, as well as cover the Bank's losses incurred due to the Client's breach of the terms of the Agreement.
7.5.4. Ensure the safety of the Card, not to transfer the Card and its details to any third parties. Keep PIN code, OTP (one-time passwords), CVV2/CVC2 codes and Code Word strictly secret.
7.5.5. Bear full responsibility for all Card Transactions, including those performed by third parties (with or without the Client's knowledge), as well as for Transactions conducted without Authorization in accordance with the rules of the IPS.
7.5.6. Perform Transactions within the Active Balance. Monitor the absence of over-the-limit debt (technical overdraft) on IPS Cards. If it occurs, pay off the overdraft amount within 30 calendar days.
7.5.7. Notify the Bank about changes in the data in the identity documents, address or phone number within 5 (five) banking days and provide supporting documents.
7.5.8. Perform no Transactions using the Card's details after depositing it to the Bank or after its expiration date, as well as using a Card declared lost.
7.5.9. In cases of loss, theft and/or illegal use of the Card/Card details to suspend Card Transactions, the Client/Cardholder should immediately inform the Bank thereof.
7.5.10. If a previously declared lost Card is found, the Client/Cardholder shall immediately notify the Bank and return the Card to the Bank for subsequent unblocking or destruction.
7.5.11. If this Agreement is terminated, the Card expires, or a written request from the Bank is received, the Client shall return the Card to the Bank within 5 business days for its subsequent cancellation and destruction. If it is impossible to return (loss/theft), submit an appropriate application.
7.5.12. If the RSO (outlet) returns the purchase amount paid by the Card to the Client, require no refund of it again in cash from the outlet. The specified refund can only be made to the Card Account in a non-cash manner.
7.5.13. At the request of the Bank, provide any additional information and documents (including filling out specialized Client Questionnaires) required by the Bank to comply

with legal requirements (including AML/CFT/FPWMD), the Bank's internal rules and Instructions. The Client recognizes the Bank's right to request information not only at the time of account opening, but also during the entire term of the Agreement.

7.5.14. Terminate the Transactions specified in the Bank's notification in cases of termination of the Bank's relationship with the Partner.

7.5.15. Take necessary legal, organizational and technical measures to protect the Client's personal data from illegal processing, disclosure, accidental loss or destruction, ensuring their confidentiality and security.

7.5.16. Carefully read the notifications sent by the Bank, including PUSH notifications in the mobile application, SMS notifications regarding detected signs of fraud, information security, cybersecurity, and fraud incidents,

- Take into account the information provided by the Bank about detected signs of fraud and exercise increased caution when confirming any payment transactions after receiving these notifications;
- immediately, but no later than 1 (one) day from the moment the fact is identified, to notify the Bank of the loss (theft) of the device through which access to banking services is carried out or on which Card Tokens in Digital Wallets are activated, or of the establishment of control over such a device by third parties;
- notify the Bank of the transaction without its consent within 1 (one) day from the moment of detection of such fact;
- provide the Bank with the contact information necessary for communication, in case of their change, within 3 (three) days from the date of such changes;
- at the request of the Bank, the Client undertakes to provide information that the transaction was carried out thereby independently or performed by a third party on its behalf or with its voluntary consent;
- provide the Bank with information about fraud cases.

8. CONFIDENTIALITY AND PROTECTION OF PERSONAL DATA

8.1. By accepting this Offer, the Client gives the Bank its free, informed and unconditional consent to the processing of its personal data (recorded on electronic, paper and (or) other tangible media of information related to the Client or enabling its identification).

8.2. The personal data is processed by the Bank solely for the following purposes:

8.2.1. Conclusion and execution of this Agreement, issue and servicing of Cards;

8.2.2. Identification of the Client (including Remote identification) and compliance with AML/CFT/FPWMD legislation requirements;

8.2.3. Informing the Client about the Bank's services, conducting marketing research and loyalty programs;

8.2.4. Ensuring the security of individuals, society and the state in accordance with the principles of the laws of the Republic of Uzbekistan.

8.3. The composition of the processed data includes: Full Name, passport data (PINFL), address, phone number, email address, biometric data (facial photograph for identification), information on financial transactions, technical parameters of Devices, and service provider account data (Apple Account, Google Account, etc.) transmitted during tokenization, as well as other data provided by the Client.

8.4. Processing includes: collection, systematization, storage, modification, addition, use, provision, depersonalization and destruction of personal data.

8.5. The Bank collects, systematizes and stores personal data of Clients (including biometric data) in personal data databases located on the premises in the territory of the Republic of Uzbekistan.

8.6. The Client consents to the cross-border transfer of their data (disclosure to specific persons outside the Republic of Uzbekistan) to ensure the conduct of Operations, as well as for the purposes of issuing and servicing Tokens, their authentication, and countering fraud by transmitting data to foreign Service Providers (including Apple Inc., Google

LLC, Samsung Electronics Co., Ltd. and their affiliates) and international payment system operators (Visa, Mastercard, etc.) within the procedures provided for in Appendix №2 to this Offer.

8.7. The data is subject to destruction upon the purposes of processing are achieved or the storage period expires, unless otherwise provided by the laws of the Republic of Uzbekistan.

8.8. The Client agrees that the Bank has the right to entrust data processing to a third party (Partners, Processing Centers), provided that they comply with confidentiality and security requirements provided for by the laws of the Republic of Uzbekistan.

8.9. The Client has the right to withdraw consent to data processing by submitting a written application 30 days in advance. This entails termination of the Agreement if the data is necessary for its execution.

9. FORCE MAJEURE CIRCUMSTANCES

9.1. The Parties are released from liability for partial or complete non-fulfillment of their obligations under this Offer if it was the result of force majeure circumstances that arose after the conclusion of the Agreement as a result of extraordinary events that the Parties could not have foreseen or prevented by reasonable measures.

9.2. Force majeure circumstances include:

9.2.1. Natural disasters (earthquakes, floods, fires, epidemics/pandemics);

9.2.2. Socio-political events (military actions, terrorist acts, strikes, civil unrest);

9.2.3. State legal acts (adoption by state authorities, management bodies or the Central Bank of the Republic of Uzbekistan of acts or measures of a restrictive and prohibitive nature, including sanction restrictions);

9.3. Technological factors arising not through the Bank's fault but affecting the fulfillment of obligations: systemic failures in the software of MPS/NPS Processing Centers, failures on servers and tokenization platforms of Service Providers, global failures in the operation of the Internet network, power supply, or main data transmission systems.

9.4. The Party for which it is impossible to fulfill its obligations shall immediately (but no later than 3 business days) notify the other Party of the beginning and termination of the specified circumstances.

9.4.1. The Bank notifies the Client in one of the ways provided for in the Section of 6this Offer.

9.4.2. The Client notifies the Bank by submitting a written application.

9.5. The fact of force majeure circumstances shall be documented by the relevant authorized state bodies or organizations of the Republic of Uzbekistan.

9.6. Late notification of force majeure deprives the Party of the right to refer to them as a basis for exemption from liability, except in cases where the circumstance itself prevented such notification.

9.7. The period for fulfilling obligations under the Agreement is postponed in proportion to the time during which the force majeure circumstances and their consequences were in effect. If the specified circumstances last more than 30 (thirty) calendar days, the Parties have the right to terminate the Agreement by making full settlements on the date of termination.

10. ANTI-CORRUPTION CLAUSE

10.1. The Parties recognize and confirm that they pursue a zero tolerance policy towards corruption and other manifestations of corruption. The Parties undertake to comply with the requirements of the laws of the Republic of Uzbekistan on combating corruption, as well as the applicable norms of international law.

10.2. In fulfilling their obligations under this Agreement, the Parties, their affiliates, employees, or intermediaries undertake not to commit (offer, promise, or authorize) actions that qualify as:

10.2.1. Giving or receiving a bribe;

10.2.2. Mediation in bribery;
10.2.3. Commercial bribery;
10.2.4. Abuse of official position or other actions that breach the requirements of anti-corruption laws in order to obtain undue advantages.

10.3. If one of the Parties suspects that any anti-corruption provisions have been breached or may be breached, the relevant Party undertakes to notify the other Party in writing or through the communication channels specified in the Section 6within 3 (three) business days.

10.4. The Bank has the right to request additional documents and explanations on Transactions from the Client if the nature of such Transactions gives reason to believe that there is a corruption component or other illegal purposes.

10.5. Consequences of the breach:

10.5.1. A breach of the Client's anti-corruption obligations, documented or identified during an internal audit of the Bank (compliance control), is a significant breach of the terms of the Agreement.

10.5.2. In case of breaches, the Bank has the right to unilaterally suspend the Card service, block access to the RSS, or terminate the Agreement completely.

10.5.3. The Party guilty of breaching the anti-corruption conditions shall compensate the other Party for the losses incurred as a result of such breach.

10.6. The Bank is not responsible for any negative consequences (losses, fines) incurred by the Client in connection with the lawful application by the Bank of the measures provided for in this section.

11. RESPONSIBILITY OF THE PARTIES

11.1. The liability of the Parties in cases not provided for by this Agreement is regulated by the applicable laws of the Republic of Uzbekistan.

11.2. The Client is fully responsible for the accuracy of all information provided to the Bank and for the proper performance of its duties stipulated in the Agreement.

11.3. The Client is responsible for all Operations performed using the Card or its details, including Operations performed using Tokens in Digital Wallets, until the moment they actually apply to the Bank with a request for blocking. Losses caused to the Bank as a result of the Client's (the Holder's) failure to fulfill or improper fulfillment of the terms of the Agreement shall be subject to unconditional compensation by the Client. The fact of registering biometric data (fingerprints, facial scans) of third parties in the settings of the Client's Device is recognized by the Parties as a voluntary transfer of access to the Card to third parties and entails the imposition of all financial responsibility for the performed operations exclusively on the Client.

11.4. The Client guarantees that it is familiar with the currency legislation of the Republic of Uzbekistan, and is responsible for its observance when making Currency transactions.

11.5. The Client is fully responsible for the safety of the Card and its data while located outside the Republic of Uzbekistan, as well as for timely notifying the Bank of the need to block the Card or its associated Tokens in the event of its loss abroad.

11.6. In case of technical failures on the part of mobile operators or Internet service providers, the Client shall exercise due diligence independently and check for notifications and changes in Tariffs by contacting the Bank.

11.7. The Bank is responsible for late blocking of the Card or Token after receiving a proper notification from the Client in due manner.

11.8. The Bank is responsible for maintaining banking secrecy. Information about the Card Account and Transactions may be disclosed to third parties only in cases stipulated by the laws of the Republic of Uzbekistan, or with the consent of the Client.

11.9. The Bank is not responsible for delays in issuing/reissuing the Card or crediting funds if this is caused by the provision of inaccurate data or incomplete documents by the Client.

11.10. The Bank is not responsible for the Client's losses incurred as a result of technical failures on the part of the IPS/NPS, other participating banks, or failures in the operation of communication networks, power supply and equipment serviced by third parties.

11.11. The Bank shall not be liable for the Client's losses resulting from technical failures on the part of the IPS/NPS, other participating banks, failures in software and servers of Service Providers, operating systems, and hardware of mobile devices, or failures in the operation of communication networks, power supply, and equipment serviced by third parties.

11.12. The Bank is not responsible for any financial losses in the event that the Card or Tokenis used by a third party within 24 (twenty-four) hours from the moment the Client submits an application for the loss of the Card or Device.

11.13. The Bank is not responsible for the Client's losses incurred as a result of misleading the Client by third parties (social engineering, fishing), including the Client's voluntary transfer of OTP to third parties, or in connection with non-fulfillment of obligations by the recipients of funds.

11.14. The Bank is not responsible for situations beyond its control, as well as in case of non-fulfillment by the Client of the terms of this Agreement and its Appendix.

11.15. If one of the Parties breaches the laws of the Republic of Uzbekistan during the execution of the Agreement, the other Party is not responsible for this.

11.16. Failure by a Party to fulfill the obligations stipulated in this Agreement gives the other Party grounds for its unilateral termination.

12. CONCLUSION, AMENDMENT, AND TERMINATION OF THE AGREEMENT

12.1. This Agreement is considered concluded from the moment the Client accepts the terms of the Offer (by submitting a signed Application to the Bank or performing Implicative Actions in the RSS) and is valid for an indefinite period until its termination by one of the Parties.

12.2. This Agreement, the Tariffs and the Bank's Instructions may be amended and supplemented by the Bank at its sole discretion. The changes will take effect on the date specified in the notification and after their publication on the Bank's official website.

12.3. The Client has the right to terminate the Agreement at any time by submitting a written application to the Bank. Termination is possible if the following conditions are met:

12.3.1. Return to the Bank of all physical Cards issued under the Agreement (with the exception of Virtual Cards);

12.3.2. Complete fulfillment by the Client and the Holders of all obligations and no debt owed to the Bank.

12.4. Refunding upon termination of the Agreement:

12.4.1. The amount of funds exceeding the Non-Deductible Balance is returned to the Client on the day of submitting the application for closing the Card Account (subject to the return of the physical Card);

12.4.2. The amount of the Non-Deductible Balance is refunded to the Client within 30 (thirty) calendar days after the Card is returned to the Bank and the application for termination of the Agreement is submitted.

12.4.3. In case of non-return of the physical Card on the day of submitting the application, the Bank will block the Card, and the Non-Deductible Balance (and other funds in the account) will also be returned to the Client strictly within 30 (thirty) calendar days.

12.5. The Bank may unilaterally terminate the Agreement and close the Card Account in the following cases:

12.5.1. Destruction (cancellation) by the Bank of all the Client's Cards due to their expiration date and non-demand during the period specified in the Instructions;

12.5.2. Breaches by the Client or the Holder of the terms of the Agreement, the rules of the IPS/NPS or the requirements of the laws of the Republic of Uzbekistan;

12.5.3. There are reasonable suspicions of using the Bank's services to legalize income from criminal activities, terrorist financing (AML/CFT/FPWMD) or other illegal purposes;

12.5.4. If the Client withdraws consent to the processing of personal data, if this makes it impossible to further fulfill the obligations under the Agreement.

12.5.5. Failure by the Client to provide documents, information or Client Profiles requested by the Bank in accordance with this Offer.

12.5.6. In other cases stipulated by the laws of the Republic of Uzbekistan.

12.6. Final termination of the Agreement and closure of the Card Account shall be carried out on the day the application is submitted, provided there are no blocks (holdings) on the cards. In the event of existing blocks on operations, the final closure of the Card Account shall be carried out within 30 (thirty) calendar days from the date of application submission. Upon closure of the Card Account and/or cancellation of the Cards, the Bank unilaterally initiates the deactivation (removal) of all Tokens issued to these Cards in the Digital Wallets.

12.7. After termination of the Agreement, the remaining funds (taking into account the retention periods of the Non-Deductible Balance according to clause 12.4) shall be transferred to the Client's Bank account or, upon written request, issued in cash at the Bank's cash department.

12.8. Upon termination of the Agreement, Card issuance/maintenance fees, transaction processing fees and other fees previously paid to the Bank in accordance with the Tariffs will not be refunded to the Client.

12.9. By accepting this Offer, the Client applies to the Bank in advance with a request to terminate the Agreement and close the Card Account in case of no funds and incomplete transactions within 6 (six) consecutive months. The Parties also recognize this clause of the Agreement as a proper application by the Client to close the account in accordance with part 1 of Article 788 of the Civil Code of the Republic of Uzbekistan. The procedure provided for in this paragraph is a simplified termination procedure by agreement of the parties in the absence of Client activity.

13. DISPUTE RESOLUTION

13.1. All disputes and disagreements arising in the process of fulfilling the terms of this Agreement are subject to settlement in a preliminary claim procedure through negotiations.

13.2. If the Parties failed to reach an agreement through negotiations, the dispute is referred to the judicial authorities in accordance with the laws of the Republic of Uzbekistan.

13.3. The Parties define that all disputes under this Agreement shall be considered in court at the Bank's venue, unless otherwise expressly provided for by mandatory laws.

14. FINAL PROVISIONS

14.1. By accepting this Offer, the Client confirms that it has fully read, agrees and undertakes to comply with the Bank's applicable Tariffs, which are an integral part of the Agreement.

14.2. All issues not directly regulated by this Agreement are governed by the applicable laws of the Republic of Uzbekistan, as well as business customs applicable in banking practice.

14.3. The Bank's information messages and notifications are communicated to the Client by the methods specified in the Section of 6this Agreement.

14.4. The Client's consent to the processing of personal data given under this Agreement is valid until the complete termination of the obligations of the Parties, or until the data retention periods established by law expire. The procedure for revoking consent is regulated by the Section 8 of this Offer.

14.5. By accepting this Offer, the Client agrees that the Bank has the right to unilaterally amend this Agreement or to set out the Agreement in a new version.

14.6. Continuing to use the Card or Tokens in Digital Wallets, or performing any Operation after notifying the Bank of changes to the Agreement or presenting it in a new edition, is recognized as acceptance by the Client. At the same time, all previously provided consents by the Client within the framework of this Offer shall retain their legal force.

14.7. By accepting this Offer, the Client confirms that it has sufficient command of the English language, understands the meaning of all terms and conditions of this Agreement, and by its informed decision, it has chosen the English version of the Offer. The Client confirms that all the provisions of the Agreement are clear thereto, accepted thereby without any exceptions and accepted in this language by virtue of his full understanding, preferable to any other language.

14.8. The following applications are an integral part of this Offer:

14.8.1. Appendix No. 1 – Compliance conditions

14.8.2. Appendix No. 2 – T&C for the tokenization and use of JSC "Octobank" bank cards in digital wallets and payment services

15. BANK DETAILS

Octobank JSC
Legal address: 100021, Republic of Uzbekistan, Tashkent, Furkat st., 2
TIN: 203644820
NCEA: 64190
Bank code: 00980
Address: 2980 2000 7000 0098 0110
Website: www.octobank.uz
Phone: +998 (71) 202-33-33
Email address: info@octobank.uz

Appendix No. 1
to the Public Offer on Issuing and
Servicing Individual Bank Cards.

COMPLIANCE CONDITIONS

1. PURPOSE AND DEFINITIONS

1.1. The purpose of these Terms of Compliance (the "Terms") is to prevent the risks associated with compliance with the laws and international standards for the Client arising in the areas of:

- "Combating money laundering, terrorist financing and financing the proliferation of weapons of mass destruction" ("AML/CFT/FRMU/FPWMD");
- "Combating bribery and corruption" (CB&C);
- Sanctions and export control measures.

Money laundering shall mean legitimization of the possession, use, or disposal of funds or other property obtained as a result of a crime.
Terrorist financing shall mean provision of funds or financial support to terrorists.
Corruption shall mean illegal use of an official position to gain benefits.
Bribery shall mean transfer, promise, or authorization of receiving a bribe for illegal influence.
Sanctions shall mean financial and property restrictions, economic and trade measures imposed by government agencies.
Sanctions list shall mean a list of individuals and/or legal entities, countries, goods and services subject to sanctions.
Export control shall mean laws and regulations governing the import, export, and transfer of goods, technologies, and services.
Bank shall mean Octobank Joint Stock Company, which is a financial institution providing banking services, including cash transactions and lending.
Client shall mean an individual who has entered into a contractual relationship with the Bank and undertakes to comply with these Terms.

2. LEGAL BASIS

2.1. As part of these Terms, the client undertakes to comply with the laws of the Republic of Uzbekistan and international standards.

2.2. The following documents are not limited to local requirements:

- Criminal Code of the Republic of Uzbekistan;
- Law On Combating Corruption;
- Law On Combating the Legalization of Proceeds of Crime and the Financing of Terrorism;
- Client's procedures in the field of AML/CFT/CFMEU/FPWMD, CB&C and sanctions.

2.3. International standards include:

- FATF recommendations on combating money laundering;
- ISO 37001:2025 — Anti-corruption system standard;
- Sanctions lists of the UN Security Council, the EU, OFAC, the UK and other bodies.

3. INTERNATIONAL SANCTIONS

3.1. International sanctions shall mean financial and material restrictive measures, economic and trade restrictions imposed or applied by international organizations such as the United Nations, the EU, the United States, the United Kingdom and others.

3.2. For the purposes of these Terms, a person subject to restrictive measures" shall mean a legal entity or individual subject to international sanctions.

3.3. The Client undertakes not to provide goods, services or financing that may violate international sanctions.

4. CLIENT'S RESPONSIBILITIES

4.1. The Client undertakes to comply with the laws of the Republic of Uzbekistan and the international standards specified in paragraphs 2 and 3, in particular:

- not to engage in money laundering
- not to engage in terrorist financing;
- not to contribute to financing the proliferation of weapons of mass destruction;
- not to engage in financial fraud;
- not to provide bribes to employees or third parties;
- not to enter into transactions with sanctioned clients;
- ensure full and transparent provision of documents on transactions and goods.

4.2. The Client releases the Bank from liability for any losses, costs or penalties related to the breach of these terms.

5. BANK'S RIGHTS

5.1. If the Client breaches the terms of these Terms, the Bank has the right to unilaterally terminate contractual relations with the Client without any liability.

5.2. If there is a risk of sanctions being applied to the Bank, it may refuse to conclude a contract or conduct operations.

---

end

Appendix No. 2
to the Public Offer on Issuing and
Servicing Individual Bank Cards.

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.

---

end