APPROVED
by resolution of the Board of KOMPANION BANK CJSC
dated 23 January 2026

EFFECTIVE from
6 February 2026

PUBLIC OFFER OF KOMPANION BANK CJSC FOR INDIVIDUALS TO CONCLUDE A REMOTE BANKING SERVICE AGREEMENT

This Offer shall be deemed public in accordance with Part 2 of Article 398 of the Civil Code of the Kyrgyz Republic and shall constitute a perpetual offer by Kompanion Bank CJSC (hereinafter referred to as the Bank) to eligible and capable individuals to conclude a Remote Banking Service Agreement, the terms and conditions of which are set forth in this Offer below (hereinafter referred to as the Agreement).

The Agreement shall be deemed concluded in writing upon acceptance by the responding individual (hereinafter referred to as the Client). The acceptance shall be considered complete and received upon installation and first login to the Kompanion mobile application (hereinafter referred to as the Mobile Application). The acceptance shall be considered complete and unconditional and, in accordance with Part 3 of Article 399 and Article 402 of the Civil Code of the Kyrgyz Republic shall mean the conclusion (signing) and acceptance by the Client of all the terms of the Agreement.

The Agreement shall enter into force only upon successful completion of the Client's due diligence, including the procedure for identifying and verifying the Client remotely, as well as the provision by the Client of all documents and/or information required for remote banking service in accordance with the requirements of the legislation of the Kyrgyz Republic, local regulations of the Bank and the Agreement.

This Offer shall be valid until it is declared invalid, or a new version of this Offer or a new offer is published.

1. SUBJECT MATTER OF THE AGREEMENT

1.1. In accordance with the Agreement, the Bank shall provide remote banking service to the Client who has access to the Internet and an appropriate access device (mobile device), i.e. services for remote round-the-clock management of an electronic wallet, as well as bank accounts and a payment card (if any) of the Client using the Mobile Application in real time on the terms stipulated by the Agreement and the legislation of the Kyrgyz Republic.

1.2. The list of remote services/transactions available in the Mobile Application (hereinafter referred to as the List of Services), tariffs and limits (restrictions) on transactions shall be an integral part of the Agreement and shall be posted on information stands at the Bank's branches and on the Bank's website www.kompanion.kg (hereinafter referred to as the Bank's Website) and/or in the Mobile Application. The list of services, tariffs and limits (restrictions) may be changed and/or supplemented by the Bank unilaterally, including on the basis of the requirements of the legislation of the Kyrgyz Republic, and shall be communicated to the Client by posting on information stands at the Bank's branches, on the Bank's Website and/or in a Mobile Application and/or by other available means.

for Official Use Only

2. USING A DIGITAL IDENTIFIER

2.1. The use of passwords, codes and other identifiers for logging into the Mobile Application and/or confirmations (hereinafter referred to as the Code/Codes) shall be recognized as the use of a digital identifier in accordance with the Digital Code of the Kyrgyz Republic (hereinafter referred to as the Identifier). In accordance with the legislation of the Kyrgyz Republic the Client's use of the Identifier shall be considered equivalent to the use of a handwritten signature and shall entail the same legal consequences as a handwritten signature.
2.2. Instructions to carry out transactions (payment orders), statements and other actions performed in the Mobile Application after logging in using Codes (authorization, authentication) shall be considered to have been properly performed by the Client and sufficient to confirm the Client's decision to perform an action/transaction.
2.3. The Client's last name, first name, patronymic (if any) contained in the Client's application form, as well as the phone number and Codes entered by the Client, shall be considered contact information that clearly identifies the Client who signed the Agreement or digital document.
2.4. The identification of the person who signed the Agreement or digital document with an Identifier shall be carried out by comparing and determining the identity of:
1) the phone number specified in the Client's application form during his/her identification with the phone number to which the Code was sent;
2) and/or a Code sent to the Client's phone number with the entered Code;
3) and/or the PIN code entered for the first time when logging into the Mobile Application with the PIN code entered at the subsequent login to the Mobile Application.
It is sufficient to use one of the listed methods to identify a Client. The Bank may, at its discretion, use additional methods to identify the person who signed the digital document.
2.5. Relations regarding the use of the Identifier, which are not regulated in the Agreement, shall be governed in accordance with the Digital Code of the Kyrgyz Republic.

3. CONSENTS AND ACKNOWLEDGEMENTS

3.1. The Client hereby confirms and guarantees that:
– The Code/Codes contact information are considered to be his/her Identifier, which can be used to send notifications for the purpose of establishing, changing, or terminating legal relationships, including signing the Agreement, orders, consents, applications, and other digital documents in the Mobile Application;
– accurate data and contact information have been provided when filling out the application form;
– when logging into the Mobile Application and in the application form, he/she has entered a telephone number that belongs to him/her (the subscriber);
– there is no third-party access to the Client's phone number, as well as to the mobile device itself;
– he/she has read and agrees with the text of this Offer (Agreement), including the List of Services, tariffs, limits (restrictions), information on compliance with the Security Requirements for Remote Banking Services (Annex 1 to the Agreement, an integral part of the Agreement);
– he/she agrees and fully accepts the risks associated with the use of unsecured communication channels when exchanging information via SMS messages and the Internet, associated with unauthorized access by third parties to the Code/Codes.

for Official Use Only

3.2. The Client confirms that he/she is the legitimate owner of the funds and that the source of the funds credited to his/her bank account/payment card/e-wallet is legitimate; his/her bank account/payment card/e-wallet will not be used for any illegal purposes.
3.3. The Client freely, consciously, and voluntarily gives consent to the Bank for the collection, processing, transfer, and cross-border transfer of his/her personal data in accordance with Annex 2 to the Agreement.
3.4. The Client gives his/her consent to the provision of any information regarding the Client's credit history to credit bureaus, as well as to the receipt by authorized employees of the Bank of a credit report from credit bureaus in accordance with the legislation of the Kyrgyz Republic and other participants in the credit information exchange system for the purposes stipulated by the legislation of the Kyrgyz Republic. The date of consent shall be the date of signing the Agreement (Acceptance of this Offer).
3.5. The Client gives his/her consent to the Bank to receive from it advertising messages, newsletters about the products, services of the Bank and its partners, about promotions, discounts and special offers, sweepstakes, competitions, surveys by email and phone number of the Client, as well as in instant messengers, including Telegram, WhatsApp, by mail, SMS messages, push notifications, as well as communicating such information to the Client verbally by phone.
3.6. The Client gives his/her consent to the Bank to disclose banking secrets, including information about the Client and his/her banking operations (transactions) in case the Bank initiates civil, administrative or criminal proceedings in connection with violation of the legislation of the Kyrgyz Republic using the Bank's services and products. The date of consent shall be the date of signing the Agreement (Acceptance of this Offer).
3.7. If the Client or his/her ultimate beneficiary is a resident of the United States of America, he/she agrees to provide the Bank with information in accordance with the US Foreign Account Tax Compliance Act (FATCA) and an intergovernmental/international agreement.
3.8. The Client agrees and gives his/her order (instruction) to the Bank:
– to write off funds from his/her accounts/cards/e-wallets as a matter of priority and without acceptance, in order to pay for the Bank's services and/or repay debts owed to the Bank;
– to close the Client’s bank account without notice if there are no funds in the said bank account for 12 (twelve) calendar months or no transactions have been made at the Client’s request (with the transfer of the remaining funds to the Bank’s off-system accounts for the possibility of their further withdrawal by the Client at the Bank’s cash desks);
– in the event of closure/return of a fixed-term bank deposit opened in accordance with paragraph 4 of Chapter 5 of the Agreement (hereinafter referred to as the deposit), to close the deposit account without notice;
– close (terminate) without notice the payment card and the corresponding demand account (card account) of the Client in the event of the Client’s failure to appear at the Bank to receive the payment card within a period of more than 3 (three) calendar months from the date of filing the application for the issue of the payment card, or in the event that there are no funds/movements on the payment card for 12 (twelve) calendar months, or if the amount of funds on the payment card (card account) of the Client is below the established minimum amount.
3.9. The Parties acknowledge and confirm that all orders and other electronic documents received by the Bank in the Mobile Application system:
– are considered to be genuine, identical and complete documents originating from the Client;

for Official Use Only

– are the basis for performing transactions in the Mobile Application and other legally significant actions;
– are equivalent to and have the same legal force as orders/documents received from the Client on paper, signed with the Client's own signature and executed in accordance with the legislation of the Kyrgyz Republic.
3.10. The Parties acknowledge that any notifications and correspondence are considered delivered and received by the Client if sent in accordance with the Agreement and/or the legislation of the Kyrgyz Republic using contact information, including the last known addresses/numbers of the Client, or via the Mobile Application system.
3.11. The Parties acknowledge that the Mobile Application system is sufficient to ensure reliable and efficient operation during processing, storage, reception and transmission of information.
3.12. The Parties acknowledge that the technologies used are sufficient to protect against unauthorized access, as well as to confirm the authenticity of digital documents.

4. REGISTRATION AND IDENTIFICATION OF THE CLIENT

4.1. **Registration in the Mobile Application:**
4.1.1. To install a Mobile Application on a mobile device, it is necessary to download it from the Apple (Apple Store) or Google/Android (Play Market) app stores.
4.1.2. When first logging into the Mobile Application, the Client provides his/her valid mobile phone number, creates and enters a password for the Mobile Application, consisting of at least 8 characters: letters (upper and lower case), special characters, and numbers. The password is optional, and the Client can configure it to be mandatory or optional, if needed. An SMS message containing a one-time four-digit code (OTP code) is sent to the specified phone number. This OTP code must be entered by the Client within a short period of validity in a special field in the Mobile Application.
4.1.3. For the convenience of subsequent logins to the Mobile Application, the Client must create and enter a four-digit PIN code that meets the security requirements (Annex 1 to the Agreement), and also, if desired, scan a fingerprint (if this function is available on the Client's mobile device).
4.1.4. In certain cases of subsequent login to the Mobile Application (for example, in the case of updating the Mobile Application, changing the PIN code, etc.), the Client must perform the actions specified in subparagraphs 4.1.2 and 4.1.3 of the Agreement.
4.1.5. The Client's mobile phone number specified when logging into the Mobile Application is assigned to the e-wallet as its identification number. Assigning an identification number to the e-wallet does not mean that the e-wallet or the Client has been identified. The Client's e-wallet is considered identified only after the Client has been successfully identified. It is necessary to visit a Bank branch to change the e-wallet identification number (if the Client's phone number has changed).
4.2. **Identification of the Client:**
4.2.1. Identification of the Client shall be carried out:
– at the Bank's branches (or, if possible, at the branches of the Bank's agents);
– remotely via the Mobile Application;
– in any other manner provided for by the legislation of the Kyrgyz Republic.
4.2.2. To identify remotely via the Mobile Application, the Client must, following the instructions, enter passport and other data, take a photo of the front and back of the passport,

for Official Use Only

take a photo of themselves with the passport, answer questions by voice, initiate a video call (performing one or more of these actions may not be required), and perform other actions.
4.2.3. The Client must undergo the identification procedure at the Bank's branches (or, if possible, at the branches of the Bank's agents) in cases stipulated by the legislation of the Kyrgyz Republic, or at the request of the State Financial Intelligence Service, the National Bank of the Kyrgyz Republic, and the Bank.
4.2.4. No more than one identified e-wallet can be opened in the Client's name.
4.2.5. The Bank refuses to identify the Client in the event of failure to perform or improper performance of the actions specified in subparagraphs 4.2.2, 4.2.3 and 4.2.4 of the Agreement, as well as in other cases stipulated by the Agreement and/or the legislation of the Kyrgyz Republic.
4.3. The personal data of the Client (last name, first name, patronymic, passport details or details of another submitted identity document, in accordance with the legislation of the Kyrgyz Republic) and other personal data of the Client provided to the Bank during the identification of the Client shall be considered an integral part of the Agreement.

5. PROCEDURE FOR PROVIDING REMOTE SERVICES/CONDUCTING TRANSACTIONS

§1. General service procedure

5.1. Remote banking services shall be provided to the Client remotely via the Internet using a Mobile Application installed on the Client's mobile device that meets technical and other requirements.
5.2. Services/transactions in the Mobile Application according to the List of Services within the established limits (restrictions) shall be available to the Client in case of successful registration in the Mobile Application and identification of the Client. Services/transactions on bank accounts and/or payment cards in the Mobile Application may not be available to certain categories of Clients, as well as if they have not been used for more than 3 (three) consecutive months and may be activated on the basis of a written application submitted by the Client at the Bank's branches (or, if possible– at the branches of the Bank's agents), or after additional identification/verification of the Client through the Mobile Application, the procedure of which can be determined by the Bank independently.
5.3. Transactions in the Mobile Application shall be conducted based on the Client's instructions (payment orders). Transactions may be conducted on other grounds specified in the Agreement and the legislation of the Kyrgyz Republic.
5.4. An order for a transaction in the Mobile Application shall be considered to be generated, certified and given by the Client to the Bank upon provision of payment details by filling out the relevant forms in the Mobile Application, except for the cases stipulated in paragraph 3.7 of the Agreement.
5.5. All payments made through the Mobile Application shall be considered confirmed and final (unconditional and irrevocable) from the moment the mutual settlements are completed in the relevant service provider's system and final settlements are made. For the Client, a payment shall be considered irrevocable upon receipt of confirmation of payment acceptance for execution and final when funds are debited from the Client's e-wallet, bank account, or payment card and simultaneously credited to the recipient's account.
5.6. If the currency of the received amount of money differs from the currency of the account/card/e-wallet, the Bank may (if possible) convert this amount at the Bank's purchase

for Official Use Only

rate for the corresponding currency, or at the official rate of the National Bank of the Kyrgyz Republic.
If an amount is converted at an erroneous exchange rate due to a technical failure or other reasons, the transaction amount will be recalculated and converted at the Bank's accurate exchange rate for the relevant currency, or at the official exchange rate of the National Bank of the Kyrgyz Republic. The Client is obligated to reimburse the Bank for the resulting difference within 5 (five) business days.
5.7. The transaction cannot be performed in the following cases:
– exceeding the limits and violating the restrictions provided for by the Agreement and the legislation of the Kyrgyz Republic;
– insufficient funds to carry out the transaction, with the exception of cases of overdraft and payment for services of the Bank and/or the Bank's agent;
– error when specifying payment and/or other details;
– failure to provide at least one of the required documents (details) necessary for the Bank to carry out the transaction and/or proper verification of the Client in accordance with the legislation of the Kyrgyz Republic, the Agreement;
– blocking of the Client's e-wallet/account/card at the initiative (application) of the Client or the Bank in accordance with the Agreement, as well as seizure in accordance with the legislation of the Kyrgyz Republic;
– the transaction will be a violation of the legislation of the Kyrgyz Republic and/or the terms of the Agreement, including the receipt of a transfer from a legal entity or individual entrepreneur in favor of a Client identified remotely, with the exception of a transaction to return a previously made payment (for example, in connection with the refusal of a product or service), as well as a payment by a Client identified remotely in favor of a non-profit organization (resident);
– no connection or failures in connection to the Internet;
– technical work carried out by the Bank in the Mobile Application system;
– in other cases stipulated by the Agreement and the legislation of the Kyrgyz Republic.

§2. E-wallet servicing

5.8. E-wallet transactions shall be carried out only with electronic money denominated (expressed) in the national currency of the Kyrgyz Republic.
5.9. In case of replenishment of the e-wallet with funds in foreign currency through the Bank's cash desk, the Bank shall credit (issue) an equivalent amount of money in national currency, converted at the foreign currency purchase rate established by the Bank, or at the official rate of the National Bank of the Kyrgyz Republic on the date of crediting.
5.10. In the event of deactivation or cancellation of the mobile phone number in the cellular operator's system used to register the Client's e-wallet (the e-wallet identification number), the Client's e-wallet will be blocked/closed. In this case, the remaining e-money will be transferred to a special Bank account and may be retrieved by the Client upon written request.

§3. Bank account servicing

5.11. Bank accounts can be opened/closed upon the Client's request:
– at the Bank's branches;
– remotely via the Mobile Application (if such an option is provided).

for Official Use Only

5.12. The Client can only open demand deposit accounts and deposit accounts through the Mobile Application. If an account is opened remotely through the Mobile Application, the account number will be communicated to the Client by any means of communication no later than the next business day after it is opened.
5.13. In addition to the Client's personal funds, demand deposit accounts may be credited with wages, royalties, pensions, alimony, social benefits, funds from another bank account, payments related to inheritance, fees for the sale of personal property belonging to the account holder, money transfers and other receipts and payments, including loan payments.
5.14. From the demand deposit account, the Client can make personal payments, including payments for goods purchased for personal purposes (services rendered), loan repayments, utility bills and other similar payments of a personal nature.
5.15. Interest on funds held in demand deposit accounts is not accrued or paid by the Bank unless otherwise provided for in separate contracts/agreements between the Parties.
5.16. All payments and transactions on the account shall be carried out in the account currency.
5.17. Crediting of funds in foreign currency received in favor of the Client shall be carried out by the Bank no later than the business day following the day of receipt of the account statement of the relevant correspondent bank.
5.18. Transactions on the account at the Bank’s branches shall be carried out under the following conditions:
– transactions are carried out after receiving a written order on the basis of a payment document drawn up in accordance with the requirements of the legislation of the Kyrgyz Republic, within the limits of the balance of funds in the account, unless otherwise provided by the Agreement or the legislation of the Kyrgyz Republic;
– payment documents are accepted for execution within the time period established by the Bank for servicing Clients (hereinafter referred to as Operational Hours), including settlements carried out on the day of submission of documents received during Operational Hours. Documents received by the Bank after the expiration of Operational Hours are executed by the Bank on the following business day;
– if the Client instructs the Bank to carry out several transactions, the amount of which exceeds the balance on his/her account, the Bank carries out the transactions at its own discretion within the limits of the balance on the account and/or in accordance with the legislation of the Kyrgyz Republic;
– under other conditions stipulated by the legislation of the Kyrgyz Republic and the requirements of the Bank.
5.19. The terms of the deposit shall be governed by a separate agreement, and in the case of its remote opening via the Mobile Application, by paragraph 4 of this Chapter. The deposit shall be returned and interest shall be paid by crediting it to the Client's demand deposit account, unless otherwise provided by the Term Deposit Agreement or paragraph 4 of this Agreement.
5.20. The terms of a deposit with other terms of return shall be regulated by a separate agreement.

§4. Deposit servicing

5.21. In accordance with the Agreement, the Client may open a deposit account through the Mobile Application, the terms of which are contained in this paragraph, the List of Services, as

for Official Use Only

well as in the deposit information in the Mobile Application, which is an integral part of the Agreement.

5.22. Information about the deposit offers general terms of the deposit (currency, possible terms, minimum initial amount, maximum initial amount, minimum one-time replenishment amount, maximum replenishment amount per month, interest payment procedure, interest capitalization procedure and period (if capitalization is provided), and other conditions) shall be specified in the List of Services.

5.23. The Client selects the deposit term from the available terms on the relevant pages of the Mobile Application, and the deposit amount is deposited (replenished) by the Client. The nominal interest rate on the deposit shall be determined based on the deposit term. The amount, term, and nominal interest rate on the deposit are further specified in the deposit information in the Mobile Application, which is an integral part of the Agreement.

5.24. The terms of this paragraph and other terms of the Agreement regarding the deposit shall come into force from the moment the deposit amount is received into the deposit account and shall remain valid until the date of return of the deposit.

5.25. In case of opening a deposit or additional replenishment of the deposit (if replenishment is provided) on weekends/holidays, the deposit/additional replenishment is considered accepted on the next business day.

5.26. Interest on the deposit amount is accrued from the date of its receipt by the Bank, and on the deposit replenishment amount (if replenishment is provided) - from the date of such replenishment until the day preceding its return to the Client or its debiting from the Client's account for other reasons.

5.27. When calculating the annual base for interest accrual, the actual number of days in the year is taken into account.

5.28. Payment of accrued interest is carried out depending on the terms of the deposit product as follows:

- *quarterly, by capitalization on the scheduled interest capitalization dates. Interest capitalization is an automatic increase in the deposit amount due to accrued interest within the timeframes established by the agreement.*
- *monthly on the scheduled dates of interest payment to the Client's account. The scheduled date of interest payment is the date of each month similar to the date of opening of the deposit.*
- *at the end of the deposit term (on the date of return of the deposit).*

5.29. If the date for the return of the deposit and/or accrued interest falls on a weekend or holiday, then the payment is made on the following business day.

5.30. Automatic extension of the deposit term is not provided.

5.31. Upon the deposit's return date and unclaimed status, this paragraph shall cease to be in effect, and the terms of the demand deposit shall apply to the deposit at the Bank's current rates. The Bank shall credit the deposit amount and accrued interest to the demand deposit account and close the deposit account.

5.32. In the event of early full or partial withdrawal of the deposit amount at the initiative of the Client, the total accrued amount of interest on deposits in foreign currency is not paid, and for deposits in national currency it is recalculated and paid in the following order:

1) within a period of 12 (twelve) months from the date of receipt of the deposit:

- for savings and term deposits – is not paid;

for Official Use Only

- for a pension deposit – is recalculated from the date of receipt of the deposit to the date preceding the date of return of the deposit, and paid at an interest rate of 3% (three percent) per annum;
2) after 12 (twelve) months from the date of receipt of the deposit, it is recalculated from the date of receipt of the deposit to the date preceding the date of return of the deposit, and is paid at the following interest rate:
- for savings and pension deposits - 3% (three percent) per annum;
- for other term deposits - in the amount of 30% (thirty percent) of the established nominal interest rate of the deposit.
5.33. If, in accordance with the requirements of the legislation of the Kyrgyz Republic, tax withholding is provided for on the amount of interest received under the terms of this paragraph (deposit agreement), the Bank shall withhold taxes on the amount of interest paid or the amount of the deposit returned.
5.34. Other conditions of the deposit, not provided for in this paragraph, shall be governed by the legislation of the Kyrgyz Republic, as well as the Agreement to the extent applicable.
5.35. The deposit is protected in accordance with the Law of the Kyrgyz Republic "On the Protection of Bank Deposits".

§5. Payment card servicing

5.36. The issue and servicing of a payment card issued by the Bank shall be carried out in accordance with the Rules for Issuing and Servicing Bank Payment Cards in Kompanion Bank CJSC, which are an integral part of the Agreement and published on the Bank's Website, as well as the legislation of the Kyrgyz Republic and the Agreement to the extent applicable.
5.37. If such a service is available in the Mobile Application, the Client may link a payment card issued by another issuing bank in the Client's name to the Mobile Application and perform transactions in the Mobile Application using the funds on it (in accordance with the tariffs and within the established limits (restrictions)). Linking is carried out by entering the payment card details (payment card number, expiration date, CVV/CVC code) in the Mobile Application or by another method provided in the Mobile Application.

6. PROCEDURE FOR PAYMENT FOR SERVICES

6.1. The Bank's remote services (the Bank's fees for conducting transactions, hereinafter referred to as the fees) shall be paid by the Client in accordance with the Bank's current tariffs, unless otherwise provided by a written additional agreement to the Agreement.
6.2. Payment for the Bank's services under the Agreement may be made by direct debiting (without the Client's consent) from any account and/or card and/or e-wallet of the Client. In the event of a currency difference, the Bank may convert the debited Commission amount at the Bank's purchase rate for the relevant currency or the official exchange rate of the National Bank of the Kyrgyz Republic on the day of debiting.
6.3. All expenses of the Bank and/or third parties associated with the execution of the Client's orders shall be reimbursed at the expense of the Client, including in the manner specified in paragraph 6.2 of the Agreement.
6.4. If a transaction is carried out through a Bank agent, an additional commission may be charged in accordance with the Bank agent's tariffs, information about which is provided directly by the Bank agent.

for Official Use Only

6.5. If a transaction is carried out in the Mobile Application using funds in a linked payment card issued by another bank (if such a service is available in the Mobile Application), a commission may be charged in accordance with the issuing bank's tariffs, information about which is provided directly by the issuing bank.
6.6. The commission is not included in the transaction amount and does not reduce it. The commission amount includes all taxes and fees in accordance with the legislation of the Kyrgyz Republic, unless otherwise provided in tariffs and legislation of the Kyrgyz Republic.
6.7. The amount of the Commission written off for a transaction carried out due to the Client's error is not subject to return.

7. RIGHTS AND OBLIGATIONS OF THE CLIENT

7.1. **The Client has the right to:**
7.1.1. use the services in the manner and under the conditions stipulated by this Agreement;
7.1.2. freely dispose of funds in the account, card, e-wallet, except for cases stipulated by the Agreement and the legislation of the Kyrgyz Republic;
7.1.3. if necessary, receive from the Bank confirmation on paper (certified copies) of the execution of instructions (payment orders) for transactions carried out in the Mobile Application system, and account statements in the manner prescribed by the Agreement;
7.1.4. terminate the Agreement unilaterally by submitting a written application subject to payment of Commissions or debt to the Bank and completion of other mutual settlements.
7.1.5. close a bank account/payment card/e-wallet or one of the bank accounts/deposits by submitting an application for closure at the Bank's branches, or individual ones by performing the relevant operation in the Mobile Application (pressing the "close" button), which is equivalent to submitting the application specified in Annex 3 to the Agreement, if such an option is provided.

7.2. **The Client is obliged to:**
7.2.1. independently and at its own expense provide the technical, software and communication resources necessary for accessing the Internet and connecting to the Mobile Application system;
7.2.2. strictly maintain the confidentiality of the Codes and do not disclose them to third parties, comply with and be guided by the Security Requirements for Remote Banking Services (Annex 1 to the Agreement);
7.2.3. provide the Bank with all documents and information required by the legislation of the Kyrgyz Republic, local regulations of the Bank and the Agreement for opening an account/card/e-wallet, as well as for carrying out transactions on them;
7.2.4. after sending orders, independently verify their receipt and execution by the Bank. If the fact of their receipt and/or execution is not confirmed, the Client may submit a request to the Bank to clarify the reasons for non-receipt/non-execution;
7.2.5. when sending orders, use information processing, storage and protection systems only on a serviceable access device that has been checked for the absence of computer viruses;
7.2.6. promptly provide information and copies of documents in the event of a change in contact information, including phone number and other information specified in the Client's and/or beneficial owner's application form, or in other cases stipulated by the legislation of the Kyrgyz Republic;
7.2.7. immediately inform the Bank in writing or by calling (0312) 338800 or 8800 (customer

for Official Use Only

service phone numbers):
– about the detection of unauthorized access or an attempt of unauthorized access to the Code/Codes, phone number (SIM card), or the Client's access device;
– about the loss or theft by a third party of the Code/Codes, phone number (SIM card), or the Client's access device;
7.2.8. inform the Bank about erroneous crediting of funds to the Client's account/card/e-wallet and return to the Bank the erroneously credited funds no later than the next day after detection and/or notification by the Bank;
7.2.9. not use the services or products provided by the Bank for illegal purposes, including not carry out actions/transactions aimed at financing terrorist or extremist activities and legalization (laundering) of criminal proceeds or in the interests of third parties for the purpose of committing illegal/fraudulent actions, not sell/transfer to third parties accounts/cards/e-wallets, access to the Mobile Application, as well as details, PIN/Codes, logins and passwords to them;
7.2.10. upon the Bank's first request, provide, within 3 (three) business days, the requested information and documents related to the Client's activities and banking transactions, as well as documents confirming the legality and economic feasibility of the transaction/transactions in accordance with the requirements of the legislation of the Kyrgyz Republic. The Bank's request may be either written or oral;
7.2.11. for proper use of the Mobile Application, including in the event of prolonged non-use for more than 3 (three) months, follow the sequence of actions specified in the Guide to Using the Kompanion Mobile Application (Annex 4 to the Agreement).
7.2.12. fulfill other obligations stipulated by the Agreement and the legislation of the Kyrgyz Republic.

8. RIGHTS AND OBLIGATIONS OF THE BANK

8.1. **The Bank has the right to:**
8.1.1. require the Client to provide additional documents and information related to the account/card/e-wallet transaction and/or confirming the legality of the transaction, for the purpose of combating the financing of terrorist activities and the legalization (laundering) of criminal proceeds, and the economic feasibility of the transaction, including one already completed. In the event of the Client's refusal to provide the required documents, the Bank reserves the right to refuse to carry out any banking transactions of the Client.
8.1.2. unilaterally terminate the Agreement in whole or in part, in cases where:
– the Client has not submitted the relevant documents/information necessary to meet the requirements for identification and verification of the Client and the establishment of the beneficial owner, other measures for due diligence of the Client, for conducting transactions on the account/card/e-wallet;
– the Client has not provided the documents/information required to carry out transactions on the account/card/e-wallet, confirming the economic feasibility of the transaction being carried out and the validity of the Client's real economic activity;
– the Client provided false documents/information;
– the Client does not pay for the services provided by the Bank according to the Tariffs;
– this Offer will be deemed to have lost its force, or a new offer will be published;
– in other cases stipulated by the legislation of the Kyrgyz Republic, the Agreement;

for Official Use Only

8.1.3. unilaterally (without concluding separate agreements with the Client) make changes/additions to the Agreement, except in cases of reducing the amount of interest on the deposit, by changing/supplementing this Offer and notifying the Client via the Mobile Application and/or posting (publishing) them on information boards in the Bank's branches, the Bank's Website, in the Mobile Application at least 10 (ten) business days prior to the effective date of these amendments/additions;
8.1.4. change the Client's bank account number with subsequent notification to the Client via the Mobile Application and/or at the last known address and/or via phone/email message to the phone number/email address. After changing the bank account number, all funds are transferred to the new bank account and subsequent transactions are conducted through the new bank account;
8.1.5. engage other banks, other financial and credit organizations, payment organizations or payment system operators at their discretion to conduct transactions;
8.1.6. write off funds from all of the Client's accounts/cards/e-wallets with the Bank without further authorization in the cases and in the manner stipulated by the legislation of the Kyrgyz Republic and the Agreement, as well as in the event of the Client's outstanding debt to the Bank arising from any legal relationship between the Bank and the Client, in the event of an erroneous or unjustified crediting of funds to the Client. If the currency of the Client's debt differs from the currency of the account/card/e-wallet, the exchange rate set by the Bank or the official exchange rate of the National Bank of the Kyrgyz Republic shall be applied for conversion;
8.1.7. in cases where the Client's order (payment instruction) contains incomplete, distorted, inaccurate, or contradictory information, or is missing, the Bank may delay crediting the amount to the Client until it receives documents containing the necessary information. The Bank also reserves the right to return the amount to the sender if the document contains missing information or incorrect information necessary for proper verification of the Client;
8.1.8. suspend/block the Mobile Application or all or individual transactions on the account/card/e-wallet in cases stipulated by the legislation of the Kyrgyz Republic, the Agreement, including in the event of failure to comply with subparagraphs 4.2.3 and 7.2.9 of the Agreement, change of the Client's phone number, as well as in cases of commission or any suspicion of commission of fraudulent or criminal transactions;
8.1.9. refuse the Client to perform a transaction:
– in case of incomplete/incorrect indication by the Client of the details of the transaction being carried out, or violation of the deadlines for its execution;
– non-compliance of the transaction with the legislation of the Kyrgyz Republic, including the requirements of the legislation in the area of combating the financing of terrorist or extremist activities and the legalization (laundering) of criminal proceeds;
– in cases where there are insufficient funds in the Client’s account/card/e-wallet to complete the transaction and/or to pay the Bank’s fee for the transaction being completed;
– in cases stipulated by the legislation of the Kyrgyz Republic;
8.1.10. in order to carry out the transaction, if necessary, request the Client to issue a hard copy of the document with the Client's handwritten signature. At the same time, the Bank will not execute the Client's order given through the Mobile Application until it receives the order in hard copy;
8.1.11. suspend the operation of the software and/or hardware of the Mobile Application for the purpose of carrying out preventive and technical work and eliminating faults, errors and failures;

for Official Use Only

8.1.12. modify the interfaces and software of the Mobile Application, as well as carry out the actions specified in paragraph 3.5. of the Agreement;
8.1.13. for security purposes, block access to the Mobile Application system if more than 6 (six) calendar months have passed since the last use of the Mobile Application. The Client's access to the Mobile Application system will be restored in accordance with the procedure established by the Bank;
8.1.14. block and/or close (deactivate) the Client's e-wallet regardless of the balance of funds in the e-wallet in the event that:
- no incoming and/or outgoing transactions have been made through the e-wallet for 12 (twelve) calendar months, and there are no active banking products; the mobile phone number used to register the e-wallet has been deactivated or cancelled in the mobile operator's system;
– more than one e-wallet is registered in the Bank in the Client's name.
In the event of deactivation of the Client's e-wallet, the remaining electronic money is transferred to a special account of the Bank and can be requested by the Client upon written request.
8.1.15. other rights provided for by the legislation of the Kyrgyz Republic, the Agreement.

8.2. **The Bank undertakes to:**
8.2.1. provide remote banking services to the Client in the manner prescribed by the Agreement;
8.2.2. carry out the Client's orders to conduct transactions, accept and credit funds received on the Client's account/card/e-wallet;
8.2.3. ensure access to the text of the Agreement, the List of Services, tariffs and limits (restrictions) by posting them on information boards in the Bank's branches, on the Bank's Website and/or in the Mobile Application;
8.2.4. keep bank secrecy regarding transactions carried out on the Client's accounts/cards/e-wallets and provide information on them only in cases stipulated by the legislation of the Kyrgyz Republic;
8.2.5. immediately block the Client's account/card/e-wallet upon written request from the Client or upon phone request in accordance with the procedure established by the Bank;
8.2.6. take measures to eliminate possible technical problems within a reasonable time; promptly notify Clients when carrying out preventive and technical work.

9. LIABILITY OF THE PARTIES

9.1. The Parties shall be liable for failure to perform or improper performance of the terms of the Agreement.
9.2. The Parties shall be exempt from liability for the duration of a force majeure event. The Party citing force majeure must notify the other Party in writing no later than 10 (ten) business days from the date of occurrence of such circumstances, with the provision of a supporting document issued by a competent government agency.
9.3. The Client shall be liable:
– for failure to implement or improper implementation by the Client of security and confidentiality measures for access to the Mobile Application system (mobile device, phone number, Codes) and other measures provided for in the Security Requirements for Remote Banking (Annex 1 to the Agreement);
– for failure to comply with the rules for the use of payment instruments and the procedure

for Official Use Only

for processing payment documents in accordance with the legislation of the Kyrgyz Republic;
– for all transactions carried out during the period from the moment of loss/theft by a third party of the mobile device on which the Mobile Application was installed, phone number (SIM card), Codes, payment card, until the moment the Bank blocks access to the Mobile Application/payment card system, as well as for all losses caused as a result.
– for carrying out actions/transactions aimed at financing terrorist or extremist activities and legalization (laundering) of criminal proceeds or in the interests of third parties for the purpose of committing illegal/fraudulent actions, as well as for selling/transferring to third parties an account/card/e-wallet, access to the Mobile Application, as well as details, PIN/Codes, logins and passwords to them.

9.4. The Bank shall not be liable:

– for failure to execute or untimely execution of the Client's orders, if the Client has provided incomplete or erroneous details, or if this failure to execute occurred due to the fault of a correspondent bank or other third party, or if the Client's account/card/e-wallet has been frozen or transactions have been suspended/blocked in accordance with the Agreement, the legislation of the Kyrgyz Republic or the recipient's country;
– for the consequences of the Client providing false personal data, a mobile phone number of which he/she is not the owner (subscriber);
– for the consequences of an unauthorized person receiving information, if this information was sent by the Bank to the phone number/address specified by the Client in the application form, the Mobile Application system or other automated systems of the Bank;
– for the consequences of third party access to the Client's phone number (SIM card), mobile device and/or Codes.
– for malfunction and/or insecurity of the Client's equipment, software, communication channels, for means and services provided by a third party (Internet access provider, etc.);
– for failures in the operation of mobile communications, the Internet information and telecommunications network, electrical communication networks that arose for reasons beyond the control of the Bank and resulted in the untimely receipt or non-receipt by the Client of an SMS message with the Code, as well as their untimely entry or non-entry by the Client.

10. OTHER TERMS AND CONDITIONS

10.1. The location of the Bank/relevant subdivision of the Bank shall be considered the place of conclusion of the Agreement.
10.2. The Client's requests shall be considered in the manner and within the timeframes stipulated by the legislation of the Kyrgyz Republic, local regulations of the Bank (the Procedure for considering requests from consumers of financial services in Kompanion Bank CJSC), the Agreement and/or the rules for handling claims established by the relevant payment systems (in terms of payment cards).
10.3. If it is impossible to resolve disputes through negotiations, they shall be resolved in accordance with the legislation of the Kyrgyz Republic. The Parties, guided by Article 34 of the Civil Procedure Code of the Kyrgyz Republic (CPC KR), have agreed to change the jurisdiction established by Article 30 of the CPC KR, in connection with which the Bank has the right to file claims at the location of the Bank or its branches, or at the location of the defendant, except for claims whose jurisdiction is established by Article 32 of the CPC KR. The Client has the right to file claims against the Bank only at the location of the Bank.

for Official Use Only

10.4. Conditions not stipulated in the Agreement shall be regulated in accordance with the legislation of the Kyrgyz Republic and business practices.

11. BANK DETAILS

Bank Kompanion CJSC
Address: 62 Shota Rustaveli Street, Bishkek 720044, Kyrgyz Republic
BIC: 113001
OKPO: 23672096
TIN: 01210200410119
Customer service phone numbers – 0 312 338800, 8800

for Official Use Only

Annex 1
to the Remote Banking Service Agreement

SECURITY REQUIREMENTS FOR REMOTE BANKING SERVICES

Clients must adhere to the following rules to ensure safety when using the Mobile Application:

1. Do not store Codes, card details or passwords on a mobile device (including screenshots with codes) or unprotected media, or in other accessible places in plain text;

2. Use special software to store the Codes, for example, KeePassXC Password Manager;

3. Do not communicate, disclose or otherwise transfer to third parties the Codes and data for logging into the Mobile Application or Internet Banking (login, password);

4. Do not follow links received through chats or received by e-mail. Periodically change the PIN code, password, do not use a simple or obvious combination of symbols and signs, such as name or date of birth, numbers from a phone number, etc;

5. Do not disclose personal and banking information (passport data, TIN/PIN, bank account number or email address, e-wallet number, card details: card number, CVV code, card expiration date, PIN code, password and one-time verification codes (OTP), etc.) to third parties without the need to complete a transaction and clarify, including via instant messengers or telephone conversations;

6. Regularly check the transaction history and balance on your accounts/card/e-wallet to track errors or unauthorized transactions through the Mobile Application, and do not disclose information about your transactions, accounts, or balance to anyone;

7. Do not use third-party mobile devices to log in to the Mobile Application, do not send them screenshots of the Mobile Application, SMS with confirmation codes, or your biometric data (selfies, videos, passport photos);

8. Protect your access device (mobile device) from unauthorized access and malware, while ensuring that your antivirus software and Mobile Application are regularly updated to the latest version and are running at all times. Never install applications from third-party sources (only from the App Store/Play Market);

9. It is necessary to log out of the Mobile Application after performing electronic transactions, even if the access device is left unattended for a short period of time;

10. Do not allow other persons to use your mobile device on which the Mobile Application is installed, do not provide access to the device through remote applications (TeamViewer, AnyDesk, etc.);

11. Immediately inform the Bank by any available means (in writing or by phone 0312338800 or 8800) of any cases of unauthorized use of the account/card/e-wallet, unauthorized and/or fraudulent transactions by third parties, in the event of loss or theft of the mobile device on which the Mobile Application was used, for timely blocking of the account/card/e-wallet.

12. Do not carry out other people's requests to transfer money to an account/card/e-wallet. If you decide to do so, save the contact information of those who contacted you and screenshots of the correspondence. Copies of the correspondence may serve as evidence for law enforcement agencies.

Risks that Clients may be exposed to when using the Mobile Application:

for Official Use Only

– **Risk of loss/theft/disclosure of personal data** - may lead to the use of the Client's personal data by attackers for their own purposes (for example, they may extort money if the data is sensitive or present a copy of the Client's passport to organizations).

– **Risk of theft of money from an account/card/wallet** if access is gained.

13. Never transfer or sell the Bank's products and services, as the use of banking products is permitted exclusively by the Client.

14. If such cases are identified:

- the Bank has the right to block access to applications and products;
- data may be transferred to law enforcement agencies;
- the Client's actions may be qualified as a violation of the legislation of the Kyrgyz Republic.

15. Beware of social engineering. Social engineering is a deception in which you are forced to reveal your information or perform actions under pressure.

Fraudsters can:

- say that "you received a loan" and ask to return the "mistakenly issued amount";
- report a "hack" and ask to install a "security program" - in fact, this is a spy program;
- introduce themselves as bank employees and request information.

Remember: bank employees never ask for a PIN code, password, OTP, passport photo, selfie, or never ask to transfer money.

Beware: fraud under the guise of the National Bank of the Kyrgyz Republic

There have been more and more cases where attackers:

- introduce themselves as employees of the National Bank, a bank or the police;
- claim that your money is supposedly "in danger";
- ask to transfer funds to a "safe account";

This is a fraud. No bank or the National Bank of the Kyrgyz Republic makes such calls.

16. The Bank shall not be liable if:

- the Client himself/herself provided his/her data (password, PIN code, card details, account details) to third parties;
- the Client withdrew or transferred the funds himself/herself on the instructions of outsiders;
- the Client clicked on suspicious links;
- the Client has installed malicious software on his/her own;
- the Client has transferred the device to another person without blocking it;
- the Client used unsecured Wi-Fi networks;

for Official Use Only

- the Client has carried out transactions on behalf of unknown persons, despite warnings from the Bank;
- the Client has provided photos or videos of documents or face to third parties.

for Official Use Only

Annex 2
to the Remote Banking Service Agreement

Consent of the Personal Data Owner to the Collection and Processing of Personal Data

The Client freely, consciously, and voluntarily gives consent to the Bank:

–for processing (any operation or set of operations performed, regardless of the methods, by the holder (owner) of personal data or on his/her instructions, by automatic means or without them, for the purpose of collecting, recording, storing, updating, grouping, blocking, erasing and destroying personal data), as well as:

–for transfer of personal data (provision by the holder (owner) of personal data to third parties in accordance with the Digital Code of the Kyrgyz Republic and international treaties);

–for cross-border transfer of personal data (transfer by the holder (owner) of personal data to holders under the jurisdiction of other states)

of the following personal data:

national passport type, PIN, passport series and number, full name, date of birth, name of the issuing authority and its code, date of issue, expiration date, gender, digital image of the face, address of the place of residence (registration), marital status, credit repayment discipline, phone number, terms of use of mobile communication services, monthly amount of expenses for mobile communication services, types of terminal equipment used for mobile communications, geolocation, identifiers of software, end product, data subject and environment, data on the use of the call functionality and authentication on the device by fingerprint, data on installed applications (package names, paths, permissions, certificates, sources, used libraries, date and time of installation, reputation) and files (name, hash, size, path), active network connections, device roaming, data on network connections, data on device properties and other data in accordance with the legislation on electrical communication, etc.

The above personal data is provided for processing for the purpose of providing the Client with state (municipal) services, banking and payment services, in order to comply with the requirements of the legislation of the Kyrgyz Republic in the field of combating the financing of terrorist activities and the legalization (laundering) of criminal proceeds, as well as for any other purposes.

The Client is aware that:

1) Consent to the processing of personal data is valid from the date of signing the Agreement (Acceptance of this Offer) for the entire period of provision of state (municipal) services, banking and payment services and storage of data on the service provided in accordance with the legislation of the Kyrgyz Republic;

2) Consent to the processing of personal data may be revoked on the basis of a written statement in any form;

3) In the event of withdrawal of consent to the processing of personal data, the processing of his/her personal data in whole or in part may be continued in accordance with the Digital Code of the Kyrgyz Republic.

The date of commencement of processing of personal data shall be the date of signing the Agreement (Acceptance of this Offer).

for Official Use Only

Annex 3
to the Remote Banking Service Agreement

Kompanion Bank CJSC

From the Client

APPLICATION FOR CLOSING
OF BANK ACCOUNT(S), E-WALLET

I kindly ask you to close my demand account/s (deposit) or e-wallet specified by me in the Mobile Application and, if there are any remaining funds, transfer them to any other demand account or e-wallet opened with your Bank.

Client's full name /_____/

Date:

for Official Use Only

Annex 4

to the Remote Banking Service Agreement

Guide to Using the Kompanion Mobile Application

1. Registration in the application

Logging into the application for the first time and creating an account.

To start using the Kompanion application, follow these steps:

1. Make sure you have a SIM card from one of the mobile operators in the Kyrgyz Republic. Registration in the mobile application is only possible with a number belonging to a Kyrgyz mobile operator.
2. Download the Kompanion application from the **Play Market (Android)** or **App Store (iOS)**.
3. Enter your phone number and confirm it with a one-time verification code (OTP) received via SMS.
4. Set a 4-digit PIN and confirm it again.
5. Scan your Kyrgyz Republic citizen's passport (front and back sides).
6. Check the automatically recognized data (passport and TIN).
7. Go through a video identification **to confirm your identity using biometric data** - turn on the camera and follow the instructions.

Security:

During registration, **a PIN code and video identification** are used **to verify your identity using biometric data**—these are basic security measures.

- **A password is not required at the registration stage**, but you can set it **yourself later** for additional login protection:
  Menu → Security → Set Password.
- Optionally, you can enable **biometric authentication** (Face ID or fingerprint)—recommended.

Status after registration

After registering remotely outside the Bank's office, you are assigned the status of **a remotely identified user** with the limits set in the List of Services.

- The Bank uses an anti-fraud system that analyzes transactions made in the application, including transfers, payments, and cash withdrawals. If suspicious indicators are detected, transactions may be temporarily blocked until additional identification is completed or clarification is received from the client.
- To gain full access to all banking products and extended limits, the mobile application user must undergo full identification at a bank branch. After this, the limits increase and become as follows:

2. Re-login to the application

If you logged out of the Kompanion application yourself or at the Bank's initiative, changed/lost your phone, reinstalled the application, or updated the system.

1. Enter the phone number you used to register.

for Official Use Only

2. If available, enter the password you set.
3. **A one-time verification code (OTP)** will be sent to the specified number.
4. When logging in from a new device, the system automatically initiates **video identification to confirm your identity using biometric data**.
5. After successful verification of the user's identity, the device is added to the trusted list.
6. Enter the previously set PIN code and you are back in the application.

3. Reset password

If you set a password as additional security but forgot it.

1. Click "Forgot your password?" on the login screen.
2. Follow the instructions and go through a **video identification to confirm your identity using biometric data**.
3. Set a new password (6-18 characters, preferably with letters, numbers, and special characters).
4. Confirm the new password.
5. Enter the **one-time verification code (OTP)** received via SMS.
6. Set a new PIN code.
7. If desired, enable biometrics (Face ID / Touch ID).

4. Reset PIN code

If you forgot your PIN and can't log in to the application.

1. Click "Forgot your PIN?".
2. Go through a **video identification to confirm your identity using biometric data**.
3. Receive a temporary PIN code via SMS.
4. Enter the temporary code and set a new PIN code.
5. (Optional) Enable biometrics.

For additional security, you can set a password at any time:
Menu → Security → Set Password.

5. PIN code change

If you want to change your current PIN code to a new one.

1. Go to **Menu → Security → Change PIN code**.
2. Enter your current PIN.
3. Enter and confirm the new PIN code.

6. Blocking and unblocking an application

If you temporarily do not plan to use the application and want to block access to it.

Blocking:

- Go to **Menu → Security → Block Wallet**.
- The application will log you out of your account.
- A blocking notification will appear the next time you log in.

Unblocking:

- Click “Unblock”.
- Enter the **one-time verification code (OTP)**.
- Scan your passport.
- Go through a **video identification to confirm your identity using biometric data** - access will be restored.

for Official Use Only

The anti-fraud system may also temporarily restrict access to the application or transactions automatically if abnormal activity consistent with fraudulent scenarios is detected. In such cases, the client will be notified via an intuitive banner.

7. Change password

If you have set a password and want to change it.

1. Go to **Menu** → **Security** → **Change Password**.
2. Enter your current password.
3. Set and confirm a new password.
4. Click Save».

8. Remove password

If you decide to use only a PIN code and/or biometrics.

1. Go to **Menu** → **Security** → **Remove Password**.
2. Enter your current password.
3. Confirm the action and accept the warning.
4. After removal, login will be possible via PIN code and/or biometrics.

9. Set password

If you want to add additional security when logging in.

1. Go to **Menu** → **Security** → **Set Password**.
2. Enter a new password (6-18 characters).
3. Confirm and click Save.

10. Access control: log out from all devices

If you suspect unauthorized access or want to terminate all active sessions.

1. Go to **Menu** → **Security** → **Devices**.
2. View a list of all devices from which you have logged into your account.
3. If necessary, click **"Log out from all devices"**.
4. All sessions, including the current one, will be terminated. You will need to log in again.

This is your security monitoring tool—use it if you have any doubts.

If you suspect fraudulent access, we recommend using this feature immediately. However, please note that the Bank may also automatically log out sessions and require re-identification if it detects signs of account compromise.

11. Biometrics management

If you want to enable or disable Face ID / Touch ID.

1. Go to **Menu** → **Security** → **Biometrics**.
2. Enable or disable biometrics.
3. Biometrics only works if it is pre-configured on your device.

for Official Use Only