APPROVED

by the decision of the Management Board of «Kompanion Bank» CJSC

dated "25" May 2023

ACTIFIED

from "09" June 2023

PROVISION OF REMOTE BANKING SERVICES FOR INDIVIDUALS AND LEGAL ENTITIES (PUBLIC OFFER)

This offer, published on the Kompanion Bank (hereinafter referred to as the Bank) web-site https://www.kompanion.kg, is an offer of the Bank for conclusion of an Agreement on Remote Banking services provision.

This Offer is addressed to individuals and legal entities and is an official public offer of the Bank for conclusion of an Agreement on Provision of Remote Banking services (hereinafter referred to as the Agreement, conditions of the Agreement are stipulated in this Offer) in accordance with the civil legislation of the Kyrgyz Republic.

The Agreement on Provision of Remote Banking Service is deemed to be concluded and becomes effective from the moment of signing by individual or legal entity of the Application in a prescribed form, which means the unconditional acceptance of all the conditions of the Offers by individual or legal entity without any waivers or restrictions on the connection conditions.

1. TERMS AND DEFINITIONS

Internet Banking – Client's remote control of bank account/accounts opened in the Bank under the Bank Account General Agreement. Use of the Internet Banking system is carried out through generally available Internet channels using a personal computer or laptop and client's other devices. Access to the Remote Banking system can be implemented at http://www.kompanion.kg/.

Mobile Banking – Client's remote control of bank account/accounts opened in the Bank under the Bank Account General Agreement. Use of the Mobile Banking system is carried out through messages and commands sent by the Client to the Bank from mobile phone and/or tablet and other devise using mobile application.

OTP-TOKEN (hereinafter – otp-token) – is a special device, which generates one-time access passwords (one-time password-OTP) in to the Internet Banking system at each subsequent visit, and also ensures identification and authentication of the Client.

Electronic Payment Document (hereinafter - EPD) – is a remote order and/or corresponding application of the Client about performance of a banking operation within a bank account opened in the Bank, and/or performing another operation within the Bank's services, sent to the Bank electronically, generated and confirmed by the corresponding identification data using the Client's electronic signature.

Electronic signature – is an information in electronic form, which is attached to EPD

and (or) logically connected to it and which is used for identification of an individual, on behalf of which the EPD was signed. The EPD signed with the Client's electronic signature is considered to be an electronic document, which is equivalent to the physical document signed with the Client's handwritten signature.

2. SUBJECT OF THE AGREEMENT

2.1. The Bank provides the Client, who has an access to the Internet and/or corresponding necessary technical equipment, with services for performance of banking operations against the Client's account/accounts through the Internet Banking system, Mobile Banking system (hereinafter referred to as the remote banking system) under the conditions stipulated by the Account General Agreement, on the basis of which was opened account/accounts and/or for depositing and/or crediting of the Client in the manner and on the conditions stipulated by the legislation of the Kyrgyz Republic and/or provision of another bank services, stipulated by conditions of the relevant agreements concluded with use of the Client's electronic signature.
2.2. The Client pays for provided services in accordance with the Bank's tariffs applicable at the moment of operation under the conditions stipulated by this Agreement.

3. PROCEDURE AND CONDITIONS OF CLIENT SERVICES

3.1. In the framework of this Agreement the Client can receive services in accordance with the Bank's tariffs indicated on the http://www.kompanion.kg website and/or in the corresponding mobile application of the Bank.
This list of services is not exhaustive and can be changed and/or updated by the Bank unilaterally by posting the relevant information on the http://www.kompanion.kg website.
3.2. Connection of the Client to the Internet Banking system is carried out on the basis of a written application for connecting to the Internet Banking system in the Bank's form, in which should be indicated the Client's account/accounts, connected to the service through the Internet Banking system, a list of the Client's responsible employees with classification in roles (executor, verifier, controller and authorizer) documents confirming the powers of these persons, and documents certifying their identities and other information at the discretion of the Bank.
3.3. Service in remote banking systems is provided to the Client remotely through the Internet using a personal computer, tablet, mobile phone and Client's other devices.
3.4. The Client obtains the right to be serviced in remote banking systems after the conclusion of this Agreement, receive at the Bank identification data for access to remote banking systems and familiarization with the Guidelines for use of the remote banking (Internet Banking, Mobile Banking), which are found in Annex No. 1 and are integral part of this Agreement.
3.5. The Parties acknowledge that the identification data for access to remote banking systems is analogous to the electronic signature of the Client, which is regulated by the legislation of the Kyrgyz Republic (hereinafter referred to as the Kyrgyz Republic). The Parties to this Agreement also acknowledge that the identification data for access to the remote banking systems is considered to be equivalent to the handwritten signature of the Client/authorized persons, indicated in the signature card and the impression of the Client's seal.
3.6. Safety protection supplementary tools include receipt of one-time passwords to phone numbers provided by the client or using fingerprints/face id through SMS sending/push

notifications and other authentication methods. Logging into remote banking systems without a one-time password is impossible, except for cases of using the corresponding mobile equipment, using the Client's phone number provided to the Bank or the client's biometric data. Client's phone number is indicated in the application for connection to the remote banking systems services.

3.7. It is necessary to purchase otp-token if an application for connection to the Internet Banking system includes the possibility of making money transfers and/or conversion operations for legal entities/individual entrepreneurs.

3.8. The Client's responsible employee with the role of Authorizer should receive the otp-token, to confirm all performed operations, according to the act of delivery and acceptance.

3.9. From the moment of sending of the otp-token to the Client's responsible employee, any EPD, confirmed by the relevant OTP and obtained through the Internet Banking/Mobile Banking system, considered to be directed by the Client in a proper manner and shall be performed by the Bank in accordance with conditions of this Agreement.

3.10. The Parties acknowledge that the Client's EPD on performance of operation through the remote banking systems are equivalent to the orders received from the Client on paper drawn up in accordance with the legislation of the Kyrgyz Republic.

3.11. Orders or applications of the Client about the performance of operations in the remote banking systems are sent electronically in the form of EPD, confirmed by the Client in the system.

3.12. The EPDs are executed by the Bank on banking days in accordance with the List of services and the services schedule in the remote banking systems published on the Bank's website. EPDs received after the set time will be executed on the next banking day.

3.13. Payment in a cashless form becomes irrevocable for the Client when he/she receives a confirmation of acceptance of the payment document for execution by the Bank and becomes final at the moment of writing off of amounts from the Client's account/accounts.

3.14. The bonk stops/terminates the access to the remote banking systems in the following cases:

3.14.1. closing of account/accounts, connected to the services through the remote banking systems;

3.14.2. making 3 (three) consecutive failed attempts to enter identification data (user name, password);

3.14.3. non-payment for the Bank's services;

3.14.4. occurrence of technical malfunctions during work with the remote banking systems;

3.14.5. changing of software and carrying out of scheduled maintenance;

3.14.6. occurrence of disputable situation connected with use of this Agreement;

3.14.7. In other cases stipulated by the legislation of the KR.

3.15. During the period of elimination of technical malfunctions, the Client must provide payment document drawn up on paper signed by the Client to the Bank for performance of banking operations. The procedure for submission/receipt of complaints and claims of the Client, conditions for their consideration and decision, are determined in accordance with the legislation of the Kyrgyz Republic.

3.16. Phone number for the Clients services: 0312 33 88 00, 8800.

3.17. All payments made through the remote service are considered to be confirmed and final (unconditional and irrevocable) from the moment of completion of settlements in the relevant

system of the service provider and performance of final settlements.

4. RIGHTS AND LIABILITIES OF THE PARTIES

4.1. The Bank undertakes to:

4.1.1. register the Client in the remote banking systems, according to the Client's application in the Bank's form after the payment of appropriate fees by the Client, in accordance with the Bank's tariffs;
4.1.2. service the Client in the remote banking systems in accordance with procedure provided in this Agreement;
4.1.3. keep bank secrecy about operations performed against the Client's accounts, and provide information on them only in cases provided for by the legislation of the Kyrgyz Republic;
4.1.4. immediately block the Client's account upon a written request from the Client or by telephone call after appropriate verification of the client (code word and/or passport details, etc.);
4.1.5. take measures for elimination of the possible technical malfunctions within reasonable time frame.

4.2. The Bank has a right to:

4.2.1. make non-acceptance writing-off (without the Client's consent) of the Bank's commissions/fees for services provided at the moment of transaction in the remote banking systems from any Client's accounts opened in the Bank, as well as writing-off of incorrectly credited amounts, if the fact of incorrect crediting to the Client's account/accounts was established, writing-off of amounts of any debts of the Client to the Bank, and in other cases stipulated by the legislation of the Kyrgyz Republic;
4.2.2. deny the Client to perform an operation in the remote banking systems if the Client incompletely/incorrectly indicated the details of operation to be performed, violates the deadlines for its performance, if the operation to be performed does not comply with the legislation of the Kyrgyz Republic, including requirements of the legislation of the Kyrgyz Republic for anti-money laundering and counter-terrorism and extremism financing, if funds on the Client's account/accounts for performance of an operation and/or for payment of remuneration of the Bank for the transaction to be performed are insufficient, as well as in cases stipulated by the legislation of the Kyrgyz Republic;
4.2.3. request from the Client for drawing up a physical document with the Client's signature for conduction of the operation, if necessary. At the same time, the Bank will not execute the electronic document until the receipt of the physical document;
4.2.4. to suspend/block the remote banking systems or all or separate operations on the account(s) in the following cases:
- in cases stipulated by the legislation of the Kyrgyz Republic and this Agreement, including in case of non-compliance with the requirements of this Agreement;
- in the case of execution or any suspicion of fraudulent or criminal transactions;
- in case more than 3 (three) months have passed since the Customer's last contact with the Bank via remote banking systems. In such case, the Client's access to the Remote Banking

Systems shall be resumed upon the Client's written application;
4.2.5. set/change limits on operations in the internet banking systems;
4.2.6. to request from the Client for provision document to confirm the legality and economic viability of the operation, in cases stipulated by the current legislation of the KR;
4.2.7. deny unilaterally to perform operation against the account in cases stipulated by the current legislation of the KR;
4.2.8. unilaterally change the conditions of this Agreement, while methods of notification the Client are as follows: a message in the remote banking systems or sending a written notice. If the Bank made amendments into the conditions of the offer, the changes come into force from the moment of publishing of the amended conditions of the offer on the https://www.kompanion.kg website, unless other term is specified by the Bank in the publication;
4.2.9. terminate this Agreement unilaterally in cases stipulated by the legislation of the KR.

4.3. The Client undertakes to:

4.3.1. ensure availability of software and hardware which provide access to the Internet;
4.3.2. observe and follow the Guidelines for use of the remote banking (Internet Banking, Mobile Banking) for the Client when working in remote banking systems set in Annex No. 1;
4.3.3. check the fact of receipt and execution by the Bank of transferred EPD after they were sent. If the fact of receipt and/or execution was not confirmed, the Client should contact the Bank give a request to find out the reason why this EPD was not received and/or executed by the Bank;
4.3.4. when exchanging EPDs, use information processing, storage and protection systems only on working PC that has been checked for computer viruses;
4.3.5. ensure confidentiality when using identification data (username, password);
4.3.6. immediately notify the Bank about detection of unauthorized access or unauthorized access attempts, and about cases of loss, theft of the Client's identification data, change/loss of number;
4.3.7. not to use the services provided by the Bank for illegal purposes, also not to perform actions/operations aimed at money laundering and terrorism or extremism financing;
4.3.8. provide documents confirming the legality and economic viability of operation/operations within 3 (three) banking days upon the Bank's request in accordance with the requirements of the legislation of the Kyrgyz Republic.

4.4. The Client has a right to:

4.4.1. use services in the manner and on the conditions stipulated by this Agreement;
4.4.2. apply to the Bank with request to block the Client's identification data (username, password) if unauthorized access or attempts of unauthorized access to the remote banking systems were detected;
4.4.3. receive from the Bank a paper confirmation (certified copies) of execution of payment orders against banking operations made through the remote banking systems and account/account statements for the required period, if necessary;
4.4.4. for on-site consultation of the Bank's specialist regarding rules for operation of the

remote banking systems upon the Client's request, a fee is charged in the amount established by the Bank's tariffs. The request is made through sending of an application by the Client, drawn up in writing and sent by e-mail, mail, fax or in person;

4.4.5. set daily limits and limits for one operation within the general limits set by the Bank on the basis of an application;

4.4.6. change the identification data (username, password).

5. PROCEDURE OF PAYMENT FOR SERVICES

5.1. The Client undertakes to pay for the Bank's services, in accordance with the Bank's current tariffs, unless otherwise provided by an additional agreement to this Agreement. Tariffs are placed on information boards in the customer floors and on the Bank's website.

5.2. The Bank can change the tariffs unilaterally. Change tariffs are brought to the notice of the Client not later than 30 (thirty) calendar days prior to their coming into effect through placing them on information boards in the customer floors and on the Bank's website or through informational notice in the remote banking systems.

5.3. Payment for the Bank's services under this Agreement is made through non-acceptance writing-off of amounts from any account/accounts of the Client. The Bank has the right to use funds on any of the Client's accounts with their conversion at the Bank's rate of purchase of the relevant currency, to pay for conduction of the Client's operations.

6. LIABILITIES OF THE PARTIES

6.1. The client is liable for the safety and confidentiality of means of access to the remote banking systems (username, password, OTP-token), for losses resulted from unauthorized use of access means, and for non-performance/improper performance of the conditions of this Agreement.

6.2. The Client is responsible for compliance with the rules for use of payment instruments and the procedure for drawing up of payment documents in accordance with the legislation of the Kyrgyz Republic.

6.3. The Client bears the risk and liability for the non-performance or improper performance of the established security and confidentiality measures, as well as the Guidelines for use of the remote banking (Internet banking, Mobile banking) (Annex No. 1).

6.3.1. The Client is liable for all operations performed from the moment of loss of phone number and/or identification data (user name, password), until the moment of Client's application to the Bank in order to block access to the remote banking systems.

6.4. The Parties are exempted from liability for the period of force majeure. The party referring to force majeure is obliged to notify the other Party in writing no later than 10 (ten) banking days from the date of occurrence of force majeure, with provision of supporting document issued by the competent state authority.

6.5. The Bank is not liable for:

6.5.1. malfunction and/or safety of: equipment, software of the Client, communications in communication channels, for funds and services provided by a third party (Internet provider, etc.);

6.5.2. non-performance or improper performance by the Client of the established security and confidentiality measures, and the Guidelines for use of the remote banking (Internet banking,

Mobile banking) (Annex No. 1);

6.5.3. non-execution of the Client's orders the remote banking systems, if the Client's account was arrested or operations were suspended by the Client in the manner prescribed by this Agreement, by the Account General Agreement and/or in accordance with the legislation of the Kyrgyz Republic;

6.5.4. receipt of information by an unauthorized person, if this information was sent by the Bank to the email address indicated by the Client in the application, and for changing of email address by the Client without notification of the Bank;

6.6. Regarding other aspects, not stipulated by this Agreement, the Parties bear responsibility in accordance with the Account General Agreement and the legislation of the KR.

7. VALIDITY OF THE AGREEMENT

7.1. This Agreement is valid until it is terminated through the Client's written request to the Bank, or until the date of termination of the Bank Account General Agreement.

7.2. The Parties are entitled to terminate this Agreement unilaterally be means of notification of the other Party in writing at least 10 (ten) banking days prior to the date of its termination, with obligatory execution of all liabilities and mutual settlements under this Agreement.

8. PROCEDURE FOR SETTLEMENT OF DISPUTES

8.1. Any disputes which arose from this Agreement shall be settled through negotiations.

8.2. If it is impossible to solve the disputes through negotiation, the disputes should be solved in accordance with the legislation of the Kyrgyz Republic.

9. OTHER CONDITIONS

9.1. The Parties acknowledge that any notifications, correspondence and etc., are considered to be delivered, if they were at the addresses specified in this Agreement. In case of change – at the address specified in the written notification.

9.2. The Parties acknowledge that the remote banking systems used by them under this Agreement are sufficient for insurance of secure and effective processing, storage, receipt, and transfer of information.

9.3. The Parties acknowledge that the used technology is sufficient for protection from unauthorized access and for confirmation of the EPD authenticity.

9.4. The Parties acknowledge that if the identification data or access devices were lost, stolen, or transferred to the third parties, the Client bears all responsibility for unauthorized access to the system.

Regarding other aspects, not stipulated by this Agreement, the Parties shall be guided by the Account General Agreement and the legislation of the KR.

10. BANK'S DETAILS

Kompanion Bank CJSC
Address: 720044, Kyrgyz Republic
Bishkek city, Shota Rustaveli str., 62

BIC: 113001
All-Kyrgyz Classification of Enterprises and Organizations code: 23672096
TIN: 01210200410119

Annex No. 1 To the Agreement on provision of remote banking services (Internet Banking) for individuals and legal entities – public offer

GUIDELINES FOR USE OF THE REMOTE BANKING (INTERNET BANKING, MOBILE BANKING) for individuals and legal entities

1. Requirements for work:

1.1. to ensure the confidentiality mode regarding the Client's workplace location where he works in the remote banking systems, OTP tools and security certificates of the Client, logins, passwords to the Client's operating system at his workplace;

1.2. to correctly finish work by using the "Exit" software button after finishing work in remote banking systems;

1.3. to disable the function of autorun of removable media in the operating system of the Client's workplace used for work in the remote banking systems;

1.4. to connect the Client's workplace to the Internet for work in the remote banking systems only while working with the remote banking systems;

1.5. before entering the personal account, make sure that the secure connection with use of the https protocol is established with the Bank's official website (https://kompanion.kg);

1.6. to ensure that users of the system have a password-protected account in the operating at their workplace;

1.7. not to save the password in text files on a computer or on other media;

1.8. never, under no event, not to disclose the password to anyone - Bank employees and technical support service don't require it for your connection, maintenance and keeping the service in working order;

1.9. not to use the Client's workplace for connection to social networks in the Internet, to forums, conferences, chat rooms, telephone services and other websites containing potential malicious programs, also reading mail and opening mail documents from unreliable senders;

1.10. not to disclose logins and passwords to third parties, including Bank employees (in particular when unidentified individuals contact the Client on behalf of the Bank by phone, email, via SMS);

1.11. not to save logins and passwords in text files on the hard disk of the Client's workplace, or other electronic data storage.

2.Recommendations for work:

2.1. to use the Client's separate workplace for work with the remote banking system, which is not used by the Client for other purposes;

2.2. to ensure operation of licensed (non-counterfeit) operating system Microsoft Windows XP/2003/Vista/7, Apple Macintosh Mac OS X or older, Linux, Android, iOS, and its timely update in accordance with recommendations of the development company in order to eliminate the identified vulnerabilities which allow access to confidential information;

2.3. to ensure functioning of licensed (non-counterfeit) anti-virus software at the Client's workplace and its timely update as recommended by the development company in

order to prevent the Client's workplace from being infected with malicious software that can allow access to the Client's remote banking systems by unauthorized third parties;

2.4. to ensure the functioning of licensed (non-counterfeit) firewall software at the Client's workplace in the mode of blocking of unauthorized remote access to the workplace from the Internet and the Client's local network;

2.5. to restrict access to the Client's workplace/where the OTP will be used at the Client's workplace and provide minimum rights to change the configuration of operating system of the Client's workplace (administrator rights are not advisable);

2.6. not to work in remote banking systems in the Internet using unreliable connection source (an Internet cafe), or using public communication channels (free Wi-Fi, etc.);

2.7. to pay attention to any changes and software errors in the Bank's remote banking systems work or during connection to the remote banking systems, if there are any doubts concerning the correctness of the remote banking operation, immediately stop working and contact the Bank to establish the non-existence/existence of unauthorized operations;

2.8. to visit https://www.online.kompanion.kg / only at the Bank's official link (www.kompanion.kg);

2.9. to download the mobile application only from PlayMarket or AppStore;

2.10. to postpone transactions if browser warnings about redirecting to another site appeared during connection to the remote banking systems, and contact the Bank's technical support service in order to determine the reason of redirection.

2.11. to notify the Bank's authorized employees about any attempts to obtain the remote banking systems password;

2.12. to regularly check the history of operations and statements for tracing through errors or unauthorized operations against the account;

2.13. to leave the website where electronic operations are performed, even if the personal computer and/or any other equipment is left unattended for a short period of time;

2.14. to log out after performing of electronic operations; before performing any online operations or providing personal information, make sure that the correct web page or the remote banking systems application is used. Avoid fake web pages, mobile applications created for fraud;

2.15. to make sure that the web page is secure before logging in, by checking for Unified Resource Pointers (URLs) existence, which should begin with "https", and a secure connection sign should appear in the status of the Internet browser;

2.16. Non-execution of the above requirements and recommendations by the Client will be the basis for laying the responsibility for the disputed operations performed through the remote banking systems on the Client.