OptimaBank

Appendix 2
to the Agreement for a Full Package of Banking Services
for Individuals at Optima Bank OJSC

DIRECTIONS FOR USING BANK CARDS OF OPTIMA BANK OJSC

CONTENTS

Glossary

1. **Authorization** – the procedure of confirmation by the issuer of the authority or authorship of the cardholder to an operation using a bank payment card (transaction), as a result of which the issuer shall bear an obligation to the acquirer to execute a payment document drawn up using the card of the above-mentioned issuer. Authorization can be automated (via a terminal) and voice (via telephone communication). If the issuer and acquirer are the same person for the operation carried out using a bank payment card, then authorization is a permission granted by the issuer to a customer for this operation.
2. **A Bank Payment Card (hereinafter referred to as the Card)** – a payment instrument used to make payments when purchasing goods, services, receiving cash in national and foreign currencies, making money transfers, as well as for payments in the form of electronic money through terminals, ATMs or other devices (peripheral devices). A card issued under a card account in the name of the card account owner is the primary card, and cards issued under a card account for third parties are additional cards. If the primary card expires, or is lost or stolen, a card issued to replace the primary card shall also serve as the primary card. Cards are divided into debit and credit cards, issued in the form of a plastic card or in electronic form, or a tokenized / digitized version of the card stored on a mobile device and allowing contactless payment transactions using NFC technology.
3. **ATM** – a hardware and software complex for disbursing and / or accepting cash, crediting funds to a card, receiving information on transactions made by the cardholder, making cashless payments and issuing a card check for all types of transactions made. An ATM is banking equipment and is intended for the independent performance of transactions by the cardholder using the card without the participation of an authorized employee of a commercial bank.
4. **Card Blocking** – a complete or temporary ban on transactions using the card, initiated by the cardholder, the Bank or an enterprise in one of the ways established by the payment system. In the event of a complete ban, the payment card is confiscated upon presentation for servicing.
5. **Friendly Fraud** – an intentional or unintentional disclosure and/or transfer of the card or card details to a circle of people close to the cardholder (relatives, friends, colleagues, etc.), and, as a result, the performance by these persons of card transactions not authorized by the cardholder. The cardholder is responsible for such transactions.
6. **Cardholder** – a Bank's customer, an individual, including one authorized by a legal entity/individual entrepreneur - the owner of a card account, who has the right for transactions using the card on the basis of an Agreement with the Bank, including holders of the primary and additional cards opened on the card account. A cardholder may also be a child aged from 6 (six) to 16 (sixteen) years (holder of a card for kids), in whose name a card was opened by the child's parent.
7. **Card for a kid** – a bank payment card opened as an additional card to the parent's account.
8. **Optima24 Remote Banking Servicing System** (hereinafter referred to as Optima24) – a software package consisting of an Internet and mobile banking system through which the Bank provides electronic banking services to the user.
9. **Card Account** – a bank account that reflects transactions carried out using a card or its details.
10. **Card transaction** – a transaction using a card and/or its details and other remote service tools (for example, the purchase of goods, services, transfer of funds, currency exchange or receipt of cash), which results in change of the balance of funds on the cardholder's card account.
11. **Compromise of a Card** – the fact of access by a third party other than the cardholder to confidential information related to the card, its details or card account, as well as to passwords and logins from Optima24, as well as a suspicion of the fact of such access.
12. **Call Centre** – a Bank subdivision, which is a 24-hour call centre designed to process remote requests from existing and potential customers of the Bank. **Call Centre phones can be found on the Bank's official web-site at www.optimabank.kg**.
13. **Single-Currency Card** – a card with one currency for maintaining the card account.

14. **Mobile Device** – any portable device of the cardholder, which has the Mobile Payment Service installed and support for NFC technology (for example, a smart watch, smartphone, tablet, etc.).
15. **Multicurrency Card** – a card linked to a single card account with several currency sub-accounts (currency baskets). Each sub-account stores funds in its own currency: Kyrgyz soms (KGS), US dollars (USD), euros (EUR), and rubles (RUB). The Bank's mobile app displays the following information to the customer:
    - Total available balance – in Kyrgyz soms (KGS), calculated as the sum of all currency balances, recalculated at the Bank's commercial exchange rate (buy rate) at the time of the request;
    - Separate balances for each sub-account – in their own currencies (KGS / USD / EUR / RUB)
16. **Normalization** – an automatic process of redistributing funds between currency sub-accounts of a single card. It is used if the corresponding currency sub-account has insufficient funds (the currency sub-account is overlimit) in the course of a transaction. In this case, the system uses the positive balances in other currency sub-accounts of the same card to process the transaction. Recalculation is performed at the Bank's commercial exchange rate in effect on the date and time of the normalization.
17. **Payment System of Settlements Using Bank Payment Cards** (hereinafter referred to as the Payment System) – a system of settlements using cards issued and serviced in accordance with the requirements of the operators of these systems and the legislation of the Kyrgyz Republic. The payment system shall establish certain rules for the implementation of mutual settlements on payments using cards between the system participants. Payment systems shall be divided into local (for example, MIR), national (Elcard) and international (Visa, MasterCard, etc.).
18. **Mobile Payment Service** – Provider's software (including a mobile application) delivered to the cardholder under a separate agreement between the Provider and the cardholder, designed to tokenize payment cards, manage tokens, and execute payment transactions using a mobile device. The terms of use and functionality of the Mobile Payment Service shall be determined by the Provider. If the Provider is a Bank, the Mobile Payment Service shall be the Bank's mobile application. Mobile Payment Services include, but are not limited to, mobile payment systems based on e-wallets (Google Pay, Garmin Pay, etc.), which enable payment for goods and services, as well as cash withdrawals, using NFC technology.
19. **Posting (or Clearing)** – the final reflection of a card transaction on a customer's card account, during which the card transaction amount shall be debited from or credited to the card account. At this stage of card transaction processing, previously blocked funds for the authorized transaction are actually debited from (or credited to) the card account. In this case, to post card transactions on a multicurrency card, normalization between card account sub-accounts is performed, if necessary.
20. **Processing** – a licensed activity that includes interrelated processes for receiving, processing and issuing financial information to participants in the payment system.
21. **Processing Centre** (hereinafter referred to as PC) – a legal entity that shall carry out processing.
22. **Provider** – a legal entity that is the manufacturer (developer) of the Payment Mobile Service, which ensures, on the basis of the rules of payment systems and / or on the basis of a separate agreement with the payment system, information and technological interaction in the formation, maintenance and use of the token for the purpose of card transactions. In addition, the provider may be the Bank, if the cardholder uses the Bank's software.
23. **Recurring Payments** – regular card transactions (payments) initiated by the recipient of the payment (the supplier of goods and/or services) on the basis of consent previously provided by the cardholder, carried out using previously saved card details without the need for repeated participation and confirmation by the cardholder, including, but not limited to, subscription fees and payments for Internet resource services, as well as other periodic payments for goods and/or services.

24. **Social Engineering** – a set of psychological and sociological techniques, methods and technologies that allow fraudsters to obtain protected/secret information of the cardholder, in order to steal money.
25. **Stop List** – a list of blocked cards, for which all and/or certain types of transactions have been canceled or temporarily suspended.
26. **Card Tokenization** – a technology provided by payment systems and designed to exchange confidential card data for a special impersonal equivalent (token), to protect card details. During the tokenization process, a link is created between the card and token details, which allows for the card used to perform transactions using the token to be uniquely identified. Transactions performed using the token shall be equivalent to transactions performed by the cardholder using the card itself or its details.
27. **Token** – a digital representation of the card, which is formed upon card tokenization and stored in encrypted form in the secure cloud storage of the payment system and is also saved in the memory of the mobile device.
28. **Digital Customer** – an individual citizen of the Kyrgyz Republic who uses the Bank's services and products and who has registered in the Optima24 system by completing remote identification (an electronic identification and verification procedure for individuals) without visiting a Bank division. A digital customer may also hold a Bank card.
29. **Digital Card** – a bank card without a physical plastic card, available only in electronic form in Optima24.
30. **Fishing** – a type of online fraud aimed at gaining access to a cardholder's confidential information (card details, passwords, and access data for remote banking systems) by misleading them, including through mass mailings and messages purporting to be from a bank or other organization containing links to fake online resources. Use of the obtained information may lead to unauthorized cashing-out from the card account, for which the cardholder shall be responsible.
31. **Acquirer** – a Bank that has received permission to acquiring, the owner of a network of peripheral devices that provides the ability to carry out authorization or transactions through its peripheral devices in accordance with the technology and regulations of the relevant payment systems and the legislation of the Kyrgyz Republic.
32. **Acquiring Network** – includes all peripheral devices of acquiring banks of participants in payment systems, which are intended to carry out card transactions: ATMs; cash POS terminals installed in bank divisions; trade POS terminals installed in merchants; payment terminals; automatic deposit machines; electronic commerce.
33. **Electronic Commerce** *(E-commerce)* – the activities of merchants in the remote sale of goods and/or provision of services using information and telecommunications networks (including the Internet), providing for the implementation of non-cash payments, including the use of payment cards.
34. **Embossed Name of the Cardholder** – the cardholder's surname and first name in Latin transcription, printed on the front side of the card.
35. **Issuer** – a bank that issues cards in accordance with the technology and rules of the relevant payment systems and the legislation of the Kyrgyz Republic.
36. **CVV2 code** *(Card verification value)* – a three-digit code for verifying the authenticity of the card, requested when paying via the Internet and other transactions.
37. **Near Field Communication (NFC)** is a short-range wireless data transmission technology that enables data exchange between devices and/or a card and devices. Most payment systems require that cards support contactless payment technology (NFC).
38. **PIN code** *(Personal identification number,* hereinafter referred to as PIN code) – a personal identification number that allows the user to be authenticated to perform a transaction. The PIN code is a password for accessing the card and is classified as protected information that is not subject to disclosure to third parties other than the cardholder. The PIN code of the card is assigned to **identify** its holder when performing card transactions.
39. **POS Terminal** *(point-of-sale)* – a terminal for accepting payment for goods and services in merchants using a card and other remote service tools.
40. **3D Secure password** – a secure protocol that is used as an additional level of security for two-factor authentication of the user for transactions without a card. The technology was developed for the Visa payment system to improve the security of online payments within

the Verified by Visa (VbV) service. Services based on this protocol have also been adopted by Mastercard payment systems under the name Mastercard SecureCode (MSC). 3D Secure password is generated dynamically and is intended for use when making Internet purchases on the Internet.

41. **QR code** – a two-dimensional barcode symbol for transmitting payment data, which is used when making cashless payments and transfers.

Chapter 1. General Provisions

42. The Rules for Using Cards of Optima Bank OJSC (hereinafter referred to as the Rules) shall define the terms of use, terms of service and security measures in course of card transactions using payment system cards issued by Optima Bank OJSC (hereinafter referred to as the Bank).
43. These Rules have been drawn up in accordance with the Regulation of the National Bank of the Kyrgyz Republic "On Bank Payment Cards in the Kyrgyz Republic", the Regulation on Payment Cards of Optima Bank OJSC and the rules of the relevant payment systems.
44. These Rules shall be standard (typical) and shall not be subject to change by the cardholder. The Bank may revise these Rules unilaterally as necessary by posting information about the changes made on the corporate website at https://www.optimabank.kg/index.php?option=com_newscatalog&view=default&cid=4&Itemid=215&lang=ru in the "News" section, considering the period established by the legislation of the Kyrgyz Republic in force for informing about upcoming changes.
45. These Rules shall be an integral part of the Agreement for a Full Package of Banking Services for Individuals at Optima Bank OJSC (hereinafter referred to as AFPBS).

Chapter 2. Procedure for Card Issue and Storage

46. The Bank shall issue a card directly to the cardholder or to an authorized person acting on the basis of the notarized power of attorney.
47. A card for kids shall be issued directly to the child's parent with mandatory submission of a birth certificate.
48. Optima24 digital customers shall be automatically issued a digital card with established restrictions and limits in accordance with the Bank's Tariffs. After full identification and verification of the customer, these restrictions are lifted, and the limits are set to the amounts provided for standard cards. The digital card shall be issued exclusively electronically in the Optima24 system and shall not be issued on a physical medium (plastic card).
49. The cardholder shall be prohibited from transferring the card, PIN code, logins and passwords for access to Optima24, one-time transaction confirmation codes (OTP) and 3D Secure passwords to third parties, as well as from providing the card or its details for use, as collateral, or using them on the instructions of third parties to commit financial or illegal actions.
50. Delivery of the card (including the PIN envelope) outside the Kyrgyz Republic shall not be carried out in accordance with the legislation of the Kyrgyz Republic in force.
51. The front side of the card shall contain:
    - Bank logo;
    - Payment system logo;
    - Embedded chip - an integrated circuit with information encoded on it;
    - Card number, consisting of 16 digits;
    - Embossed customer's name (last name and first name of the cardholder in Latin or initials if the customer's last name and first name exceeds 22 Latin characters);
    - Card expiration date;
    - Customer code in the Bank (client ID)
52. The back of the card shall contain:
    - magnetic strip
    - space for the customer's signature (optional);
    - hologram with an image of a dove (Visa cards);
    - Bank Call Centre number;

- Verification code (CVV2);
- Unique bank card number (card ID) – optional.

53. The cardholder must protect the card from mechanical damage and from exposure to electromagnetic fields (car alarms, mobile phones, computers, checkpoints at airports, banks, stores, etc.) in order to avoid damage to the magnetic strip.
54. It shall be prohibited to exert any physical impact with any object on the surface of the PIN envelope, chip or card. In the event of damage to the card, chip or PIN envelope as a result of intentional, negligent or unintentional actions of the cardholder, the card shall be reissued at the cardholder's expense in accordance with the Bank's current Tariffs.
55. The rate of commissions and tariffs for issuing and servicing cards, as well as spending and income limits for card transactions, limits on money transfer transactions, limits on conversion of funds by currency and/or type of bank account, limits on contactless payments permitted to be made without entering a PIN code, shall be determined by the Bank's Tariffs. Information on the amount of limits, rates of commissions and tariffs shall be posted on the Bank's corporate website at https://optimabank.kg/ru/for-individuals/rates.
56. For security purposes, the Bank shall not recommend setting extremely large amounts of limits for a long period of time. Responsibility for the consequences of non-compliance with this clause shall rest with the cardholder.
57. The card account shall be intended only for the following card transactions:
    57.1. Crediting to/debiting from card accounts of individuals of funds in cash and cashless form of a non-commercial nature;
    57.2. crediting to card accounts of legal entities of funds in cash and cashless form of a commercial nature;
    57.3. debiting from card accounts of individuals and legal entities of funds to pay for goods, services of merchants and other third parties;
    57.4. debiting from the card account of the cardholder of funds to pay Bank fees and debt on a loan(-s) (including technical overdraft);
    57.5. debiting from the card account of individuals and legal entities of funds to pay off debt to the Bank that arose in the process of issuing and servicing a payment card, including in excess of the balance of funds on the card account;
    57.6. crediting to and debiting funds from card accounts of individuals and legal entities in the amount of transfer transactions (including Bank fees in accordance with the current Tariffs);
    57.7. debiting funds from card accounts of individuals and legal entities based on execution orders stipulated by the legislation of the Kyrgyz Republic in force.
58. Remote service of cardholders can be carried out through the Call Centre, corporate website of the Bank www.optimabank.kg and the Bank's remote banking system (Optima24). The terms of service shall be regulated by the Bank's internal regulations and tariffs.
59. The Bank shall have the right to provide the cardholder with the opportunity to carry out tokenization for further card transactions using a token (a mobile device on which the token is stored) in the manner and on the terms stipulated by the AFPBS.
60. At the initiative of the cardholder, the card can be linked to mobile payment services (electronic wallets Google Pay, Garmin Pay) for payment of goods and services and withdrawal of funds using tokenization technology and payment via a mobile device using the NFC module. In the course of transactions using a token, the cardholder shall be verified by the cardholder entering the password, biometric data or by any other means of verification provided for by the payment mobile service and, in cases established by the payment system rules, it may be additionally required to enter a PIN code (for payments via POS terminals or ATMs).
61. In order to ensure the possibility of card transactions using contactless payment technology (NFC), including for the purpose of providing the Cardholder in the Bank's mobile application with information about the card transactions performed by him/her, the Bank shall have the right to transfer information about the amount of the card transaction, the date and time of its performance, the type of transaction, the currency code, the

authorization status for its processing to the Providers (Google Ireland Limited, Garmin Ltd., etc.) of the software of mobile payment services (Google Pay, Garmin Pay, etc.).

62. When the Cardholder uses NFC technology, the Bank shall not be liable:
    62.1. for the consequences that may arise if information about a tokenized card, including the balance of such a card, displayed on the screen of the device, becomes known to third parties;
    62.2. for situations related to failures in the operation of systems that ensure the receipt, processing and transmission of data on transactions performed using the card or its token for reasons beyond the control of the Bank, as well as for failures, interruptions or errors caused by the actions of providers, payment systems or telecommunication networks.
63. The use of mobile payment services (Google Pay, Garmin Pay) shall be carried out considering the technical and functional capabilities of the Cardholder's mobile device and the installed software required to use the relevant services.
64. When using mobile payment services (Google Pay, Garmin Pay), the security of card transactions shall depend, among other things, on the Cardholder's compliance with requirements for protecting access to the mobile device and the software installed on it. The Cardholder shall undertake to take reasonable measures to ensure the confidentiality of one-time passwords, passwords, PIN codes, and other means of access to the mobile device, mobile application, and a payment card.
65. The token shall be issued for a period of up to 6 (six) years. The token can be deleted by the Cardholder independently on a mobile device directly via electronic wallet (Google Pay, Garmin Pay) or by contacting the Bank. The token can be blocked by contacting the Bank.

Chapter 3. PIN Code

66. By default, for security reasons, cards, including digital cards, shall be issued without a paper envelope containing the card's PIN code. The cardholder shall set the card's PIN code independently in Optima24. The cardholder can further manage (change) the PIN through the Bank's mobile app (using the "Change PIN code" function).
67. At the cardholder's request, the card may be issued with a special envelope containing the PIN code. Upon receipt of the card, the cardholder should be advised to open the envelope immediately upon receiving the card, make sure that the PIN code is printed legibly, remember the PIN code and then destroy the PIN envelope for security reasons. Given that the PIN code can be changed in the Bank's mobile app, it shall be recommended to store the envelope separately from the card and out of the reach of third parties after card activation.
68. The PIN code should not be known to Bank employees and must be kept secret by the cardholder for the entire period of using the card.
69. A lost PIN code on paper, as well as a PIN code set through the Bank's mobile application, can be changed independently by the cardholder through Optima24.
70. It shall be recommended to adhere to certain rules to ensure the secrecy of the PIN code:
    70.1. it shall be prohibited to indicate the PIN code on the card;
    70.2. it shall be prohibited to store the PIN envelope with the PIN code and the card next to each other (in the same place);
    70.3. do not allow third parties to watch the PIN code numbers entered on the device keyboard (ATM, terminal);
    70.4. do not make mistakes when entering the PIN code numbers. If the limit of attempts to enter the PIN code incorrectly (5 attempts in a row) permitted by the bank is exceeded, the card shall be automatically blocked, and further card transactions are impossible. In case of loss of the PIN code (forgotten), the cardholder is advised to use the PIN code change function in the Bank's Optima24 mobile application or contact the nearest division of the Bank or the Bank's Call Centre to reset the attempts to enter the PIN code incorrectly.
71. Card transactions confirmed by entering a PIN code should be considered by the Bank to be made by the cardholder and shall not be subject to challenge due to unauthorized access to the card account and/or fraud.

Chapter 4. Use of a Card in Merchants

72. Cashless payment for goods, services and work in merchants shall be made within the established limit on the card and the limit on the acquiring device of the acquiring bank.
73. The maximum amount of one transaction and the number of transactions per day on the acquiring device of the Bank and/or a third-party acquiring bank shall be determined by the Bank's Tariffs, the acquiring bank's policy and the rules of payment systems.
74. Payment for goods and services can be made by:
    74.1. reading the card's magnetic strip and entering a PIN code;
    74.2. reading the card's magnetic strip without entering a PIN code;
    74.3. reading the card's chip and entering the PIN code;
    74.4. reading the card's chip without entering the PIN code;
    74.5. reading a contactless chip through a contactless chip reader without entering a PIN code within the established limits according to the Bank's Tariffs, the acquiring bank and/or the rules of payment systems;
    74.6. reading a contactless chip through a contactless chip reader with entering a PIN code for amounts above the established limit according to the Bank's Tariffs, the acquiring bank and/or the rules of payment systems;
    74.7. using a card token without entering a PIN code (within the established limits) or with entering a PIN code (for amounts above the established limit). The limits shall be regulated by the policy of the Bank, the acquiring bank and/or the rules of payment systems;
    74.8. reading a QR code.
75. Cashless payment for goods and services in a merchant can be made either online or offline, depending on the settings of the acquiring bank's devices. The cardholder shall be responsible for offline transactions. However, payment for goods and services in POS terminals owned by the Bank in offline mode shall be prohibited by default.
76. Payment for goods and services, as well as withdrawal of funds with a chip reading error in devices supporting chip technology, shall be prohibited (Fallback transactions).
77. The Bank's cards shall be issued with the ability to make contactless payments (PayWave / NFC), which cannot be disabled at the initiative of the cardholder due to the requirement of payment systems for mandatory support of contactless payment technology.
78. All transactions using a card in a merchant must be carried out in the presence of the cardholder. This is necessary in order to reduce the risk of unauthorized receipt of the cardholder's personal data indicated on the card. Some merchants may request an identity document. Therefore, when paying for a purchase with a card, the Bank shall recommend having a passport or other identity document with you.
79. All merchants shall be equipped with payment systems logos to inform cardholders about the possibility of servicing a particular card in a given merchant, as well as the possibility of accepting payments using a QR code.
80. Card transactions require the cardholder to insert or tap the card or, in the case of card tokenization, hold the mobile device to a service device (ATM, payment terminal, POS terminal), or scan the QR code through the Optima24 mobile application when paying by QR code. The cardholder shall acknowledge that not all service devices support contactless transactions and/or transactions using mobile payment services, and therefore the Bank shall not be responsible for the inability to perform such transactions for reasons beyond the Bank's control.
81. Card transactions through a merchant or Bank shall require an employee of the merchant or Bank to carry out authorization using a POS terminal. The card shall be inserted or tapped to the reading device of the POS terminal. First, the merchant's or Bank' employee shall enter the card transaction amount on the POS terminal keyboard. In some cases, for example, if the limit of the card transaction amount permitted to be carried out without a PIN code is exceeded, the cardholder may be asked to enter the PIN code on a special keyboard. If the correct PIN code is entered and there are sufficient funds on the card account, a receipt is printed in two copies confirming the successful completion of the card transaction. When using contactless payment technology or a tokenized card, the Cardholder must bring the card or mobile device to a minimum distance from the POS

terminal or ATM to perform a card transaction or scan the QR code through the Optima 24 mobile application when paying with a QR code.

82. The Cardholder shall be recommended to:
    82.1. make sure that the data specified in the receipt is correct;
    82.2. take one copy of the POS terminal receipt until the full settlement of the card transaction, as well as for the purpose of reconciling the expenditure transactions on the card account.
83. For transactions confirmed by a PIN code, as well as contactless transactions carried out without entering a PIN code within the established limit, the cardholder's signature on the receipt shall not be required.
84. The requirements for signing a receipt when conducting transactions in the acquiring network of a third-party acquirer shall be determined by the policy of the acquirer.
85. The cardholder shall be prohibited from signing a POS terminal receipt that does not indicate the purchase amount (amount for goods / services).
86. According to the rules of payment systems, merchants shall not have the right to overstate the cost of goods and services when accepting a card for payment compared to cash. If such cases are detected, the cardholder shall be advised to notify the Bank.
87. A refund of a purchase or service paid for by card shall be made with the consent of the merchant. To do this, at the request of the cardholder, a merchant's employee must initiate a "return of purchase" operation on the POS terminal. Refund of the purchase amount in cash shall not be provided.
88. The amount of the return card transaction will be restored to the card account on the next banking day after the Bank receives the register of transactions on the return transaction on the card. This information should be considered when calculating the amount available on the card.

Chapter 5. Using a Card at an ATM

89. As a rule, cash on the card shall be withdrawn in the currency of the country of stay. Some acquiring banks may set an additional fee for cashing-out. Also, in some countries, the frequency and maximum amount of cashing-out on the card may be limited by legislation.
90. Before using an ATM, it shall be required to inspect it for devices that are not typical for it: an unevenly installed PIN-keyboard, overlays in the card receiver, the presence of mini-video cameras aimed at the PIN-keyboard, overlays above the ATM screen and other suspicious devices. If the cardholder discovers the presence of unusual devices, it is recommended not to use this ATM and notify the Call Centre of the acquiring bank by phone numbers indicated on the ATM.
91. To receive cash or other services at an ATM, it is necessary to insert card into the ATM card receiver or bring the mobile device in case of card tokenization, enter a PIN code, select the appropriate menu and follow the instructions on the screen.
92. To refuse the service, you must cancel the operation by pressing the "Cancel" button.
93. When operating an ATM, it shall not be allowed to use physical force to insert the card into the ATM. If the card cannot be inserted, you must refrain from using such an ATM.
94. When entering a PIN code, you must make sure that the PIN code is not visible to third parties. After 3 (three) attempts to enter the wrong PIN code, the card is blocked and may be detained (confiscated) by the ATM.
95. After the screen displays "TAKE YOUR CARD" command, you must immediately take the card, otherwise the card may be captured by the ATM after 15-30 seconds.
96. After the screen displays "TAKE YOUR MONEY" command, the cardholder must immediately withdraw the funds. If the funds are not withdrawn within the limited time (usually about 20 seconds) set by the ATM, such funds will be retained by the ATM.
97. It is recommended to take the receipt after each ATM transaction, since the receipt is a document confirming the card transaction in the event of dispute resolution. As the receipt contains the cardholder-related information, it is recommended to take the receipt with you and not leave it near the ATM.
98. The following may be the reasons for unsuccessful card transactions with the card at the ATM:

98.1. the requested amount cannot be withdrawn at the moment with the banknotes available on the ATM cassettes. In such a situation, it is recommended to request an amount that is a multiple of the minimum banknote denomination specified in the instructions (on-screen menu) for this ATM;

98.2. the requested amount exceeds the one-time withdrawal limit determined by the technical characteristics of the ATM. In such a situation, it is recommended to divide the requested amount into parts and repeat the transaction several times;

98.3. the requested amount exceeds the available balance of the card account (considering the commission of the Bank and/or of the acquiring bank). In such a situation, it is recommended to request a smaller amount. The available balance of the card account can be clarified, including by requesting the available balance of funds on the card through the ATM menu.

99. If the card is swallowed by an ATM, you should make sure that the card is actually swallowed (the ATM continues to serve other customers or has stopped functioning). Otherwise, the ATM may return the card to another customer and / or issue the requested funds to him/her.

100. If the card is swallowed by an ATM, the cardholder shall be recommended to immediately block the card in any convenient way: by contacting the Bank's Call Centre or independently through Optima24. In the future, the Bank shall recommend issuing a new card with new details, since when the card is swallowed, there is a risk of third parties accessing the card and / or card details.

101. If the card or funds are swallowed by an ATM, you must immediately contact the Bank or the acquiring bank by phone numbers indicated on the ATM.

Chapter 6. Using the Card on the Internet

102. Card transactions on the Internet shall be performed within the established limit for Internet payments and the limit of the acquiring bank.

103. Payment for goods or services on the Internet shall be made without the physical card, but using the card details, the mandatory ones of which are: card number, card expiration date, embossed name of the cardholder. Additionally, payments on the Internet may require the following card details: CVV2, 3D Secure password in accordance with the terms of service of the Internet resource. Payment for goods or services on the Internet can also be made using a token.

104. The Bank shall issue cards with an open access to Internet payments.

105. The cardholder can close access Internet payments (except for card transactions carried out with the introduction of a 3D Secure password, and recurring payments). To do this, the cardholder should be advised to apply to the Bank in writing to disable access to Internet payments or independently disable access via Optima24.

106. VISA cards of the Bank shall be issued with connected 3D Secure service. The 3D Secure protocol should not be used for transactions carried out using Elcard.

107. Payment for goods and services on Internet resources that support 3D Secure technology and require entering a 3D Secure password, without entering a 3D Secure password shall be prohibited (ECI 06).

108. Card transactions on the Internet can be carried out in the following ways:

108.1. by providing payment card details on the Internet resource, including the cardholder's name, card number, and expiration date; additionally, depending on the requirements of the Internet resource and the security measures applied, a CVV2 code and/or confirmation of the transaction using 3D Secure technology may be requested on Internet resources that support this technology;

108.2. by using a payment card token, including through mobile payment services and other solutions that support tokenized Internet payments, without transferring payment card details to the Internet resource, in accordance with the rules of the payment systems and the terms of service of the relevant service;

108.3. by linking the payment card details and/or token to an Internet account, e-wallet, store, trading platform, or other Internet resources in accordance with the terms of service of the resource. In case of linking a card / token, it shall become possible to make recurring payments. The cardholder shall be responsible for such

transactions until the card details are unlinked / the token is deactivated. In this case, the cardholder shall be recommended to keep the certificates of unlinking the card or deactivation of the token, which may be required in the event of a dispute between the cardholder and the Internet resource.

109. Access to transactions on the Internet in excess of the limit established by the Bank's tariffs shall be provided:
    109.1. by the cardholder contacting a division of the Bank and submitting a written application to change the current limits and restrictions on Internet payments;
    109.2. by the cardholder independently by changing the current limits and restrictions on Internet payments in Optima24;
    109.3. by contacting the Bank's Call Centre after passing remote identification of the cardholder, while the change in the current limits and restrictions on Internet payments can be set for a period not exceeding 14 (fourteen) calendar days.
110. Before making a transaction on the Internet, the Bank shall recommend the cardholder:
    110.1. to check the card's expiration date and make sure that the card is not blocked;
    110.2. to make sure there are sufficient funds on the card;
    110.3. to make sure that there is open access to Internet payments via the card and that the limits are sufficient for this type of card transaction;
    110.4. to make sure that security updates are installed on your browser;
    110.5. to make Internet payments only on verified websites with a good reputation, as well as websites that support secure Internet payments technology (3D Secure);
    110.6. to refrain from transactions on automatically redirected pages or pop-up windows to avoid "Fishing". In most cases of "Fishing", the fraudulent clone site to which the redirection can be set up looks identical to the real one and may have just slight differences from the original site, for example, by part of the URL;
    110.7. to cancel an online payment, in full or in part, the cardholder must first contact the customer support service of the online store to initiate a refund.
111. When booking goods and/or services on the Internet that fall under the Travel & Entertainment Category, including, but not limited to, hotel reservations, car rentals, purchase of transportation tickets, and similar services, a pre-authorization (blocking) of funds may be made on the cardholder's card account until final settlement with the merchant is completed. The final debit amount may differ from the pre-authorization amount and be increased within the limits permitted by the rules of the relevant payment system, including with consideration of the actual services rendered and additional expenses. The cardholder shall undertake to ensure that sufficient funds are available to pay for such transactions and any associated additional amounts.

Chapter 7. Security Measures to be Taken When Using the Card

112. The card number, PIN code, CVV2 code, card expiration date, embossed cardholder name, client ID in the Bank, 3D Secure and OTP passwords, as well as the Optima24 login and password shall represent the card details and confidential information that provide access to the cardholder's funds, therefore they fall under the category of protected information that is not subject to declassification and transfer to third parties.
113. The cardholder shall be responsible for the safety of the card details and confidential information. The card details and confidential information must not be known to third parties. The cardholder shall be obliged to store the card details and confidential information in a safe place inaccessible to third parties.
114. The use of the card, card details, confidential information (PIN code, 3D Secure and OTP passwords, Optima24 login and password), as well as the use of a mobile device containing data on the tokenized card, by third parties shall be prohibited.
115. The cardholder shall be responsible for compliance with and for the consequences of non-compliance with clauses 112-114 of these Rules. The cardholder shall agree that in the event of detection of cases of violation of clauses 112-114 of these Rules, the card will be unilaterally blocked by the Bank.
116. The cardholder shall be prohibited from:

116.1. writing down any data from the card details, as well as the Optima 24 password/login or mobile device passwords on the card itself or storing them together with or near the card;
116.2. leaving the card and/or its details, as well as the mobile device or other confidential information in places accessible for copying and/or recording and/or using by third parties;
116.3. transferring to third parties the card details (all or part of them), one-time passwords, as well as the Optima24 password/login, mobile device passwords.

117. All financial and material responsibility for card transactions made using the card and/or its details, including with or without the use of card passwords (PIN code, 3D Secure password), as well as for transactions made in Optima24 (including transactions conducted by scanning a QR code) or using a mobile device (including tokenized transactions) by third parties, shall be rest on the cardholder.
118. In case of loss, theft or suspicion of using the card or its details by a third party, and/or receipt by the cardholder of an SMS/push notification with information about a card transaction that he/she did not perform, as well as in case of voluntary transfer of a mobile device or confidential information to third parties, or in case of loss/theft of a mobile device and/or compromise of a token, the cardholder shall be obliged to contact the Bank IMMEDIATELY via official communication channels posted on the corporate website of the bank at www.optimabank.kg, to block the card/token, or block the card independently via Optima24, selecting the appropriate reason for blocking, when this fact became known to the cardholder or the cardholder has suspicions about this fact. The cardholder shall be responsible for all card transactions and his/her actions or inactions and/or the actions or inactions of third parties until the card/token/Optima24 is blocked.
119. A lost/stolen card or a card with compromised details or secret information shall be subject to blocking and cannot be reissued while maintaining the primary card details. The cardholder must contact the Bank to issue a new card with the new card details. Further use and/or unblocking of lost/stolen/compromised cards shall be prohibited.
120. If a lost/stolen/compromised card was unblocked at the initiative of the cardholder, all responsibility for possible subsequent unauthorized write-offs on the card shall rest on the cardholder. The cardholder shall lose the right to initiate a dispute process in accordance with the rules of the payment systems.
121. The Customer shall be obliged to comply with the following security requirements in order to exclude unauthorized transactions using the token:
121.1. Do not leave your mobile device unattended;
121.2. Ensure an adequate level of security on your mobile device by using passwords and other possible methods of locking/unlocking your mobile device;
121.3. Make sure that no fingerprints or other authentication methods of another person, including facial recognition, are registered on your mobile device;
121.4. Do not disclose your mobile device password to third parties;
121.5. Delete all personal data and financial information from your mobile device if you no longer use it;
121.6. Immediately contact the Bank by phone number indicated on the back of the card or via the official communication channels posted on the Bank's corporate website at www.optimabank.kg if you suspect any unauthorized use of the token, or if your mobile device has been hacked, lost or stolen;
121.7. Do not block any security functions provided on the mobile device for the purpose of protecting the token;
121.8. It is mandatory to create a complex password and save only your biometric data (fingerprints, facial recognition, etc.) for using the mobile device;
121.9. When transferring a mobile device to third parties, the cardholder shall be obliged to delete personal and financial data from it or immediately contact the Bank to temporarily suspend the use of mobile payment services and, if necessary, the payment card;
121.10. Do not subject the mobile device to privilege escalation/hacking operations of the device's operating system (jail break, rooting, etc.);

121.11. Do not use the mobile payment service when connected to public wireless networks;

121.12. Do not perform verification in the mobile payment service on the mobile device(s) belonging to the third party (parties).

122. The cardholder shall be fully liable for any losses incurred as a result of card transactions within the framework of “Friendly Fraud” and/or as a result of “Fishing” and/or “Social Engineering”, since such transactions are carried out using data and authentication tools voluntarily transferred by the cardholder to third parties or used in the absence of proper control on the part of the cardholder over the safety of payment details, one-time passwords, PIN codes and other means of access.

123. In order to track card account transactions and promptly respond and block the card in case of unauthorized access to the card account, the cardholder should be recommended to activate the service for receiving SMS/push notifications on card transactions. Payment for this service shall be paid according to the Bank’s Tariffs.

124. The cardholder should be recommended to monitor the status of the card account at least once a month. For these purposes, the cardholder can independently generate a statement in Optima 24 or contact the Bank to receive a card account statement.

Chapter 8. Processing of Card Transactions

125. A card transaction within the rules of payment systems shall be processed in two stages:

125.1. **Authorization** - stage 1, which involves blocking funds on the cardholder’s card account; at the authorization stage, the available balance of the card account shall be reduced by the amount of the successfully authorized card transaction.

125.2. **Posting** - stage 2, which involves accepting the card transaction for accounting, which is carried out after receiving all documents for this card transaction. At this stage, the final financial processing of the card transaction occurs, i.e. debiting or crediting funds to the cardholder’s card account depending on the type of card transaction (debit or credit).

126. For the period between the date of authorization and posting of the card transaction, the amount of the card transaction (including commissions) shall be blocked on the cardholder’s card account and shall be finally posted within a period of up to 30 (thirty) calendar days.

127. Blocking funds for successful card transactions at the authorization stage shall result in a decrease or increase in the available card account balance depending on the nature of the card transaction: expenditure or receipt. An expenditure card transaction shall always result in a decrease in the available balance, and a receipt card transaction shall increase the available card account balance if this is provided for by the rules of the payment systems (for example, when processing incoming money transfers from Visa cards issued by third-party banks to an Optima Bank card (Visa Direct), the available balance of the card account increases).

128. Posting of transactions shall be performed after the Bank receives an electronic financial document from the acquiring bank through the relevant payment system.

129. **Instant Posting mode** shall be used to process card transactions on multicurrency cards. In this mode, funds are credited/debited for certain types of card transactions immediately upon receipt of an authorization notification from the payment system or the Bank’s mobile application. These types of card transactions shall include:
- incoming/outgoing money transfers within the Bank (by phone number, card number, QR code);
- incoming money transfers from Visa cards issued by third-party issuing banks (Visa Direct);
- incoming/outgoing transfers from other banks of the KR by phone number/card number;
- conversion transactions carried out on multicurrency card sub-accounts;
- card top-ups with cash at Bank divisions and payment terminals;
- incoming/outgoing transfers via QR code from other banks of the KR.

130. If the Bank does not receive confirmation of a Visa Direct transfer via the Visa payment system from the sending bank, the previously credited transfer amount may be debited

from the customer's card without further consent. If a negative balance is subsequently created on the card, the cardholder shall be obligated to top it up by the corresponding amount.

131. Instant Posting **shall not apply** to the processing of the following multicurrency card transactions:
   - transactions at POS terminals in its own or third-party network;
   - cashing-out at ATMs in its own or third-party network;
   - online transactions (e-commerce), including recurring payments.

When performing the above transactions, if there are insufficient funds in the currency sub-account where the transaction is being conducted, there is a sufficient overall available balance on the card account (due to funds in other currency sub-accounts), a negative balance (overlimit) may temporarily accumulate on the corresponding sub-account until the sub-accounts are automatically normalized upon posting the transaction in accordance with clause 135.5 of these Rules.

132. If the acquiring bank fails to post the transaction (financial document) after 30 (thirty) calendar days, the amount of funds for the card transaction shall be automatically unblocked and shall become available to the cardholder for reuse.
133. If the Bank receives a financial document for debiting from the acquiring bank within 30 calendar days (posting of transactions within 30 calendar days), the Bank shall have the right to debit funds from the cardholder's card account without acceptance in the amount of previously unblocked amounts of successful card transactions.
134. Features of processing card transactions for **single-currency cards**:
   134.1. when conducting a card transaction in the acquiring network of the Bank in a currency different from the currency of the card account, the card transaction shall be processed at the commercial rate of the Bank set on the day of authorization.
   134.2. when conducting a card transaction in the acquiring network of a third-party Bank in a currency different from the currency of the card account, the card transaction shall be processed in USD at the exchange rate of the payment system on the date of **authorization** of the card transaction.
   134.3. In the event of a technical overdraft on the card account, this debt should be considered at the commercial rate of the Bank (Buy) in effect at the time this debt was created.
135. Features of processing card transactions for **multicurrency cards**:
   135.1. The available balance of a multi-currency card account shall be displayed in KGS by recalculating and summing up the balances of all currency baskets (the sum of the sub-account balances KGS + USD + EUR + RUB) at the commercial rate of the Bank (Buy) in effect at the time the cardholder requests the available card balance;
   135.2. Blocking of funds during a card transaction in foreign currency shall be carried out in KGS at the commercial rate of the Bank (purchase) in effect on the date of **authorization**.
   135.3. In the course of a card transaction in the currencies of a multicurrency card account's sub-accounts (KGS, USD, EUR, RUB), funds shall be blocked in the amount and currency of the transaction and reflected in the corresponding currency sub-account. Therefore, for transactions in these currencies, the sub-account balance should be adjusted in the same currency for the transaction amount.
   135.4. In the course of a card transaction in currencies other than the sub-account currencies (KGS, USD, EUR, RUB), funds shall be blocked in USD at the Visa exchange rate in effect on the authorization date.
   135.5. If the corresponding sub-account has insufficient funds at the authorization stage, but other currency sub-accounts have a sufficient balance (equivalent to the missing amount at the Bank's commercial exchange rate), this sub-account may temporarily overflow its currency sub-account (negative balance). After the final mutual settlements for the card transaction (posting) have been completed, this overlimit of the foreign currency sub-account will be automatically settled (normalized) using funds in the customer's other foreign currency sub-accounts.

135.6. Mutual settlements (posting) for card transactions of the multi-currency card account shall be carried out as follows:

135.6.1. For card transactions made in a foreign currency other than KGS, USD, EUR, or RUB, posting shall be performed in USD at the payment system exchange rate as of the **authorization** date (provided the sub-account has a sufficient balance);

135.6.2. When posting a card transaction made in KGS, funds should be debited in KGS from the KGS sub-account (provided the sub-account has a sufficient balance).

135.6.3. When posting a card transaction made in USD, funds should be debited in USD from the USD sub-account (provided the sub-account has a sufficient balance).

135.6.4. When posting a card transaction made in EUR, the card transaction amount should be debited in EUR from the EUR sub-account (provided the sub-account has a sufficient balance).

135.7. If there are insufficient or no funds on the relevant sub-account for posting a card transaction, the Bank shall automatically **normalize** this sub-account by converting the balances of funds on the balances of other sub-accounts of the card at the commercial rate of the Bank.

135.8. **The procedure for normalizing currency sub-accounts** is as follows (in descending order of priority): 1. KGS sub-account, 2. USD sub-account, 3. EUR sub-account, 4. RUB sub-account.

135.9. In the event of a debt on the customer's card account (technical overdraft), this debt should be recorded on a KGS sub-account at the Bank's commercial rate Buy), in effect at the time of its creation.

136. In course of card transactions in a currency other than the card account currency, the Bank shall automatically convert funds into the card account currency without acceptance in accordance with Chapter 12 of these Rules. The cardholder hereby shall authorize the Bank to conduct such non-acceptance conversion of funds on the card account on the basis of these Rules and the Agreement and without any additional consent in any form from the cardholder.

137. Early unblocking of funds for successful card transactions that the cardholder considers unsuccessful shall be possible not earlier than 3 (three) calendar days from the date of authorization. Unblocking of a card transaction shall be carried out in an amount equal to the previously blocked amount in the card account currency. The Bank shall have the right to refuse early unblocking of funds in the following cases:

137.1. if the cardholder has failed to provide or has not provided in full supporting documents from the merchant regarding the failure of the card transaction;

137.2. if it is impossible to identify the card transaction in full for which early unblocking is requested based on the information contained in the supporting documents (information on the card transaction amount, transaction currency, date/time of the transaction, authorization code or other identifiers of the card transaction available in the Bank's PC is missing or does not match);

137.3. if the data of the relevant payment system does not confirm the fact of unsuccessful authorization of the card transaction;

137.4. if the cardholder has not paid a fee for early unblocking of funds in accordance with the Bank's Tariffs.

138. Unblocking of funds shall be carried out according to the data of the acquiring bank's authorization request received through the payment system in electronic form.

139. The amount previously debited from a card account for a card transaction may be refunded at the initiative of the acquiring bank/merchant in full or in part, in the currency of the original card transaction. If the currency of the card account or sub-account of a multicurrency card is different from the currency of the card transaction and is not equal to KGS, the full cancellation of the card transaction should be made in the USD equivalent established by the payment system.

140. In the event of receipt of funds on the card as a credit card transaction (credit and/or credit adjustment, etc.) and/or a reversal card transaction, which leads to an increase in the available balance of the cardholder's card account (hereinafter referred to as a credit/reversal card transaction), the Bank shall have the right to unilaterally block the

card account and/or card for a period of up to 30 (Thirty) calendar days if the cardholder does not have documents confirming the validity of the credit/reversal card transactions.

141. In the event of creation of a debt on a card account (technical overdraft) arising as a result of the acquiring bank recalling the amount of a previously received credit and/or reversal card transaction, the cardholder shall be obliged to repay the resulting debt in the manner and within the timeframe established by the Bank.

Chapter 9. Card Transaction Dispute Settlement

142. If the cardholder has disputed card transactions (financial claim), the cardholder should be recommended to contact the Bank to file an application of the established form for an investigation (Application for a Disputed Transaction – hereinafter referred to as the Dispute Application), and, if necessary, provide documents confirming the cardholder's right to a refund for the disputed card transaction.
143. If the cardholder's claim is justified and the commission is paid in accordance with the Bank's Tariffs, the Bank, on behalf of the cardholder, within the framework of the rules of the payment systems, shall initiate a financial claim against the acquiring bank.
144. If the acquiring bank agrees with the financial claim of the cardholder, the Bank shall restore the amount of the card transaction to the card account in the manner and within the timeframes established by the rules of the relevant payment systems and the internal procedures of the Bank.
145. In the event a financial claim is rejected by payment systems and deemed unfounded, including cases where, as a result of the review, paid arbitration commissions of payment systems are applied, the costs of reviewing such a financial claim (including arbitration and other commissions of payment systems), which may exceed the amount of the disputed card transaction, should be paid by the cardholder. The Bank shall have the right, without the additional consent of the cardholder, to directly debit the said commissions, as well as the amount of the unfounded financial claim, from the cardholder's card account and/or any other account of the cardholder opened with the Bank.
146. The following card transactions shall not be subject to challenge due to fraud or unauthorized access to the card account and shall be considered to have been conducted by the cardholder:
    146.1. card transactions conducted by entering a PIN code, completed with the physical presentation of the card, followed by the reading of the card chip and/or magnetic stripe data;
    146.2. card transactions made without entering a PIN code, for contact / contactless (PayWave) payments completed with the physical presentation of the card;
    146.3. card transactions completed with the use of 3D Secure technology (entering a one-time password or other means of authentication);
    146.4. card transactions completed in the Optima24 remote banking system of the Bank, including transactions with the use of QR codes;
    146.5. card transactions completed with the use of a card token (including payments through digital wallets and other tokenized services).
147. A card transaction shall be considered authorized by the cardholder if, within 45 calendar days from the date of its completion, the cardholder has not filed a Dispute Application with the Bank due to unauthorized access to the card account. The maximum number of disputed card transactions may not exceed 35 (thirty-five) over the last 120 (one hundred twenty) calendar days for one card.
148. The Bank shall have the right to reject a Dispute Application for a card transaction if the period of the cardholder's appeal has exceeded 120 (one hundred twenty) calendar days from the date of the disputed card transaction.
149. In order to monitor card transactions on the card account and to promptly respond and block the card in the event of unauthorized access to the card account, the cardholder should be recommended to connect the service for receiving SMS/push notifications on card transactions, and also to generate a statement on the card account in Optima24 mobile app independently on a regular basis or request a card account statement from the Bank divisions.

Chapter 10. Monitoring of Card Transactions and Blocking of Cards

150. The Bank shall monitor card transactions in order to identify suspicious, fraudulent and/or atypical card transactions in order to reduce the risk of unauthorized access to the card accounts of the Bank's cardholders.
151. The Bank may block a card based on the results of monitoring in order to clarify the participation of the cardholder in the card transaction, as well as:
    151.1. on suspicion of fraud on the part of the cardholder or the participation of the cardholder in a fraudulent scheme;
    151.2. in the event of negative feedback from social network users or group members addressed to the cardholder.
152. Blocking of a card/card account shall be carried out by the Bank unilaterally, while blocking for the reasons specified in clause 151 of these Rules may be carried out for a period of up to 30 (thirty) calendar days with the right of the Bank to further extend the blocking period until all circumstances are clarified.
153. If the Bank shall detect multiple unsuccessful card authorizations, namely 5 (five) or more unsuccessful card transactions within 2 (two) calendar days at one merchant and/or on one website, as well as for recurring payments or auto payments, including cases of refusals due to blocked access, insufficient funds, lack of communication with the cardholder to confirm participation in the card transaction, failure to top up the card account and/or failure to disable (unlink) the card from recurring payments, the Bank shall have the right to place the card on the stop list. Removing a card from the stop list shall be carried out in accordance with the Bank's Tariffs.

Chapter 11. Instructions for Payment with a QR Code and Safety Rules

154. Instructions for Payment with a QR code:
    154.1. Step 1: Open the bank's mobile app. Launch your bank's app on your smartphone.
    154.2. Step 2: Find the QR code payment option in the main menu of the Bank's mobile app.
    154.3. Step 3: Point your smartphone camera at the QR code provided to you. Make sure the QR code is fully visible in the scanning field.
    154.4. Step 4: After scanning, make sure the payment information (amount, recipient) matches the specified one. Check all payment / transfer details carefully.
    154.5. Step 5: Confirm the payment / transfer. Enter the necessary details if required (e.g. amount) and confirm the payment. You may be asked to enter your PIN or use biometric authentication (fingerprint, face).
    154.6. Step 6: Make sure you receive a notification of successful payment. Save or take a screenshot of the confirmation for your own safety.
155. Safety rules for making payments / transfers with a QR code:
    155.1. Regularly update your bank's mobile app to the latest version to protect against vulnerabilities and security threats.
    155.2. Enable transaction notifications in the bank's app to monitor all transactions on your account.
    155.3. Make purchases / transfers only through the bank's official mobile app, downloaded from trusted sources (Google Play, App Store).
    155.4. Before making payment / transfer, make sure the scanned QR code is authentic to eliminate the risk of QR code substitution (for example, make sure that the static QR code is not re-glued at the point of sale).
    155.5. If you are redirected to a website when scanning a QR code to make payment / transfer, make sure that the URL starts with https:// and belongs to the official domain. Do not enter your personal data or bank card details, including sensitive card or mobile app information, on unverified or suspicious websites.
    155.6. In case of erroneous transfer, if you transferred / paid the wrong amount with a QR code, inform the seller about it, a bona fide merchant must immediately return the excess money.
    155.7. All responsibility for payments / transfers of funds made with a QR code shall rest with the cardholder. Transfers of funds, including those made with a QR code, shall be considered voluntary and irrevocable.

Chapter 12. Conversion of Funds

156. **Basic Rules for Conversion on Single-Currency Cards**

156.1. **Rule No.1:** If the currency of the card transaction matches the currency of the card account management, no conversion of funds will be made.

156.2. **Rule No.2:** In the event of a card transaction in Kyrgyz soms (KGS) using a card with the management currency of US dollars (USD), the conversion will be made at the Bank's commercial rate **(Buy)** on the date of **authorization** of the card transaction.

156.3. **Rule No.3:** In the event of a card transaction in US dollars (USD) using a card with the management currency of Kyrgyz soms (KGS), the conversion will be made at the Bank's commercial rate **(Sell)** on the date of **authorization** of the card transaction.

156.4. **Rule No.4:** In case of a card transaction in a currency other than Kyrgyz som (KGS) or US dollars (USD), the card transaction amount will be converted in two stages:

156.4.1. Stage 1: Conversion from the card transaction currency to USD at the Visa payment system exchange rate adjusted for the OIF rate (the OIF rate is provided for in the Bank's Tariffs);

156.4.2. Stage 2: If the card is issued with the US dollar (USD) management currency, the transaction amount will be debited in USD in the amount under clause 156.4.1. If the card is issued with the Kyrgyz som (KGS) management currency, the card transaction amount will then be converted from USD to KGS at the Bank's commercial rate **(Sell)**.

157. **Examples of conversions for single-currency cards** The conditions (table below) accepted for settlements are given as an **illustration** of examples of processing card transactions on single-currency cards:

Example No.1 Expenditure transaction for KGS 5,500 and USD 68:

Card type:	Single-currency card in		Single-currency card in	
Card balance in nominal value (current balance):	KGS	USD	KGS	USD
	6 400 KGS	72 USD	6 400 KGS	72 USD
Payment card exchange rates (KGS/USD): purchase	*85*		*85*	
sale	*90*		*90*	
Expenditure transaction for KGS 5,500 and USD 68 (without instant posting), KGS	5 500 KGS	68 USD	68 USD	5 500 KGS
in processing	5 500 KGS	68 USD	6 120 KGS	65 USD
Available balance at the authorization stage:	KGS	USD	KGS	USD
	900 KGS	4 USD	280 KGS	7 USD
Posting stage - amount to be debited in the card account currency:	5 500 KGS	68 USD	6 120 KGS	65 USD
Available balance after posting:	KGS	USD	KGS	USD
	900 KGS	4 KGS	280 KGS	7 KGS

Calculation of amounts in processing: USD 68 * 90 = KGS 6,120 KGS 5,500 / 85 = USD 65

Example No.2 Expenditure transaction for TRL 1,000 and EUR 65:

Card type:	Single-currency card in		Single-currency card in	
Card balance in nominal value (current balance):	KGS	USD	KGS	USD
	6 400 KGS	72 USD	6 400 KGS	72 USD
Payment card exchange rates (KGS/USD): purchase	*85*		*85*	
sale	*90*		*90*	
VISA rates adjusted for OIF (USD/TRL):	*14,81*			
VISA rates adjusted for OIF (EUR/USD):			*1,09*	
Expenditure transaction for TRL 1 000 and EUR 65 (without instant posting), KGS	1 000 TRL	1 000 TRL	65 EUR	65 EUR
in processing	6 077 KGS	68 USD	5 367 KGS	60 USD
Available balance at the authorization stage:	KGS	USD	KGS	USD
	323 KGS	4 USD	1 033 KGS	12 USD
Posting stage - amount to be debited in the card account currency:	6 077 KGS	68 USD	5 367 KGS	60 USD
Available balance after posting:	KGS	USD	KGS	USD
	323 KGS	4 USD	1 033 KGS	12 USD

Calculation of amounts in processing: TRL 1,000 / 14.81 * 90 = KGS 6,077 EUR 65 / 1.09 * 90 = KGS 5,367
TRL 1,000 / 14.81 = USD 68 USD EUR 65 / 1.09 = USD 60

158. **Basic Rules for Conversion on Multicurrency Cards**

158.1. **Rule No.1:** during a card transaction in KGS or USD, or EUR, no conversion of funds will be performed, **provided that the available balance** on the KGS or USD or EUR sub-accounts, respectively, **is sufficient**.

158.2. **Rule No.2: In cases of insufficient or absent funds in the relevant foreign currency sub-account,** the sub-account corresponding to the transaction currency will be normalized using other sub-accounts with conversion at the Bank's commercial exchange rate on the date of posting the card transaction. Sub-accounts will be normalized based on the priority of the sub-accounts specified in clause 135.7 of these Rules.

158.3. **Rule No.3:** during a card transaction in a currency other than KGS/USD/EUR, the card transaction amount will be converted in two stages:

158.3.1. Stage 1: conversion from the transaction currency to USD at the Visa payment system exchange rate adjusted for the OIF rate;

158.3.2. Stage 2: if there are **sufficient funds** on the dollar sub-account (USD), the card transaction amount in the amount specified in Clause 158.3.1 hereof will be debited from the dollar sub-account. **If the balance is insufficient or there are no funds** on the dollar sub-account, the card transaction amount will be debited by normalizing the USD sub-account at the expense of other sub-accounts with conversion at the Bank's commercial rate on the date of posting the card transaction. Normalization of sub-accounts will be performed according to the priority of sub-accounts specified in clause 135.8 of these Rules.

158.4. **Rule No. 4:** Conversion between sub-accounts of a multi-currency card shall be carried out if there are sufficient funds in the currency sub-accounts involved in the conversion.

159. Examples of Conversion on Multicurrency Cards. The conditions (table below) accepted for settlements are indicated as an **illustration** of examples of processing card transactions on multicurrency cards:

Example No. 1. Expenditure transaction – transfer to another card or via QR code for KGS 7,000:

Balances on sub-accounts in nominal value (current	KGS	USD	EUR	RUB
balance):	5 000	150	150	1 000
available balance, KGS	33 800			
Payment card exchange rates: purchase		*85*	*100*	*1,05*
sale		*90*	*110*	*1,20*
Expenditure transaction with instant posting, KGS	7 000	card-to-card or QR transfer		
Instant posting sub-account normalization:	KGS	USD	EUR	RUB
additional collection	5 000	24		
Balances on sub-accounts in nominal value after	KGS	USD	EUR	RUB
instant posting:	0	126	150	1 000
available balance, KGS	26 800			

Posting/normalization: KGS 5,000 will be debited from the KGS sub-account, and the remaining KGS 2,000 will be normalized from the USD sub-account at the Bank's commercial exchange rate (Buy). Normalization calculation: KGS 2,000 / 85 = USD 24. Available balance: KGS 26,800.

Example No. 2. Expenditure transaction –Purchase at a POS-terminal /Cashing-out at an ATM for KGS 6,000:

Balances on sub-accounts in nominal value (current	KGS	USD	EUR	RUB	
balance):	5 000	150	150	1 000	
available balance, KGS	33 800				
Payment card exchange rates:	*KGS*	*USD*	*EUR*	*RUB*	
purchase		*85*	*100*	*1,05*	
sale		*90*	*110*	*1,20*	
Expenditure transaction without instant posting, KGS	6 000	purchase at a POS terminal or cashing-out at an ATM			
Available balance at the authorization stage (before	KGS	USD	EUR	RUB	in processing
normalization)	-1 000	150	150	1 000	6 000
available balance, KGS	27 800				
Sub-account normalization after the Bank receives a financial document for the transaction (KGS 6 000):	KGS	USD	EUR	RUB	
additional collection	0	12			
Balances on sub-accounts in nominal value after	KGS	USD	EUR	RUB	in processing
posting:	0	138	150	1 000	0
available balance, KGS	27 800				

Authorization: The KGS transaction shall be debited from the KGS sub-account because of the insufficiency of funds in the sub-account resulting in a temporary overlimit of (minus) -KGS 1,000 in the currency sub-account. The purchase amount of KGS 6,000 KGS shall be blocked. Available balance: KGS 27,800.

Post/Normalization: The remaining amount of KGS 1,000 will be normalized from the USD sub-account at the Bank's commercial exchange rate (Buy). Normalization calculation: KGS 1,000 / 85 = USD 12. Available balance: KGS 27,800.

Example No.3. Expenditure transaction – purchase at a POS-terminal / Cashing-out at an ATM for KGS 6,000, then transfer via QR code for KGS 8,000:

Balances on sub-accounts in nominal value (current balance):	KGS	USD	EUR	RUB	
	5 000	150	150	1 000	
available balance, KGS	33 800				
Payment card exchange rates:	*KGS*	*USD*	*EUR*	*RUB*	
purchase		*85*	*100*	*1,05*	
sale		*90*	*110*	*1,20*	
Expenditure transaction without instant posting, KGS	6 000	purchase at a POS terminal or cashing-out at an ATM			
Available balance at the authorization stage (before normalization)	KGS	USD	EUR	RUB	in processing
	-1 000	150	150	1 000	6 000
available balance, KGS	27 800				
Expenditure transaction with instant posting, KGS	8 000	card-to-card or QR transfer			
1) Sub-account normalization with instant posting:	KGS	USD	EUR	RUB	
additional collection	5 000	35			
Balances on sub-accounts in nominal value after instant posting:	KGS	USD	EUR	RUB	no processing
	-6 000	115	150	1 000	
available balance, KGS	19 800				
2) Sub-account normalization after the Bank receives a financial document for the transaction (KGS 6 000):	KGS	USD	EUR	RUB	
additional collection		71			
Balances on sub-accounts in nominal value after posting:	KGS	USD	EUR	RUB	in processing
	0	44	150	1 000	0
available balance, KGS	19 800				

Authorization for a purchase of KGS 6,000: The KGS transaction shall be debited from the KGS sub-account because of the insufficiency of funds in the sub-account, resulting in temporary overlimit of (minus) - KGS1,000 in the currency sub-account. The purchase amount of KGS 6,000 shall be blocked. Available balance: KGS 27,800.

When making a transfer (including via QR code) of KGS 8,000, an instant posting occurs: the KGS transaction shall be debited from the KGS sub-account, resulting in a temporary overlimit of (minus) - KGS 6,000 in the currency sub-account. The remaining amount of KGS 3,000 will be normalized from the USD sub-account at the Bank's commercial exchange rate (Buy). Normalization calculation: KGS 3,000 / 85 = USD 35. Available balance: KGS 19,800.

Then the purchase transaction for the amount of KGS 6,000 shall be posted: according to priority, if there are insufficient funds in the KGS sub-account for the amount of KGS 6,000, the amount will be normalized from the USD sub-account at the Bank's commercial exchange rate (Buy). Normalization calculation: KGS 6,000 / 85 = USD 71. Available balance: KGS 19,800.

Example No.4. Conversion inside a multi-currency card for USD 120:

Sub-account balances in nominal value (current balance):	KGS	USD	EUR	RUB
	5 000	150	150	1 000
available balance, KGS	33 800			
Payment card exchange rates: purchase		*85*	*100*	*1,05*
sale		*90*	*110*	*1,20*
Conversion with instant posting, USD	120	Conversion from USD account to EUR - USD 120		
Sub-account normalization with instant posting:	KGS	USD	EUR	RUB
conversion		-120	93	
Sub-account balances in nominal value after instant posting:	KGS	USD	EUR	RUB
	5 000	30	243	1 000
available balance, KGS	32 873			

Posting/normalization: When converting USD 120 to euros from a USD sub-account to a EUR sub-account, the conversion will be based on the dollar buy/euro sell rate: USD 120 * 85 / 100 = EUR 93. Available balance: KGS 32,873.

Example No.5. Expenditure transaction – Cashing-out abroad at an ATM for GBP 250:

Sub-account balances in nominal value (current balance):	KGS	USD	EUR	RUB	
	5 000	150	150	1 000	
available balance, KGS	33 800				
Payment card exchange rates:	*KGS*	*USD*	*EUR*	*RUB*	
purchase		*85*	*100*	*1,05*	
sale		*90*	*110*	*1,20*	
VISA rates adjusted for OIF:	*GBP / USD*				
purchase	*0,83*				
sale	*0,85*				
Expenditure transaction without instant posting, GBP	250	GBP cashing-out at an ATM			
Acquirer's commission for cashing-out	0,5%	commission of the bank, which the ATM belongs to			
Issuer's commission for cashing-out	1%	Optima Bank's commission: 1%, min. KGS 250			
Calculation of the amount to be debited from the sub-account including the acquiring bank's commission, USD	302,71	GBP debiting from a dollar sub-account at the VISA rate with consideration of OIF			
Calculation of the total amount to be debited from the sub-account including the issuer's commission, USD.	305,74	GBP debiting from a dollar sub-account at the VISA rate with consideration of OIF			
Available balance at the authorization stage (before normalization)	KGS	USD	EUR	RUB	in processing
	5 000	-156	150	1 000	25 988
available balance, KGS	7 812				
Sub-account normalization after the Bank receives the financial document for the transaction (USD 305.74):	KGS	USD	EUR	RUB	
additional collection	5 000	0	90		
Sub-account balances in nominal value after posting:	KGS	USD	EUR	RUB	in processing
	0	0	60	1 000	0
available balance, KGS	7 034				

ATM cashing-out authorization for GBP 250: a transaction other than KGS processed in USD shall be debited from a USD sub-account for USD 305.74, including cashout fees and the VISA exchange rate adjusted for OIF. Due to insufficient funds in the sub-account, a temporary overlimit of (minus)-156 USD shall be created in the currency sub-account. The cashout amount, including fees, shall be blocked at the Bank's exchange rate (KGS 25,988 blocked). Available balance: KGS 7,812.

Posting: according to priority, if funds in the USD sub-account are insufficient for the amount of USD 156, the transaction will be normalized from the KGS sub-account, then from the EUR sub-account at the Bank's commercial exchange rate. Normalization calculation: KGS 5,000 / 85 (dollar purchase) = USD 56; EUR 90 * 100 (EUR purchase) / 90 (USD sale) = USD 100. Available balance: KGS 7,034.

Example No.6. Receipt transaction – crediting EUR 300 transfer via VISA Direct, conversion inside a multicurrency card for EUR 260:

Sub-account balances in nominal value (current balance):	KGS	USD	EUR	RUB
	5 000	150	150	1 000
available balance, KGS	33 800			
Payment card exchange rates: purchase		*85*	*100*	*1,05*
sale		*90*	*110*	*1,20*
Receipt transaction with instant posting, EUR	300	incoming transfer via Visa Direct (EUR 300)		
Bank commission for crediting	0.5%	of the amount of the incoming transfer		
1) Sub-account normalization with instant posting:	KGS	USD	EUR	RUB
inflow			299	
Sub-account balances in nominal value after instant posting:	KGS	USD	EUR	RUB
	5 000	150	449	1 000
available balance, KGS	63 650			
Conversion with instant posting, EUR	260	Conversion from EUR account to USD - EUR 260		
2) Sub-account normalization with instant posting:	KGS	USD	EUR	RUB
Conversion		289	-260	
Sub-account balances in nominal value after instant posting:	KGS	USD	EUR	RUB
	5 000	439	189	1 000
available balance, KGS	62 206			

Posting/normalization for an incoming Visa Direct transfer of EUR 300: Since the incoming transfer is in EUR, the transfer shall be credited to the EUR sub-account minus a crediting fee of EUR 299. The incoming transfer amount should not be blocked. Available balance: KGS 63,650.

Posting/normalization for a conversion of EUR 260: The conversion from the EUR sub-account to the USD sub-account shall be performed at the euro buy/dollar sell rate: EUR 260 * 100 / 90 = USD 289. Available balance: KGS 62,206.