Optima Bank

"FOR EXTERNAL USE"

Appendix No. 20
to the Comprehensive Agreement on banking services
rendered to individuals in "Optima Bank" OJSC

RULES FOR USE OF BANK CARDS ISSUED BY "OPTIMA BANK" OJSC

Optima Bank

CONTENTS

Terms and Definitions

1. **Authorization** is a procedure of the issuer's confirmation of the cardholder's authority or authorship to conduct an operation using a bank payment card (transaction), which results in the issuer's obligation to an acquirer to execute a settlement document drawn up using the card of the aforementioned issuer. Authorization may be automated (via terminal) and voice (via telephone communication). If an issuer and an acquirer are one and the same person on the operation conducted with the use of a bank payment card, authorization shall be the permission granted by an issuer to a client to conduct this operation.
2. **Bank payment card (hereinafter referred to as a card)** is a payment instrument used for settlements when purchasing goods, services, receiving cash in the national and foreign currencies, making money transfers, as well as for settlements in the form of e-money through the terminals, the ATMs or other devices (peripheral devices). The card issued under the card account in the name of a card account holder shall be the main card, and the cards issued under the card account in the name of third parties shall be the additional cards. The card issued to replace the main card shall also be the main card upon expiry of the main card, as well as in case of loss or theft thereof. The cards are divided into debit and credit cards, issued in the form of a plastic card or in electronic form, or tokenized / digitized version of the card stored in a mobile device and contributing to conducting contactless operations using NFC technology.
3. **ATM** is a hardware and software complex to issue and/or accept cash, record cash to a card, receive information on transactions conducted by a cardholder, make non-cash payments and issue a card-receipt for all types of transactions made. ATM is a banking equipment and is designed to conduct card transactions by a cardholder independently without involved authorized employee of a commercial bank.
4. **Card blocking** is a full or temporary prohibition to conduct card operations imposed on the initiative of a cardholder, the Bank or a company by one of the methods established by the payment system. Withdrawal of a payment card when it is submitted for servicing shall be provided in case of complete prohibition.
5. **Friendly fraud** is intentional or unintentional declassification and/or transfer of a card or card details to the persons close to a cardholder (relatives, friends, colleagues, etc.), and, as a result, implementation by these persons of the card operations unauthorized by the cardholder. The cardholder shall be responsible for such operations.
6. **Cardholder** is a Bank's client, an individual authorized by a legal entity/individual entrepreneur-owner of a card account being entitled to conduct card operations subject to the Agreement with the Bank, including the holders of the main and additional cards opened under the card account.
7. **Card account** is a bank account with reflected operations being conducted with the use of a card or its details.
8. **Card operation** is an operation using a card and/or its details and other remote service tools (e.g. purchase of goods, services, transfer of funds, currency exchange or cash withdrawal), which results in changed balance of funds on the cardholder's card account.
9. **Card compromise** is the fact that a third party, other than a cardholder, has access to confidential information related to a card, its details or a card account, passwords and logins from Optima 24, as well as suspicion of such access.
10. **Contact Centre** is a subdivision of the Bank, being a round-the-clock contact centre, established to process remote applications of existing and potential clients of the Bank. **Phone numbers of the Contact Centre: (312) 90 59 59, 0-800-800-00-00*** (calls are free of charge from fixed phones of "Kyrgyztelecom" OJSC). **Short number** for the subscribers of O!, Beeline and MegaCom mobile networks: **9595** (call is free).
11. **Single-currency card** is a card with one currency in the card account.

12. **Mobile device** is any portable device of a cardholder with installed Payment mobile service and supported NFC technology (for example, smartwatch, smartphone, tablet, etc.).
13. **Multicurrency card** is a card, which provides the possibility to maintain a card account with several currencies being sub-accounts linked to the main sub-account. A multi-currency card contains 4 currency baskets (sub-accounts) in the following currencies: Kyrgyz soms (hereinafter referred to as KGS), US dollars (hereinafter referred to as USD), Euros (hereinafter referred to as EUR), Rubles (hereinafter referred to as RUB) with the main sub-account in the currency of account management - KGS. The available amount and the balance of a multi-currency card is displayed in the currency of the main account by recalculating the balances of currency sub-accounts at the Bank's commercial exchange rate (purchase) effective on the date of requesting the available balance in the card account.
14. **Multiplier** is a coefficient in the form of a percentage surcharge to the amount of authorization for a card operation applied by the Bank to mitigate the risk of debt on a card account in case of a card operation conducted in a currency other than the currency of the card account. Final mutual settlements on a card operation (writing the card operation amount off the cardholder's card account) shall be made without application of the multiplier. The types of card operations, for which the multiplier is applied shall be determined by the Bank independently. The multiplier amount is set by the Bank depending on the market situation in the foreign exchange market and can be unilaterally changed by the Bank. Information on the multiplier size is available on the Bank's corporate website www.optimabank.kg. More detailed examples of multiplier use can be found in Chapter 12.
15. **Normalization** is funds flow in the sub-accounts of a multi-currency card when conducting conversion operations.
16. **Payment system of settlements using bank payment cards** (hereinafter referred to as the payment system) is a system of settlements using cards issued and maintained in compliance with the requirements of the operators of these systems and the laws of the Kyrgyz Republic. The payment system establishes certain rules for mutual settlements on card payments between the system participants. Payment systems are divided into local (e.g. MIR, national (Elcart) and international (Visa, MasterCard, etc.).
17. **Mobile Payment Service** is the Provider's software provided to a cardholder under a separate agreement (contract) concluded between a provider and a cardholder being an application installed in the mobile device to tokenize the cards, delete the token, and use the token to conduct operations. Functionality of the Mobile Payment Service, the terms of its use and the procedure for providing a cardholder with the rights to use it shall be determined by the Provider. If the Bank acts as a Provider, the Bank's Mobile Application shall be the Payment Mobile Service. Such payment mobile services include the systems of mobile payments via e-wallets (Google Pay, Garmin Pay, etc.), which, combined with the software in the mobile device possessing NFC technology, provide an opportunity to pay for purchases and withdraw funds.
18. **Posting** (or clearing) is the process of collection, processing, confirmation of payments and calculation of mutual obligations of the payment system participants for the card operations conducted by mutual offset based on the conditions of the balance of payments and represent the final financial settlement on the card operation.
19. **Processing** is licensed activity, which includes interrelated processes of receiving, processing and issuing financial information to the payment system participants.
20. **Processing Centre** (hereinafter referred to as PC) is a legal entity implementing processing.
21. **Provider** is a legal entity that is a manufacturer (developer) of the Mobile Payment Service, which provides information and technological interaction on the basis of the payment systems rules and/or subject to a separate agreement with the payment system in the course of formation, maintenance and use of the token to conduct card

operations. In addition, the Bank may be a provider, when a cardholder uses the Bank's software;

22. **Recurrent payments** are regular card operations (payments) conducted in the Internet or card operations (payments) made through the remote banking services using previously saved card details, which do not require involvement and confirmation by a cardholder (e.g., subscription payment for services of the Internet resources, payment for goods or services in instalments, regular "auto payments").
23. **Social engineering** is a set of psychological and sociological techniques, methods and technologies that help the fraudsters to obtain protected/confidential information of a cardholder in order to steal funds.
24. **Stop list** is a list of blocked cards for which all and/or certain types of operations have been totally or temporarily suspended.
25. **Card tokenization** is a technology provided by the payment systems to exchange confidential card data for a special non-sensitive equivalent (token) to protect card details. Mapping of card and token details is created in the process of tokenization to provide exact identification of the card used for operations using the token. Operations conducted using the token are equivalent to the operations conducted by a cardholder using the card or its details.
26. **Token** is card digital representation being formed upon card tokenization and stored in encrypted form in the secure cloud storage of the payment system, as well as stored in the memory of the mobile device.
27. **Phishing** *(phishing derived from fishing)* is a type of Internet fraud aimed at gaining access to the cardholder's confidential and protected information - card details and passwords, and/or login and password from the remote banking systems. Most often, the fraudsters win a cardholder's confidence and obtain card details and passwords through the social networks and messengers. The main method used is mass mailings, as well as on behalf of the bank or large and well-known companies, which may contain links to false websites being outwardly indistinguishable from the real ones. In such mailings or messages, a cardholder is often asked to update or confirm correctness of the personal information by providing links to a false website where the cardholders voluntarily enter their credentials / card details. If the fraudsters manage to obtain this information, it results in theft of funds from the card account. The cardholder is responsible for such operations.
28. **Acquirer** is the Bank, which has obtained a permit for acquiring, owner of a peripheral devices network, which provides an opportunity to conduct authorization or transactions through its peripheral devices in accordance with the technology and regulations of the relevant payment systems and the laws of the Kyrgyz Republic.
29. **Acquiring network** includes all devices of the acquiring banks - payment system participants to conduct card transactions: ATMs; POS terminals installed in the banks' branches; trading POS terminals installed in the retail and service outlets; payment terminals; automatic deposit machines; e-commerce.
30. **E-commerce** is the activities of the retail and service outlets entered into contractual relations with an acquirer to conduct financial/trading non-cash card operations through the websites using computer networks.
31. **Cardholder's embossed name** is a cardholder's surname and name in Latin transcription printed on the front side of a card.
32. **Issuer** is a Bank issuing cards in accordance with the technology and rules of the relevant payment systems and the laws of the Kyrgyz Republic.
33. **CVV2-code** *(Card verification value)* is a three-digit code for card verification requested for online payment and other operations.
34. **E-PIN** (electronic PIN code) is a temporary code provided to a cardholder for further independent installation of a permanent PIN code in the Bank's devices.
35. **Near Field Communication (NFC)** is a short-range wireless data transmission technology to provide data exchange between devices, and/or card and devices. Most payment systems require from the cards to support contactless payment technology (NFC).
36. **PIN code** *(Personal identification number, hereinafter referred to as* PIN-code*)* is a personal identification number to authenticate the user for making an operation. PIN code is a card access password and refers to confidential and protected information,

which is not subject to disclosure to third parties other than a cardholder. PIN code of the card is assigned **to identify** a cardholder's identity during card operations.

37. **POS terminal** *(point-of-sale)* is a terminal to accept payment for goods and services in the retail and service outlets using a card and other remote service tools.
38. **3D Secure password** is a secure protocol used as an additional security level for two-factor user authentication for card-not-present transactions. The technology was developed for the Visa payment system to improve the security of Internet payments under the Verified by Visa (VbV) service. The 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 to be used for online purchases.
39. **QR code** is a two-dimensional barcode symbol to transmit payment data used for non-cash payments and transfers.

Chapter 1. General Provisions.

40. The rules for use of cads issued by "Optima Bank" OJSC (hereinafter referred to as the Rules) define the terms of use, servicing and security measures in conducing operations with payment system cards issued by "Optima Bank" OJSC (hereinafter referred to as the Bank).
41. These Rules are 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.
42. These Rules are standard (typical) and shall not be subject to change by a cardholder. The Bank may revise these Rules unilaterally if necessary by placing information about introduced amendments on the corporate website https://www.optimabank.kg/ru/press-centre/all-news.html in the "News" section, taking into account the term established by the current laws of the Kyrgyz Republic to inform about amendments to be intorduced.
43. These Rules shall be an integral part of the Comprehensive Agreement on banking services rendered to individuals in "Optima Bank" OJSC (hereinafter referred to as the "CABS").

Chapter 2. Procedure for Card Issue and Storage.

44. The Bank shall issue a card directly to a cardholder or to an authorized person acting on the basis of a certified power of attorney.
45. Transfer of a card to third parties who are not the cardholders for use or as a pledge shall be prohibited.
46. A card (including a PIN envelope) shall not be delivered outside the Kyrgyz Republic according to the current laws of the Kyrgyz Republic.
47. The front side of a card contains:
    - 47.1. Bank's logo;
    - 47.2. payment system logo;
    - 47.3. embedded chip - an integrated microchip with encoded information;
    - 47.4. card number consisting of 16 digits;
    - 47.5. embossed name of a client (surname and name of a cardholder in Latin alphabet or initials, if the client's surname and name exceeds 22 Latin characters);
    - 47.6. card date of expiry;
    - 47.7. client's code in the Bank (client ID)
48. The reverse side of a card contains:
    - 48.1. magnetic stripe

48.2. space for client's signature (optional);
48.3. hologram with the image of a dove (Visa cards);
48.4. number of the Bank's Contact Centre;
48.5. verification code (CVV2);
48.6. unique bank card number (card id) - optional.

49. A cardholder shall protect a card from mechanical damage and from electromagnetic fields effect (car alarms, cell phones, computers, pass frames at the airports, in the banks, stores, etc.) to avoid damage to the magnetic stripe.
50. Generally, it is forbidden to make any physical impact with any object on the surface of a PIN envelope, chip or a card as a whole. If a card, chip or PIN envelope are damaged as a result of intentional, negligent or unintentional actions of a cardholder, a card shall be reissued at the cardholder's expense according to the current Bank's Tariffs.
51. The amount of commission fees and tariffs for card issue and maintenance, as well as debit and credit limits of card operations, limits on money transfer operations, limits on fundsconversion in the context of currency and/or the type of bank account, limits on contactless payments, which may be conducted without entering PIN-code, shall be determined by the Bank's Tariffs. Information on the limits, commission fees and tariffs is available on the Bank's corporate website www.optimabank.kg.
52. For security reasons the Bank does not recommend to set huge amounts of limits for a long period of time. A cardholder shall be responsible for the consequences of non-compliance with this clause.
53. A card account is intended for the following card operations only:
    53.1. crediting/withdrawal of cash and non-cash funds of non-commercial nature to/from the individuals card accounts;
    53.2. crediting of cash and non-cash funds of commercial nature to the legal entities card accounts;
    53.3. withdrawal of funds from the card accounts of the individuals and the legal entities to pay for goods, services of the retail and service outlets and other third parties;
    53.4. withdrawal of funds from the cardholders card accounts to pay the Bank's commission fees and credit(s) debt (including technical overdraft);
    53.5. withdrawal of funds from the card accounts of the individuals and the legal entities to repay debts to the Bank arising in the process of issuing and maintenance of a payment card, including in excess of the balance of funds on the card account;
    53.6. crediting and withdrawal of funds in the amount of transfer operations from the card accounts of the individuals and the legal entities (including the Bank's commission fees according to the current Tariffs);
    53.7. withdrawal of funds from the card accounts of the individuals and the legal entities on the basis of enforcement documents stipulated by the current laws of the Kyrgyz Republic.
54. Remote services can be rendered to the cardholders through the Contact Centre, the Bank's corporate website www.optimabank.kg and the Bank's remote banking systems (Optima 24). Service conditions shall be regulated by the Bank's internal regulatory documents and tariffs.
55. The Bank shall be entitled to provide a cardholder with the opportunity to implement tokenization for further card operations using the token (mobile device in which the token is kept) in accordance with the procedure and on the terms and conditions stipulated by the CABS.
56. At the initiative of a cardholder, a card may be added to payment mobile services (e-wallets) to make payments and withdraw funds using tokenization technology and make payments via mobile device using NFC module. In this case, when conducting an operation using the token, a cardholder shall be verified by entering the cardholder's password in the Mobile Device and, if necessary, by making additional entry of PIN-code (in case of payments through POS terminal or ATM).

57. In order to ensure the possibility to conduct card operations with the use of contactless payment technology (NFC), including for the purpose of providing the Cardholder with information on card operations in the Bank's mobile application, the Bank shall be entitled to transfer information about the amount of the card operation, date and time of conducting thereof, type of operation, currency code, authorization status for its processing to the Providers (Google Ireland Limited, Garmin Ltd., etc.) of the software for payment mobile services (Google Pay, Garmin Pay, etc.).
58. When the Cardholder uses NFC technology, the Bank shall not be responsible:
    58.1. for the consequences that may arise if the information about the tokenized card, as well as about the balance of such card, displayed on the screen of the device, becomes known to third parties;
    58.2. for the situations resulted from failures in operation of the systems that ensure reception, processing and transmission of data on the card operations for reasons beyond the Bank's control, for operation of Google Pay, Garmin Pay service.
59. Conducting of card operations by the Cardholder using mobile payment services (Google Pay, Garmin Pay, etc.) may be limited by the functionality of the Cardholder's mobile device software, as well as the Bank's mobile application.
60. The Cardholder is aware of increased risk and understands that when using mobile payment services (Google Pay, Garmin Pay, etc.) access to the Cardholder's mobile device directly affects the possibility of unauthorized card operations and, therefore, the Cardholder shall be independently responsible for the confidentiality of single-use passwords, passwords, PIN, and other means of access of the Cardholder to the mobile device, mobile application, card.
61. The Token is issued for the period up to 6 (six) years. The Token can be removed by the Cardholder independently in the mobile device or through application to the Bank. The Token can be blocked through application to the Bank.

Chapter 3. PIN code.

62. A card shall be issued to a cardholder together with a special envelope where the PIN code is printed. A cardholder is recommended to open an envelope immediately upon receipt of a card, make sure that the PIN code is printed legibly, memorize the PIN code and further keep the envelope separately from the card and in a place inaccessible to third parties.
63. The PIN code is unknown to the Bank's employees and must be kept secret by a cardholder during the whole time of card use.
64. A card may be issued with an electronic PIN code (hereinafter referred to as the E-PIN). E-PIN shall be set according to Chapter 11 of these Rules.
65. Lost PIN code on paper shall not be restored, and the card shall be reissued according to the Bank's Tariffs. Lost electronic PIN code (E-PIN) can be "reset" upon written application of a cardholder.
66. It is recommended to follow certain rules to ensure PIN code secrecy:
    66.1. it is prohibited to write a PIN code on the card;
    66.2. it is prohibited to keep together a PIN envelope with a PIN code and a card (in one place);
    66.3. do not allow third parties to see the PIN code digits typed on the keyboard of the device (ATM, terminal);
    66.4. do not make any mistakes when entering PIN code digits. In case of incorrect PIN code entering (three times in a row) limit is set for PIN code entering attempts, the card shall be automatically blocked and further conducting a card operation is impossible. In such case a cardholder is recommended to apply to the nearest branch of the Bank or to the Bank's Contact Centre to reset the attempts of incorrect PIN code input.

67. The card operations confirmed by PIN code input are considered by the Bank to have been conducted by the cardholder and shall not be subject to dispute due to unauthorized access to the card account and/or fraud.

Chapter 4. Card Use in the Retail and Service Outlets.

68. Non-cash payment for goods, services and works in the retail and service outlets (hereinafter referred to as the RSO) shall be made within set card limit and the limit in the acquiring device of the acquiring bank.
69. The maximum amount of one operation and the number of operations per day in the acquiring device of the Bank and/or third-party acquiring bank shall be determined by the Bank's Tariffs, the acquiring bank's policy and the payment systems' rules.
70. Payment for goods and services may be made by:
    - 70.1. reading the card magnetic stripe and entered PIN code;
    - 70.2. reading the card magnetic stripe without entering the PIN-code
    - 70.3. reading the card chip and entered PIN code;
    - 70.4. reading the card chip without entering the PIN code;
    - 70.5. reading the contactless chip through the contactless chip reader without entering the PIN code within set limits according to the Tariffs of the Bank, the acquiring bank and/or the payment systems' rules;
    - 70.6. reading the contactless chip through the contactless chip reader with entering the PIN code for amounts exceeding set limit according to the Tariffs of the Bank, the acquiring bank and/or the payment systems' rules;
    - 70.7. use of the card token without entering the PIN code (within set limits) or with entering the PIN code (for the amounts exceeding set limit). The limits shall be regulated by the policy of the Bank, the acquiring bank and/or the payment systems' rules;
    - 70.8. reading the QR code to make money transfer or non-cash payment for goods or services of the retail and service outlet.
71. Non-cash payment for goods and services in the RSO can be made either online or offline, depending on the settings of the acquiring bank's devices. A cardholder shall be responsible for the operations being conducted offline. At the same time, offline payment for goods and services at the POS terminals owned by the Bank shall be prohibited by default.
72. Payment for goods and services, as well as withdrawal of funds with chip reading error in the devices supporting chip technology shall be prohibited (Fallback transactions).
73. The Bank's cards are issued with the possibility of contactless payments (PayWave / NFC), which cannot be disabled at the initiative of a cardholder due to the requirement of the payment systems on mandatory support of contactless payment technology.
74. All card transactions in the RSO must be conducted in the presence of a cardholder. This is necessary to reduce the risk of unauthorized obtaining of the cardholder's personal data indicated on the card. Some RSO may request an identity document. Therefore, the Bank recommends to have a passport or other identity document on hand when making payments by card.
75. All Points of sales are equipped with the payment systems logos to inform the cardholders about the possibility to maintain a particular card in this RSO, as well as about the possibility to accept payments with the use of QR code.
76. To conduct card operations, a cardholder should insert / attach a card or bring a mobile phone, in case of card tokenization, to a device (ATM, payment terminal, POS terminal) or scan a QR code through Optima 24 mobile application in case of payment by QR code.
77. In order to conduct card operations through the RSO or the Bank, an employee of the RSO or the Bank implements authorization by means of a POS terminal. The card is placed or attached to the POS terminal reader. The employee of the RSO or the Bank

enters the card operation amount on the keyboard of the POS terminal. In some cases, for example, when the limit of the card operation allowed to be conducted without PIN code entering is exceeded, a cardholder may be requested to enter the PIN code on a special keyboard. When the correct PIN code is entered and there are sufficient funds on the card account, a receipt in duplicate is printed to confirm card operation successful completion. When contactless payment technology or a tokenized card are used, the Cardholder must bring the card or mobile phone at a minimum distance to a POS-terminal or ATM to conduct a card operation or scan a QR code via Optima 24 mobile application when making payment by QR code.

78. A cardholder is recommended to:
    78.1. make sure that the data indicated in the receipt are correct;
    78.2. take one copy of the POS terminal receipt until the moment of full settlement on this card operation, as well as for the purpose of reconciliation of card account dedit operations.
    78.3. make sure that the data indicated in the receipt are correct;
    78.4. take one copy of the POS terminal receipt until the moment of full settlement of the card transaction, as well as for the purpose of reconciliation of card account debit operations.
79. A cardholder's signature should not be affixed on the receipt for the operations confirmed by PIN code, as well as for the contactless operations conducted without entering PIN code within set limit.
80. Requirements for receipt signing in conducting operations in the acquiring network of the third-party acquirer shall be determined by the policy of this acquirer.
81. A cardholder shall be prohibited to sign the receip of POS terminal, in which the amount of purchase (goods/services) is not indicated.
82. According to the payment systems rules the RSO shall not be entitled to overvalue the cost of goods and services when payment is made by card as compared to cash payment. If such cases are revealed, a cardholder is recommended to notify the Bank.
83. Purchase or service paid with a card shall bereturned with the RSO consent. For this purpose, the RSO employee shall initiate a "purchase return" operation at the POS terminal at the cardholder's request. Refund of the purchase amount in cash shall not be provided.
84. The amount of the repayable card operation will be returned to the card account on the next banking day after the Bank receives the operations register on conducted repayable card operation. This information should be taken into account when calculating the available card amount.

Chapter 5. Using a Card at an ATM.

85. Cash is generally taken off a card in the currency of the residence country. Some acquiring banks may impose additional fees for cash withdrawals. Moreover, in some countries, the frequency and maximum amount of cash withdrawals from the card account may be restricted by the laws.
86. Prior to use the ATM, it is necessary to inspect it for the presence of unusual devices: unevenly installed PIN keyboard, overlays in the card receiver, availability of mini-video cameras directed at the PIN keyboard, overlays above the ATM screen and other suspicious devices. If a cardholder has discovered availability of unusual devices, it is recommended not to use this ATM and inform the Contact Centre of the acquiring bank by the numbers indicated on the ATM.
87. To receive funds or other services at the ATM, it is necessary to insert a card into the ATM card-receiver or bring the mobile phone in case of card tokenization, enter the PIN-code, select the appropriate menu and follow the instructions on the screen.
88. In order to cancel the service, it is necessary to cancel the operation by pressing the button "Cancel".

89. When operating an ATM, it is not allowed to use physical force to insert a card into the ATM. If a card is not inserted, such ATM should not be used.
90. When entering the PIN-code, it is necessary to make sure that the PIN-code is not seen by third parties. After 3 (three) attempts to enter an incorrect PIN code, a card shall be blocked and may be detained (seized) by the ATM.
91. When the command “TAKE YOUR CARD” appears on the screen - it is necessary to take a card immediately, otherwise in 15-30 seconds the card may be detained by the ATM.
92. When the command “TAKE YOUR CASH” appears on the screen - it is necessary to take cash immediately, otherwise in 20 seconds the cash will be detained by the ATM.
93. It is always recommended to take a receipt of the operation conducted through the ATM, as the receipt is a document confirming the card operation in case of dispute resolution. Due to the cardholder related information available in the receipt, it is recommended to take the receipt and not to leave it near the ATM.
94. Reasons for unsuccessful card operations at ATM may be the following:
    94.1. requested amount cannot be issued at the moment with the banknotes available in the ATM cassettes. In such situation it is recommended to request the amount multiple of the banknotes minimum denomination indicated in the instruction (on-screen menu) for this ATM;
    94.2. requested amount exceeds the one-time withdrawal limit determined by the ATM technical characteristics. In such situation it is recommended to divide the requested amount into parts and repeat the operation several times;
    94.3. requested amount exceeds the available balance of the card account (taking into account the Bank’s and/or acquiring bank’s commission fee). In such a situation it is recommended to request a smaller amount. The available balance of the card account can be clarified also by requesting the operation of the funds balance available on the card through the ATM menu.
95. If a card has been seized by the ATM, it is necessary to make sure that the card is really detained (ATM continues to serve other clients or has stopped functioning). Otherwise, the ATM may return the card to another client and/or give him/her the requested funds.
96. If a card has been seized by the ATM, a cardholder is recommended to block the card immediately by any convenient way: by contacting the Bank’s Contact Centre or independently via Optima 24. In the future, the Bank recommends issuing a new card with new card details, since is a card has been seized there is a risk of third parties having access to the card and/or card details.
97. If a card or funds have been detained by the ATM, it is necessary to immediately contact the Bank or the acquiring bank by the phone numbers indicated on the ATM.

Chapter 6. Use of a Card in the Internet.

98. Online card operations shall be conducted within set limit for the online payments and the limit of the acquiring bank.
99. Online payment for goods or services is made without the card physical presence, but with the use of card details, mandatory of which are the following: card number, card expiration date, cardholder’s embossed name. In addition, when making online payments , such card details as: CVV2, 3D Secure password in accordance with the Internet resource terms of service. Online payment for goods or services may also be made using the token.
100. The Bank issues the cards with access to online payments “by default”.
101. A cardholder may close access to online payments (except for the card operations made with 3D Secure password and recurring payments). For this purpose, a cardholder is recommended to apply to the Bank with a written application to disable access to online payments or to implement unassisted access disabling through Optima 24.

102. The Bank's VISA cards are connected to the 3D Secure service "by default". The 3D Secure protocol is not applied to the operations conducted with Elcart cards.

103. Payment for goods and services in the Internet resources that support 3D Secure technology and require entering a 3D Secure password is prohibited without entering a 3D Secure password (ECI 06).

104. Online card operations may be conducted in the following ways:

104.1. by using the token or specifying card details, mandatory of which are: cardholder's embossed name, card number, card expiration date, additionally CVV2 code, as well as 3D Secure password, may be requested on the web-sites supporting this technology;

104.2. by linking the card or token details to an Internet account, e-wallet, store, trading platform, Internet service or other resources in the Internet in accordance with the requirements and terms of service of the Internet resource. Recurring payments become possible if card/token has been linked. A cardholder shall be responsible for such operations until the card details are unlinked /the token is deactivated. In this case, a cardholder is advised to retain evidence of the card unlinking or token deactivation from recurring payments, which may be required if the disputes arise between a cardholder and the Internet resource.

105. Access for online operations exceeding the limit set by the Bank's tariffs shall be provided:

105.1. by the cardhold's applying to the Bank's branch and submiting a written application to change the current limits and restrictions for online payments;

105.2. independently by the cardholder through changing the current limits and restrictions for online payments in Optima24;

105.3. through the Contact Centre of the Bank after remote identification of a cardholder, whereby the current limits and restrictions for online payments can be changed for a period not exceeding 14 (Fourteen) calendar days.

106. Prior to conducting online operation, the Bank recommends a cardholder to:

106.1. check the card validity period and absence of card blocking;

106.2. make sure that a card is provided with sufficient funds;

106.3. make sure that a card has open access to online payments and that the limits for this type of card operation are sufficient;

106.4. make sure that the browser is provided with security updates;

106.5. make online payments only on verified websites with a positive reputation, as well as the websites that support the technology of secure online payments (3D Secure);

106.6. refrain from conducting operations on automatically redirected pages or pop-up windows to avoid Phishing. In most cases of phishing, the fraudulent clone website used for redirection looks identical to the real one and may differ only slightly from the original website, for example, partial URL;

106.7. in order to cancel online payment, in full or in part, a cardholder should first of all contact the Online Shop Customer Service to initiate payment refund.

107. When booking services on the Internet under the Travel & Entertainment category, such as: car rental, hotels, ticket purchase, etc., the Bank shall be entitled to block funds on the cardholder's card account until full settlement with the RSO has been completed. At that, the acquiring bank has the right to increase the amount of the final debit in the amount provided by the rules of the respective payment system. A cardholder shall be fully responsible for payment of the added value on card operations related to the Travel & Entertainment category.

Chapter 7. Card-related Security Measures.

108. Card number, PIN code, CVV2 code, card expiration date, cardholder's embossed name, client ID, 3D Secure and OTP passwords, as well as Optima 24 login and password are card details and confidential information, which provide

access to the cardholder's funds, and therefore belong to the category of protected information, which shall not be subject to declassification and transfer to third parties.

109. A cardholder shall be responsible for the safety of the card details and confidential information. Card details and confidential information must not be known to third parties. A cardholder is obliged to keep the card details and confidential information in a safe place being inaccessible for third parties.

110. The card, card details, secret information (PIN code, 3D Secure and OTP passwords, Optima 24 login and password), as well as a mobile phone containing tokenized card data must not be used by third parties.

111. A cardholder shall be responsible for compliance with clauses 107-109 of these Rules and for the consequences of non-compliance. A cardholder agrees that the Bank is entitled to block a card unilaterally if cases of violation of clauses 107-109 of present Rules are revealed.

112. A cardholder is forbidden to:

112.1. specify any data from the card details as well as Optima 24 password/login or mobile phone passwords on the card itself or keep them together or near the card;

112.2. leave a card and/or its details as well as a mobile phone or other cobfidential information in places accessible for copying and/or recording and/or use by third parties;

112.3. transfer card details (all or part threof), one-time passwords, as well as Optima 24 password/login and mobile phone passwords to third parties.

113. A chardholder shall bear full financial and material responsibility for the operations conducted with the use of a card and/or its details, including card passwords (PIN code, 3D Secure password), as well as for the operations conducted in Optima 24 (including operations conducted by means of QR code reading) or with the use of mobile phone (including tokenized operations) by third parties.

114. In case of loss, theft or suspected use of a card or its details by a third party, and/or receipt by a cardholder of an SMS/push notification with information about a card operation that he/she did not make, as well as in case of voluntary transfer of the mobile phone or confidential information to third parties, or in case of loss/theft of the mobile phone and/or compromise of the token, a cardholder must IMMEDIATELY contact the Bank through the official communication channels posted on the corporate website of the bank www.optimabank.kg to block the card / token or block the card independently through Optima 24 by selecting the appropriate reason for blocking, when this fact became known to a cardholder or a cardholder has suspicions about this fact. A cardholder shal be responsible for all card operations and his/her own actions or omissions and/or the actions or omissions of third parties until the card / token / Optima 24 is blocked.

115. Lost/stolen card or a card with compromised details or confidential information shall be subject to blocking and shall not be subject to re-issue, prolongation with preservation of basic card details. A cardholder should apply to the Bank for issue of a new card with new card details. Further use and/or unblocking of lost/stolen/ compromised cards is prohibited.

116. In case the lost/stolen/ compromised card was unblocked at the initiative of a cardholder, a cardholder shall bear full responsibility for possible subsequent unauthorized card debits. A cardholder loses the right to initiate dispute proceedings according to the payment systems rules.

117. A Client shall be obliged to comply with the following security requirements in order to exclude unauthorized operations using the token:

117.1. not to leave a mobile phone unsupervised;

117.2. to ensure proper security level in the mobile phone by using passwords and other possible ways of mobile phone locking/unlocking;

117.3. to ensure that fingerprints or other means of authenticating another person are not registered in the mobile phone, including facial recognition;

117.4. not to disclose the mobile phone password to third parties;

117.5. to delete all personal data and financial information from the mobile phone if its use is terminated;

117.6. to contact immediately the Bank by the phone number provided on the back of the card or through the official communication channels posted on the Bank's corporate website www.optimabank.kg in case of suspicion of any unauthorized use of the token, as well as if a mobile phone has been hacked, lost or stolen;

117.7. not to block any security features provided on the mobile device in order to protect the token;

117.8. to create a complex password on a mandatory basis and save only your biometric data (fingerprints, facial recognition and others) to use a mobile device;

117.9. to delete all personal data and financial information from the mobile phone when transferring the mobile phone to third parties or temporarily block it by contacting the Bank;

117.10. not to subject a mobile phone to privilege escalation operations/ hacking of the device operating system (jail break, rooting and others);

117.11. not to use mobile payment service when being connected to wireless public access networks;

117.12. not to make verification in the mobile payment service on the mobile phone(s) owned by the third party(ies).

118. A cardholder shall be fully responsible for any losses incurred due to conducted card operations within the framework of "Friendly Frod" and/or as a result of "Phishing" and/or "Social Engineering".

119. In order to track card account operations and timely respond and block the card in case of unauthorized access to the card account, a cardholder is recommended to connect to the service of receiving sms/push notifications on card operations. Payment for this service shall be made according to the Bank's Tariffs.

120. A cardholder is recommended not less than 1 (one) time a month to monitor the status of the card account. For these purposes, a cardholder can independently generate a statement in Optima 24, or apply to the Bank for a statement of card account.

Chapter 8. Card Transaction Processing.

121. A card operation within the payment systems rules shall be processed in two stages:

121.1. **Authorization** is 1st stage, which provides for funds blocking in the cardholder's card account; at the authorization stage, the available balance of the card account is reduced by the amount of the successfully authorized debit card operation.

121.2. **Posting** is the 2nd stage providing for acceptance of a card operation for accounting, which is made after receipt of all documents on this card operation. The final financial processing of a card operation is made at this stage, i.e. funds debiting or crediting on the cardholder's card account depending on the card operation type (debit or credit).

122. The amount of the card operation (including commission fees) shall be blocked on the cardholder's card account for the period between the date of authorization and posting of a card operation, and finally posted within 30 (thirty) calendar days.

123. Blocking of funds on successful card operations at the stage of authorization results in a decrease or increase of the available balance of the card account depending on the nature of the card operation: debit or credit. The debit card operations regularly result in a decrease of the available balance, however the credit card operations increase the available balance of the card account if it is provided for by the payment systems rules.

124. Operations shall be posted after receipt of an electronic financial document from the acquiring bank through the relevant payment system by the Bank.

125. If operations are not posted by the acquiring bank after expiration of the term specified in clause 122 of these Rules, the amount of funds on successful card operation automatically leaves the block (is unblocked) and becomes available to a cardholder for repeated use.

126. If the Bank receives late write-off (posting of operations within the term exceeding 30 calendar days) from the acquiring bank, the Bank shall be entitled to make acceptance-free write-off from the cardholder's card account equal to previously unblocked amounts of successful card operations.

127. At the authorization stage, the Bank may apply a multiplier when blocking the amount in the card account for successful card operations conducted in a currency other than the currency of the card account. Multiplier shall not be applied in card operations posting. Examples of multiplier application are given in Chapter 12 of these Rules.

128. Peculiarities of card operations processing <u>for single-currency cards</u>:

128.1. If a card operation is conducted in the acquiring network of the Bank in the currency different from the card account currency, processing of a card operation shall be made at the Bank's commercial rate established on the date of authorization.

128.2. If a card operation is conducted in the acquiring network of the third-party Bank in the currency different from the currency of the card account, processing of a card operation shall be made in USD at the exchange rate of the payment system on the **authorization** date of a card operation.

128.3. In case of technical overdraft on the card account, this debt shall be accounted at the commercial rate of the Bank (purchase) effective on the date of debt formation.

129. Peculiarities of card operations processing <u>for multi-currency cards</u>:

129.1. available balance is displayed in KGS by recalculating and summing up the balances of all currency baskets (sum of balances for KGS+USD+EUR+RUB sub-accounts) at the Bank's commercial exchange rate (purchase) in effect at the time of the cardholder's request for available card balance;

129.2. if a card operation is conducted in foreign currency funds shall be blocked in KGS at the commercial rate of the Bank (purchase) effective on the date of **authorization**.

129.3. mutual settlements on card operations conducted in foreign currency shall be made in USD at the exchange rate of the payment system on the date of **posting**;

129.4. in case of posting a card operation conducted in KGS, the funds shall be debited in KGS from the KGS sub-account (if the balance of the sub-account is sufficient).

129.5. in case of posting a card operation conducted in USD, funds shall be debited in USD from the USD sub-account (if the balance of this sub-account is sufficient).

129.6. in case of posting a card operation conducted in EUR, the amount of the card operation shall be debited in EUR from the EUR sub-account (if the balance of the sub-account is sufficient).

129.7. in case of posting a card operation conducted in foreign currency (other than USD), the amount of the card operation shall be debited in USD from the dollar sub-account at the rate of the payment system effective on the date of **posting** (if the balance of this sub-account is sufficient).

129.8. in case of insufficiency or absence of funds on the respective sub-account for posting a card operation, the Bank shall conduct automated **normalization** of this sub-account by converting the balances of funds on the balances of other card sub-accounts at the Bank's commercial rate. The procedure of foreign

currency sub-accounts normalization shall be as follows (in priority descending order): 1. KGS sub-account (KGS), 2. USD sub-account (USD), 3. EUR sub-account (EUR), 4. RUB sub-account (RUB).

129.9. In case of technical overdraft on the card account, this debt shall be accounted for in KGS at the Bank's commercial rate (purchase) effective on the date of its formation.

130. If a card operation is conducted in the currency other than the currency of the card account, the Bank shall convert funds into the currency of the card account without acceptance in accordance with Chapter 12 of these Rules. A cardholder hereby authorizes the Bank to implement such acceptance-free conversion of funds on the card account on the basis of these Rules and the Agreement and without any additional consent in any form on the part of a cardholder.

131. Early unblocking of funds on successful card operations, which a cardholder considers unsuccessful, shall be possible not earlier than 3 (three) calendar days from the date of authorization. Unblocking of a card operation shall be performed in an amount equal to the previously blocked amount in the currency of the card account. At the same time, the Bank shall be entitled to reject early unblocking of funds if:

131.1. if a cardholder has not provided or has not fully provided supporting documents from the RSO on unsuccessful card operation;

131.2. if according to the information contained in the supporting documents it is impossible to fully identify a card operation for which early unblocking is requested (there is no or inconsistent information on the amount of a card operation, currency of operation, date / time of operation, authorization code or other identifiers of a card operation available in the Bank's PC);

131.3. if the data of the relevant payment system does not confirm unsuccessful authorization of a card operation;

131.4. if a cardholder has not paid the commission fee for early unblocking of funds according to the Bank's Tariffs.

132. Funds shall be unblocked according to the data of the acquiring bank's authorization request received through the payment system in electronic form.

133. The card operation amount previously debited from the card account shall be refunded on the initiative of the acquiring bank/RSO in the full amount and currency of the original card operation. If the currency of the card account differs from the currency of the card operation, the card operation shall be cancelled completely at the Bank's commercial rate set on the date of the original card operation.

134. Partial cancellation of a card operation shall be made on the initiative of the acquiring bank /RSO in the partial amount and the currency of the original card operation. If the currency of the card account differs from the currency of the card operation, the card operation shall be cancelled partially at the Bank's commercial rate set on the date of the card operation partial cancellation.

135. If funds are received in the card in the form of credit card operations (credit and/or credit adjustment, etc.) and/or reversal card operations, which results in an increase in the available balance of the cardholder's card account (hereinafter referred to as the credit/reversal card operation), the Bank shall be entitled to unilaterally block the card account and/or card for a period of up to 30 (thirty) calendar days if a cardholder does not have documents confirming the validity of credit/reversal card operations. If technical overdraft on the card account is formed due to withdrawal by the acquiring bank of the amount previously received on the credit and/or reversal card operations, the cardholder shall be obliged to repay the resulting debt on the card account at the Bank's first request.

Chapter 9. Settlement of Disputes over Card Operations.

136. If a cardholder has disputable card operations (financial claims), the cardholder is recommended to apply to the Bank with an application of the

established sample for investigation (Disputable Operation Application - hereinafter referred to as the Dispute Application), as well as, if necessary, to provide the documents confirming the right of the cardholder to repayable funds on the disputable card operation.

137. In case of the cardholder's claim validity and payment of the commission fee according to the Bank's Tariffs, the Bank initiates a financial claim to the acquiring bank on behalf of a cardholder within the payment systems rules.

138. If the acquiring bank agrees with the cardholder's financial claim, the Bank shall refund the amount of a card operation on the card account in the manner and within the time frame established by the rules of the relevant payment systems and the internal procedures of the Bank.

139. Penalty fees, which may exceed the amount of the disputable card operation, have been established in the payment systems for unjustified financial claims. The Bank shall be entitled to write off penalty fees and the amount of unjustified financial claim from the card account without the cardholder's consent.

140. The following card operations shall not be disputed due to fraud or unauthorized access to the card account and shall be deemed to have been conducted by a cardholder:

140.1. card operations conducted with entering the PIN code and physical presentation of a card, during which the data of the card chip and/or magnetic stripe were read;

140.2. card operations conducted without entering the PIN code, for contact / contactless (PayWave) payments, with physical presentation of a card;

140.3. card operations conducted with entering 3D Secure password;

140.4. card operations conducted in Optima 24, including QR code operations;

140.5. card operations conducted using card token.

141. A card operation shall be deemed authorized by a cardholder if within 45 calendar days from the date of its conducting, a cardholder has not submitted an Dispute Application to the Bank due to unauthorized access to the card account. The maximum number of disputable card operations cannot exceed 35 (thirty-five) for the last 120 (one hundred and twenty) calendar days for one card.

141.1. The Bank has the right to refuse to accept the Dispute Application for card operations if the term of the cardholder's application has exceeded 120 (one hundred and twenty) calendar days from the date of the disputable card operation.

142. In order to control card operations on the card account and to provide timely response and card blocking in case of unauthorized access to the card account, a cardholder is recommended to activate the service of receiving SMS/push notifications on card operations, as well as regularly independently form a statement on the card account in Optima 24 or request a statement on the card account in the Bank's branches.

Chapter 10. Card Operations Monitoring and Card Blocking.

143. The Bank shall monitor card operations to identify suspicious, fraudulent and/or uncharacteristic card operations in order to reduce the risk of unauthorized access to the card accounts of the Bank's cardholders.

144. The Bank may block a card based on the results of monitoring in order to clarify the cardholder's participation in the card operation, as well as:

144.1. in case of suspicion of fraud on the part of the cardholder or participation of the cardholder in the fraudulent scheme;

144.2. in case of negative feedback to the cardholder from the users of social networks or the group members.

145. The card / card account blocking shall be performed by the Bank unilaterally, and blocking for the reasons specified in clause 145 of these Rules may be implemented for a period of up to 30 (thirty) calendar days with the Bank's right to further extend the blocking period until all circumstances have been clarified.

146. The Bank shall be entitled to place the card in the stop-list if the Bank detects multiple unsuccessful authorizations on the card: 5 (five) and more unsuccessful card operations within 2 (two) calendar days, on recurring payments due to closed access and/or insufficient funds and/or lack of communication with a cardholder to clarify participation in the card operation and/or lack of replenishment of the card account and/or card unsubscribing/unbinding from recurring payments. A card shall be excluded from the stop-list according to the Bank's Tariffs.

Chapter 11. PIN Code Setting Procedure for E-PIN Function Provided Cards.

147. E-PIN shall not be a PIN used to conduct card operation.
148. Cards provided with E-PIN functionality cannot be activated abroad.
149. The validity period of the code for E-PIN activation in the ATM shall be 30 calendar days.
150. After receiving a card with E-PIN functionality, a cardholder should send an SMS-message to 2424 with the following format: EPIN xxxx - where xxxx - the last four digits of the card number, meanwhile case is not important, space should be inserted between letters and digits. The last four digits in the SMS-message shall be unique for each cardholder.
Example: epin 4567, either Epin 4567 or EPIN 4567.
151. Sending an E-PIN request to 2424 shall be possible only from the phone number specified in the card issuance application and if it is available in the Bank's database.
152. In response to the cardholder's SMS-message according to clause 151, the Bank's system sends the SMS-message with a temporary E-PIN code in the following format: "Vvedite na bankomate E-PIN: 9175 i pridumayte svoi PIN-kod. Srok deystviya E-PIN - 30 dney. Informaciya po tel. (0312) 90 59 59". Temporary E-PIN code shall be formed according to a special algorithm and is intended only for a particular cardholder.
153. After receiving the code, a cardholder should set a new E-PIN within 30 days, for this purpose a card should be inserted into the ATM and in the appeared window of language selection should be selected the necessary language.
154. When the screen for entering the E-PIN code appears, it is necessary to enter the temporary activation code, which was received via SMS-message according to clause 151. Each entered digit will be masked by "X" symbol.
155. In case of incorrectly entered E-PIN code, the ATM will display a corresponding warning. In this case, a cardholder should repeat entering the correct E-PIN code, which was received via SMS-message according to clause 151. A cardholder is given three attempts to enter the correct E-PIN code, thereafter a cardholder should request a new E-PIN code (clauses 151-153).
156. After entering the correct E-PIN code number, the ATM will display the screen of setting the PIN code of the payment card.
157. A cardholder should enter the PIN-code, which he/she will use in future to conduct transactions. Thereafter, the input of the chosen PIN-code should be repeated once again for confirmation.
158. After that the transaction of changing E-PIN to PIN-code will be completed, which will be evidenced by printing of the ATM receipt. Now the PIN code is set, a card is activated and ready for use by a cardholder.
159. If it is necessity to re-issue a card with E-PIN functionality, for which the PIN code has already been set:
    159.1. due to physical damage to a card, the card should be re-issued and the PIN code of a cardholder sgould be kept unchanged;
    159.2. due to loss of PIN-code by a cardholder (forgotten), card re-issue is not mandatory. PIN-code reset shall be implemented upon written application of a cardholder to the Bank. Upon resetting of the lost (forgotten) PIN-code, a

cardholder should perform actions according to clauses 151-153 of these Rules to set a new PIN-code.

160. Setting or change of PIN-code for a card issued with E-PIN function in the POS-terminal of the Bank's branch shall be implemented according to the Bank's internal procedures after a cardholder has been identified.

Chapter 12. QR Code Payment Instructions and Security Rules.

161. Instructions for payment via QR code:

161.1. Step 1: Open the bank's mobile application. Launch your bank's application in your smartphone.

161.2. Step 2: Find the QR code payment function in the main menu of the Bank's mobile application.

161.3. Step 3: Point your smartphone camera at the QR code you have been provided. Make sure that the QR code is fully visible in the scanning field.

161.4. Step 4: Upon scanning, make sure that the payment information (amount, recipient) matches the one provided. Check all details of the payment/transfer carefully.

161.5. Step 5: Confirm the payment / transfer. Enter the necessary details if required (e.g. amount) and confirm the payment. You may need to enter the PIN code or use biometric authentication (fingerprint, face).

161.6. Step 6: Make sure you receive a notification of successful payment. Save or take a screenshot of the confirmation for your security.

162. Safety rules when making payment/transfer via QR code:

162.1. Regularly update the bank's mobile application to the latest version to protect against security vulnerabilities and threats.

162.2. Activate transaction notifications in the bank's application to keep track of all operations on your account.

162.3. Make purchases / transfers only through the bank's official mobile application downloaded from verified sources (Google Play, App Store).

162.4. Prior to payment / transfer make sure that the scanned QR code is authentic, in order to exclude the risk of QR code substitution (for example, make sure that there is no re-sticker of static QR code in the point of sale).

162.5. If you are redirected to a website for payment/transfer when reading a QR code, make sure that the URL starts with "https://" and belongs to an official domain. Do not enter your personal data or bank card data, as well as confidential card or mobile application information on unverified or suspicious websites.

162.6. In case of erroneous transfer, if you transferred / paid the wrong amount via QR code, please inform the seller, the conscientious seller will immediately make a refund of the excess money.

162.7. A cardholder shall be fully responsible for payments / money transfers made via QR code. Money transfers, including those made via QR code, shall be considered voluntary and irrevocable.

Chapter 13. Funds Conversion.

163. **Basic Rules of conversion on single-currency cards.**

163.1. **Rule No.1**: if the currency of a card operation coincides with the currency of the card account, no conversion of funds shall be made.

163.2. **Rule No.2:** if a card operation is conducted in Kyrgyz soms (KGS) on the card maintained in US dollars (USD), conversion will be made at the Bank's commercial rate **(purchase)** on the date of card operation **authorization**.

163.3. **Rule No.3:** if a card operation is conducted in US dollars (USD) on the card maintained in Kyrgyz soms (KGS), conversion will be made at the Bank's commercial rate **(sale)** on the date of card operation **authorization**.

163.4. **Rule No.4:** if a card operation is conducted in a currency other than Kyrgyz soms (KGS) or US dollars (USD), conversion of the card operation amount will be conducted in two stages:

163.4.1. Stage 1: Conversion from the currency of card operation to USD at the rate of Visa payment system adjusted for OIF rate;

163.4.2. Stage 2: If a card is issued with USD as a maintenance currency, the operation amount will be debited in USD in the amount according to 164.4.1. If the card is issued with Kyrgyz soms (KGS) as a as maintenance currency, a card operation amount will be further converted from USD to KGS at the Bank's commercial rate (**sale**).

164. **Examples of conversions on single-currency cards.**

164.1. The conditions (table below) accepted for calculations are indicated as an **illustration** of examples for card operations processing on single-currency cards:

164.2. Example No.1

Card types	KGS card		USD card	
Card balance	6400 KGS		72 USD	
Bank's commercial rate ($/KGS)	purchase		sale	
	85		90	
Debit transaction	*card operation for goods/services purchase in the RSO, Internet site, payment in favour of a service provider in OPTIMA24, etc.*			
Amount and Currency of transaction	6000 KGS	68 USD	6000 KGS	68 USD
Authorization stage* - blocking of the amount in the card account currency	6000 KGS	6120 KGS	70.59 USD	68 USD
Available balance on the card at the authorization stage	300 KGS	280 KGS	1.41 USD	4 USD
Posting stage* - amount to be debited in the card account currency	6000 KGS	6120 KGS	70.59 USD	68 USD
Total balance in card account currency (+/-)	300 KGS	280 KGS	1.41 USD	4 USD

** USD 68 * 90 =* ***6120 KGS*** */ 6000 KGS / 85 =* ***70.59*** *USD*

164.3. Example No.2

Card type	KGS card		USD card	
Card balance	6400 KGS		72 USD	
Bank's commercial rate (USD/KGS)	purchase		sale	
	85		90	
OIF	1.25%			
Курс на дату	Authorization		Posting	
Visa exchange rate (EUR/USD)	1.07		1.08	
Visa exchange rate (USD/TRL)	15		14	
Visa exchange rate (EUR/USD) adjusted for OIF rate	1.08		1.09	
Visa exchange rate (USD/TRL) adjusted for OIF rate	14.81		13.83	
Debit transaction*	**card operation for goods/services purchase in the store, Internet site, etc.*			
Amount and Currency of transaction	65 EUR	1000 TRL	65 EUR	1000 TRL
Authorization stage* - blocking of the amount in the card account currency	6318 KGS	6076.80 KGS	70.20 USD	67.52 USD
Available balance on the card at the authorization stage	82 KGS	323.20 KGS	1.80 USD	4.48 USD
Posting stage* - amount to be debited in the card account currency	6376.50 KGS	6507.90 KGS	70.85 USD	72.31 USD

Total balance in card account currency (+/-)	23.50 KGS	-107.90 KGS	1.15 USD	-0.31 USD

** EUR 65 * 1.08=**USD 70.20** * 90 = 6318 KGS / TRL 1000 : 14.81 = **USD 67.52** * 90 = 6076.80 KGS*
*** EUR 65 * 1.09 = **USD 70.85** * 90 = 6376.50 KGS / TRL 1000 : 13.83 = **USD 72.31** * 90 = 6507.90 KGS*

165. **Basic conversion rules on multi-currency cards.**

165.1. **Rule No. 1:** if a card operation is conducted in KGS or USD or EUR, funds will not be converted, **provided that the available balance** on KGS or USD or EUR sub-accounts respectively, **is sufficient.** A card operation conducted in KGS will be debited from the KGS sub-account, a card operation conducted in USD will be debited from the USD sub-account, a card operation conducted in EUR will be debited from the EUR sub-account.

165.2. **Rule No.2**: if a card operation is conducted in KGS or USD or EUR in cases of **funds insufficiency or absence** on KGS or USD or EUR sub-accounts respectively, normalization of these sub-accounts will be made at the expense of other sub-accounts with conversion at the Bank's commercial rate on the date of card operation. Normalization of sub-accounts will be made according to the priority of sub-accounts specified in clause 129.8 of these Rules.

165.3. **Rule No.3**: if a card operation is conducted in a currency other than KGS/ USD/ EUR, conversion of the card operation amount will be made in two stages:

165.3.1. Stage 1: conversion from the currency of an operation to USD at the exchange rate of Visa payment system adjusted for OIF rate;

165.3.2. Stage 2: if funds on the sub-account in US dollars (USD) are insufficient, the amount of card operation in the sum according to clause 166.3.1. will be debited from USD sub-account. In case of insufficient balance or absence of funds on USD sub-account the amount of card operation will be debited through normalization of USD sub-account at the expense of other sub-accounts with conversion at the Bank's commercial rate on the date of card operation posting. Normalization of sub-accounts will be made according to the priority of sub-accounts specified in clause 129.8 of these Rules.

166. **Examples of multi-currency card conversions**.

166.1. The conditions (table below) accepted for calculations are indicated as an **illustration** of examples for processing card operations on multi-currency cards:

Sub-accounts balances	KGS	USD	EUR	RUB
	5000	150	150	1000
Available card balance in KGS	33800			
Exchange rates	purchase		sale	
Bank's commercial rate (USD /KGS)	85		90	
Bank's commercial rate (EUR/KGS)	100		110	
Bank's commercial rate (KGS)/RUB)	1.05		1.2	
	Authorization		Posting	
Visa payment system exchange rate (GBP / USD)	0.83		0.81	
Visa payment system exchange rate (USD /TRL)	15		14	
Visa exchange rate (GBP /USD) adjusted for OIF rate	0.82		0.80	
Visa exchange rate (USD/TRL) adjusted for OIF rate	14.81		13.83	
OIF rate	1.25%			
Visa to Visa transfer fee (Visa Direct)	0.8% min. 250KGS			
Fee for cash withdrawal at third-party ATMs	0.8% min. 120KGS			
Multiplier (for cash withdrawal operations in ATMs)	2%			

166.2. **Example No.1:** when a debit card operation is conducted (purchase of goods/services in the store, cash withdrawal from the Bank's ATM, payment in favour of a service provider in Optima 24, etc.) in the amount of 2500 KGS:

166.2.1. Authorization: the amount of 2500 KGS will be blocked. Available balance will be equal to 31300 KGS

166.2.2. Posting: 2500 KGS will be debited from KGS sub-account.

166.2.3. Total: the balances on the sub-accounts after final settlement will be as follows: KGS - 2500; USD - 150, EUR - 150; RUB - 1000.

166.3. **Example No.2:** when a debit card operation is conducted (purchase of goods/service in the store, cash withdrawal from the Bank's ATM, payment in favour of a service provider in Optima 24, etc.) in the amount of 6000 KGS, conversion and normalization on sub-accounts will be implemented as follows:

166.3.1. Authorization: the amount of 6000 KGS will be blocked. Available balance will be equal to 27800 KGS.

166.3.2. Posting: an amount of 5000 KGS will be debited from KGS sub-account, normalization on the remaining amount of 1000 KGS will be implemented from USD sub-account at the Bank's commercial rate (purchase). Calculation of normalization: 1000 KGS /85= 11.76 USD

166.3.3. Total: the balances on the sub-accounts after final settlements will be as follows: KGS - 0; USD - 138.24, EUR - 150; RUB - 1000

166.4. **Example No.3:** when a debit card operation is conducted (money transfer to another VISA card) in the amount of 160 USD, conversion and normalization on sub-accounts will be implemented as follows:

166.4.1. Authorization: the transfer amount of 160 USD will be blocked, as well as the transfer fee amount (0.8% min.120 KGS) at the Bank's commercial rate (purchase) $160*85=13600 KGS (transfer amount) + 120 KGS (fee amount), total 13600+120=13720. Available balance will be equal to 20080 KGS.

166.4.2. Posting: 150 USD will be debited from USD sub-account, the remaining transfer amount of 10 USD and the fee amount of 120 KGS will be normalized from KGS sub-account through conversion at the Bank's commercial rate (sale). Calculation: 10 USD *90=900 KGS. Total: 900+120 = 1020 KGS

166.4.3. Total: the balances on the sub-accounts after final settlement will be as follows: KGS - 3980; USD - 0, EUR - 150; RUB - 1000.

166.5. **Example No.4:** when a debit card operation is conducted (funds withdrawal at the ATM abroad subject to 1% fee of the acquiring bank) in the amount of 200 GBP, conversion and normalization on sub-accounts will be implemented as follows:

166.5.1. Authorization: the amount of 200 GBP will be converted to USD at VISA exchange rate adjusted by OIF rate. Calculation: 200 GBP / 0.82 = 244 USD plus 1% fee of the acquiring bank 244 USD + 1%=246.44 USD. The amount to be blocked at the Bank's commercial rate (purchase) will be 246.44USD*85=20947,40KGS + **multiplier** 20947.40KGS *2%=418.95 KGS + cash withdrawal fee 250KGS. Total 20947.40KGS + 418.95KGS + 250KGS = 21616.35 KGS. Available balance will be equal to 12183.65 KGS.

166.5.2. Posting: Step 1: the amount of 200 GBP will be converted to USD at VISA exchange rate adjusted for OIF rate. Calculation: 200 GBP / 0.80 = 250 USD plus 1% fee of the acquiring bank 250 USD+1%=252.5 USD. The entire amount of a card operation of 252.5 USD will be debited from USD sub-account, creating a debt of 102.50 USD; Step 2: the amount of 102.50 USD will be normalized through conversion from KGS sub-account. Calculation: 102.50USD*90=9225 KGS and a fee of 250 KGS, total 9475 KGS. In view of the available KGS sub-account balance of 5000

KGS, the remaining amount to be debited of 4475 KGS will be normalized through conversion from EUR sub-account at the Bank's commercial rate (purchase). Calculation: 4475KGS/100=44.75 EUR.

166.5.3. Total: the balances on the card account sub-accounts after posting a card operation will be as follows: KGS - 0; USD -0, EUR - 105.25; RUB - 1000.

166.6. **Example No.4:** credit card operation - card incoming transfer in the amount of 705 USD.

166.6.1. Authorization: the amount to be blocked (will increase the available balance in KGS currency basket) will be equal to the transfer amount minus the Bank's fee (0.7%) at the Bank's commercial rate (**purchase**). Calculation: (705-(705*0,7%)*85=59505.1KGS. ***Important!!!*** Until the final posting, the amount of incoming transfer is recorded in KGS, therefore the Bank recommends to refrain from spending money to avoid exchange rate difference.

166.6.2. Posting: the transfer amount minus the Bank's fee amount will increase USD sub-account by: 705-(705*0.7%)=700.06 USD

166.6.3. Total balances on sub-accounts of the card account after posting a card operation will be as follows: KGS - 500; USD -850.06, EUR - 150; RUB - 1000.

166.7. **Example No.5:** Debit card operation (intra-bank transfer to a card / demand account) in foreign currency in the amount of 140 USD. Data for calculations are given as an illustration of the example.

Sub-accounts balances	2000 KGS	50 USD	50 EUR	1500 RUB
Available card balance in KGS	12825			
Exchange rates	purchase		sale	
Bank's commercial rate (USD /KGS)	85		90	
Bank's commercial rate (EUR/KGS)	100		110	
Bank's commercial rate (KGS)/RUB)	1.05		1.2	
Dynamic Multiplier*:				
Dynamic Multiplier USD	6%			
Dynamic Multiplier EUR	9.09%			
Dynamic Multiplier RUB	12.5%			

** it is used to calculate the amount of minimum balance when transferring funds from a multi-currency card in foreign currency. The dynamic multiplier is automatically calculated by Optima24 system as a percentage difference between the Bank's commercial rates (buying and selling rates) of the selected foreign currency. The amount of minimum balance calculated by the dynamic multiplier reduces the available balance on the card account.*

166.7.1. Calculation of funds sufficiency on the card account: when making an intra-bank transfer in the amount of 140 USD, the card must be provided with a balance equal to the minimum balance calculated based on the dynamic multiplier rate (6%) of the transfer amount or (140 USD*6%)*85 = 8.4 USD * 85 = 714 KGS plus the transfer amount at the Bank's commercial rate (purchase) or 140 USD * 85 = 11900 KGS. Total: 12614 KGS. Since the card account balance (12825 KGS) exceeds the minimum allowed balance (12614 KGS), the system will allow a cardholder to make this transfer.

166.7.2. Authorization: the total amount to be blocked will be the amount of the transfer at the Bank's commercial rate (purchase) or 140 USD * 85 = 11900 KGS.

166.7.3. Posting:

Stage 1: an amount of 50 USD will be debited from USD sub-account, further the transfer amount will be collected additionally through normalization of other foreign currency sub-accounts of the card, namely:
Stage 2: Account normalization:

1) to normalize the transfer amount the sum of 2000 KGS / 90 = 22.22 USD will be converted;
2) to normalize the transfer amount the sum of (50 EUR * 100) / 90 = 55.55 USD will be converted;
3) to normalize the transfer amount 12.23 USD will be converted from RUB sub-account: (1048 RUB * 1.05) / 90 = 12.23.
   Total: 50 USD + (2000 KGS = 22.22 USD) + (50 EUR = 55.55 USD) + (1048 RUB = 12.23 USD) = 140 USD

166.7.4. Total balances on sub-accounts of the card account after posting a card operation will be as follows: KGS - 0; USD -0, EUR - 0, RUB- 452.

167. Conversion operations on **Elcart / Elcart + MIR Accept** cards shall be regulated by the internal regulatory documents and the payment systems rules (Elcart NSPCS / MIR NSPC).