Евразийский Сберегательный Банк

Appendix No. 1
to the Agreement on Opening and Maintaining Bank Accounts (Card Accounts)
(for individuals in national and foreign currencies)

Rules

for Using Bank Payment Cards at

OJSC “Eurasian Savings Bank”

Table of Contents:

Terms and Definitions..... Ошибка! Закладка не определена.
Chapter 1. General Provisions..... **Ошибка! Закладка не определена.**
Chapter 2. Procedure for Card Issuance and Storage ..... **Ошибка! Закладка не определена.**
Chapter 3. PIN Code ..... **Ошибка! Закладка не определена.**
Chapter 4. Using the Card at Merchant Outlets ..... **Ошибка! Закладка не определена.**
Chapter 5. Using the Card at an ATM..... **Ошибка! Закладка не определена.**
Chapter 6. Using the Card on the Internet ..... **Ошибка! Закладка не определена.**
Chapter 7. Security Measures for Card Handling..... **Ошибка! Закладка не определена.**
Chapter 8. Processing of Card Transactions ..... **Ошибка! Закладка не определена.**
Chapter 9. Settlement of Disputes on Card Transactions **Ошибка! Закладка не определена.**
Chapter 10. Monitoring of Card Transactions and Card Blocking.....**Ошибка! Закладка не определена.**
Chapter 11. Instructions for Payment via QR Code and Safety Rules....**Ошибка! Закладка не определена.**
Chapter 12. Currency Conversion ..... **Ошибка! Закладка не определена.**

Terms and Definitions

Authorization - a procedure by which the issuer confirms the authority or authorship of the cardholder to conduct a transaction using a bank payment card (transaction), resulting in the issuer's obligation to the acquirer to execute the payment document created using the card of the aforementioned issuer. Authorization can be automated (via terminal) or vocal (via telephone). In cases where the issuer and acquirer are the same entity for a transaction conducted with a bank payment card, authorization is the permission granted by the issuer to the client to perform said transaction.

Bank Payment Card (hereinafter - Card) - a payment instrument used for settlements when purchasing goods or services, withdrawing cash in national and foreign currencies, making money transfers, and for settlements in the form of electronic money through terminals, ATMs, or other devices (peripheral devices). A card issued for a card account in the name of the card account owner is the primary card, while cards issued for the card account in the names of third parties are supplementary cards. Upon the expiration of the primary card, or in the event of its loss or theft, the card issued to replace it is also considered a primary card. Cards are categorized as debit or credit, issued as a plastic card, in electronic form, or as a tokenized/digitized version of the card stored on a mobile device that allows for contactless payment operations using NFC technology.

ATM - a hardware and software complex for dispensing and/or receiving cash, recording funds to a card, obtaining information on transactions performed by the cardholder, making non-cash payments, and issuing a card receipt for all types of transactions performed. An ATM is bank equipment and is designed for the independent performance of operations by the cardholder using a card without the participation of an authorized employee of a commercial bank.

Card Blocking - a full or temporary ban on transactions using the card, initiated by the cardholder, the Bank, or a merchant via one of the methods established by the payment system. In the event of a full ban, the payment card is to be confiscated when presented for service.

Cardholder - a client of the Bank, an individual, including one authorized by a legal entity/individual entrepreneur who owns the card account, who has the right to perform operations using the card based on an Agreement with the Bank, including holders of primary and supplementary cards opened for the card account, as well as clients within salary projects.

Card Account - a bank account on which operations performed using the card or its details are reflected.

Card Transaction - an operation using the card and/or its details and other remote service tools (e.g., purchasing goods, services, transferring funds, currency exchange, or receiving cash), resulting in a change in the balance of funds on the cardholder's card account.

Contact Center - a department of the Bank serving as a 24-hour contact center designed to process remote inquiries from existing and potential Bank clients. Contact Center phone: (312) 905151

Mobile Device - any portable device of the cardholder on which a Mobile Payment Service is installed and NFC technology support is available (e.g., smartwatch, smartphone, tablet, etc.).

Multiplier - a coefficient in the form of a percentage markup on the authorization amount for a card transaction, applied by the Bank to mitigate the risk of debt arising on the card account when a card transaction is performed in a currency other than the currency of the card account. Final settlements for card transactions (debiting the card transaction amount from the cardholder's card account) are performed without applying the multiplier. The types of card transactions to which the multiplier applies are determined independently by the Bank. The size of the multiplier is set by the Bank depending on the market conditions in the foreign exchange market and may be changed by the Bank unilaterally. Information regarding the size of the multiplier is specified on the Bank's corporate website at www.esb.kg.

Payment System for Settlements Using Bank Payment Cards (hereinafter - 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 establishes specific rules for mutual settlements for payments using cards between participants of the system. Payment systems are categorized as local (national) (Elkart) and international (Visa, Mastercard).

Mobile Payment Service - software from a Provider provided to the cardholder based on a separate agreement (contract) concluded between the provider and the cardholder, representing an application installed on a mobile device that allows for card tokenization, token deletion, and the use of a token for transactions. The functional capabilities of the Mobile Payment Service, the terms of its use, and the procedure for granting the cardholder rights to use it are determined by the Provider. In cases where the Bank acts as the Provider, the Mobile Payment Service is the Bank's Mobile Application. Such mobile payment services include mobile payment systems using electronic wallets (Google Pay, Garmin Pay, etc.), which, in combination with software on a mobile device equipped with NFC technology, provide the ability to pay for purchases and withdraw funds.

Posting (or Clearing) - the process of collecting, processing, confirming payments, and calculating the mutual obligations of payment system participants for card transactions performed, carried out through mutual offsetting based on the balance of payments, representing the final financial settlement for a card transaction.

Processing - a licensed activity including interconnected processes for receiving, processing, and issuing financial information to payment system participants.

Processing Center (hereinafter - PC) - a legal entity performing processing.

Provider - a legal entity that is the manufacturer (developer) of a Mobile Payment Service, which ensures information and technological interaction during the formation, maintenance, and use of a token for card transactions based on payment system rules and/or based on a separate agreement with the payment system. Additionally, the Bank may be a provider when the cardholder uses the Bank's software.

Recurring Payments - regular card transactions (payments) conducted on the Internet or card transactions (payments) performed through remote banking services using previously saved card details, which do not require participation or confirmation from the cardholder (e.g., subscription fees / payment for internet resource services, payment for goods or services in installments, regular "auto-payments").

Social Engineering - a set of psychological and sociological techniques, methods, and technologies that allow fraudsters to obtain protected/secret cardholder information for the purpose of stealing funds.

Stop-list - a list of blocked cards for which all and/or certain types of operations have been suspended or temporarily suspended.

Card Tokenization - a technology provided by payment systems designed to exchange sensitive card data for a special anonymized equivalent (token) to protect card details. During the tokenization process, a link is created between the card details and the token, allowing for the unique identification of the card used for transactions via the token. Transactions performed using a token are equivalent to transactions performed by the cardholder using the card itself or its details.

Token - a digital representation of a card that is formed upon card tokenization and is stored in encrypted form in a secure cloud storage of the payment system, as well as in the memory of a mobile device.

Phishing - a type of internet fraud aimed at gaining access to the cardholder's secret and protected information - card details and passwords, and/or the login and password for remote banking systems. Most often, fraudsters gain the cardholder's trust and obtain card details and passwords via social networks and messengers. Generally, the method of mass mailings is used, including on behalf of the bank or large and well-known companies, which may contain links to fake websites that appear identical to the real ones. In such mailings or messages, the cardholder is often asked to update or confirm the accuracy of personal information by being redirected to a fake site where the cardholder voluntarily enters their credentials/card details. If fraudsters succeed in obtaining this information, it leads to the theft of funds from the card account. Responsibility for such operations lies with the cardholder.

Acquirer - a Bank that has received permission for acquiring, the owner of a network of peripheral devices, ensuring the possibility of performing authorizations 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.

Acquiring Network - includes all devices of acquiring banks participating in payment systems designed for card transactions: ATMs; cash POS terminals installed in bank branches; merchant POS terminals installed in merchant outlets; payment terminals; automatic deposit machines; e-commerce.

E-commerce - the activity of merchant outlets that have contractual relationships with an acquirer for the purpose of conducting financial/merchant non-cash card transactions carried out through internet websites using computer networks.

Embossed Name of the Cardholder - the surname and name of the cardholder in Latin transcription, printed on the front side of the card.

Issuer - the Bank issuing cards in accordance with the technology and rules of the relevant payment systems and the legislation of the Kyrgyz Republic.

CVV2 code (Card verification value) - a three-digit code to verify card authenticity, requested during online payments and other operations.

Near Field Communication (NFC) - a short-range wireless data transmission technology that enables data exchange between devices, and/or a card and devices. Per the requirements of most payment systems, cards must support contactless payment technology (NFC).

PIN code (Personal identification number, hereinafter - PIN code) - a personal identification number allowing for the authentication of the user to perform a transaction. The PIN code is the access password to the card and is considered secret and protected information, not to be disclosed to third parties other than the cardholder. The card PIN code is assigned for the purpose of identifying the holder's identity when performing card transactions.

POS terminal (point-of-sale) - a terminal for receiving payment for goods and services at merchant outlets using a card and other remote service tools.

3D Secure password - a secure protocol used as an additional layer of security for two-factor user authentication for transactions without the presence of the card. The technology was developed for the Visa payment system to improve the security of internet payments under the Verified by Visa (VbV) service. Services based on this protocol were also adopted by Mastercard payment systems under the name Mastercard SecureCode (MSC). The 3D Secure password is formed dynamically and is intended for use when making purchases on the Internet.

QR code - a two-dimensional barcode symbol for transmitting payment data, which is used during non-cash payments and transfers.

Chapter 1. General provisions

1.1. The Rules for Using Bank Payment Cards of OJSC "Eurasian Savings Bank" (hereinafter referred to as the Rules) define the terms of use, terms of service, and security measures for card transactions with cards of payment systems issued by OJSC "Eurasian Savings Bank" (hereinafter referred to as the Bank).

1.2. These Rules are composed in accordance with the Regulation of the National Bank of the Kyrgyz Republic "On Bank Payment Cards in the Kyrgyz Republic".

1.3. These rules are standard (model) and are not subject to change by the cardholder. The Bank may revise these Rules unilaterally as necessary by posting information about the changes on the corporate website www.esb.kg in the "News" section, considering the period established by the current legislation of the Kyrgyz Republic for informing about upcoming changes.

Chapter 2. Procedure for card issuance and storage

2.1. The Bank issues the card directly to the cardholder or to an authorized person acting on the basis of a notarized power of attorney. If the cardholder agrees, the card can be sent via a courier organization; in this case, the cardholder must confirm receipt of the card by providing the data requested by the Bank (photo/video confirmation or other information that the Bank requires from the cardholder).

2.1.1. Card issuance to holders within salary projects is carried out by the Bank transferring the cards to an authorized representative of the organization based on a notarized power of

attorney or signed by the head or another person authorized by the constituent documents, with the organization's seal attached.

2.2. Transferring the card to third parties who are not the cardholder for use or as collateral is prohibited.

2.3. The front side of the card contains:

2.3.1. the Bank's logo;
2.3.2. the payment system's logo;
2.3.3. an embedded chip - an integrated microcircuit with encoded information;
2.3.4. a card number consisting of 16 digits;
2.3.5. the client's embossed name (surname and name of the cardholder in Latin or initials if the surname and name exceed 22 Latin characters);
2.3.6. the card's expiration date;

2.4. The reverse side of the card contains:

2.4.1. a magnetic stripe
2.4.2. a place for the client's signature (optional);
2.4.3. the Bank's Contact Center number;
2.4.4. a verification code (CVV2);

2.5. The cardholder must protect the card from mechanical damage and exposure to electromagnetic fields (car alarms, mobile phones, computers, security gates at airports, banks, shops, etc.) to avoid damage to the magnetic strip.

2.6. It is prohibited to exert any physical impact with any object on the surface of the PIN envelope, chip, or card as a whole. 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 expense of the cardholder in accordance with the Bank's current Tariffs.

2.7. The amount of commissions and fees for issuing and servicing cards, as well as the expenditure and income limits for card transactions, limits on money transfer transactions, limits on currency conversion and/or bank account type, limits on contactless payments allowed without entering a PIN code, are determined by the Bank's Tariffs. Information on the amounts of limits, commissions, and tariffs is posted on the Bank's corporate website www.esb.kg.

2.8. For security reasons, the Bank does not recommend setting excessively high limits for long periods of time. The cardholder shall be liable for the consequences of non-compliance with this clause.

2.9. The card account is intended only for performing the following card transactions:

2.9.1. crediting/debiting cash and non-cash funds of a non-commercial nature to/from the card accounts of individuals;
2.9.2. crediting cash and non-cash funds of a commercial nature to the card accounts of legal entities;
2.9.3. debiting funds from the card accounts of individuals and legal entities to pay for goods and services provided by commercial and service enterprises and other third parties;
2.9.4. debiting funds from the cardholder's card account to pay the Bank's commissions and loan/loans (including technical overdrafts);
2.9.5. debiting funds from the card account of individuals and legal entities to repay debts to the Bank arising in the process of issuing and servicing a payment card, including in excess of the balance of funds in the card account, or arising under other circumstances due to other agreements between the Bank and the cardholder;
2.9.6. crediting and debiting funds from the card accounts of individuals and legal entities in the amount of transfer transactions (including Bank commissions in accordance with the current Tariffs);
2.9.7. debiting funds from the card accounts of individuals and legal entities on the basis of enforcement documents provided for by the current legislation of the Kyrgyz Republic.

2.10. The Bank has the right to provide the cardholder with the opportunity to perform tokenization for further card transactions using a token (a mobile device on which the token is stored).

2.11. At the cardholder's initiative, the card may be linked to mobile payment services (e-wallets)

for payment and withdrawal of funds using tokenization technology and payment via a mobile device using an NFC module. When performing a transaction using a token, the cardholder is verified by entering a password on the mobile device and, if necessary, by additionally entering a PIN code (for payments via a POS terminal or ATM).

2.12. In order to enable card transactions using contactless payment technology (NFC), including for the purpose of providing the cardholder with information about their card transactions in the Bank's mobile application, the Bank has the right to transfer information about the amount of the card transaction, the date and time of its execution, the type of transaction, the currency code, and the authorization status for its processing to the providers (Google Ireland Limited, Garmin Ltd., etc.) of mobile payment service software (Google Pay, Garmin Pay, etc.).

2.13. When the Cardholder uses NFC technology, the Bank shall not be liable:

2.13.1. for the consequences that may arise if information about the tokenized card, including the balance of such card, displayed on the device screen becomes known to third parties;

2.13.2. for situations related to malfunctions in the systems that receive, process, and transmit data on transactions made using the card for reasons beyond the Bank's control, for the operation of Google Pay, Garmin Pay, etc.

2.14. The Cardholder's ability to perform card transactions using mobile payment services (Google Pay, Garmin Pay, etc.) may be limited by the functionality of the Cardholder's mobile device software, including the Bank's mobile application.

2.15. The Cardholder is aware of the 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 transactions and, therefore, the Cardholder is solely responsible for the confidentiality of one-time passwords, passwords, PINs, and other means of access to the Cardholder's mobile device, mobile application, and card.

2.16. The token can be deleted by the Cardholder independently on a mobile device or by contacting the Bank. The token is blocked by contacting the Bank.

Chapter 3. PIN code

3.1. The card is issued to the cardholder together with a special envelope containing the PIN code (or by sending an SMS/PUSH notification to the mobile phone number specified in the Customer's application when opening the account). The cardholder is advised to open the envelope immediately upon receipt of the card, ensure that the PIN code is printed legibly, memorize the PIN code (SMS notification/PUSH notification), and then store the envelope separately from the card and in a place inaccessible to third parties.

3.2. The PIN code is not known to Bank employees and must be kept secret by the cardholder throughout the entire period of card use.

3.3. A lost PIN code on paper or in an SMS/PUSH notification cannot be recovered, and the card must be reissued in accordance with the Bank's Tariffs.

3.4. It is recommended to follow certain rules to ensure the confidentiality of your PIN code:

3.4.1. Do not write down your PIN code on your card;

3.4.2. Do not keep your PIN envelope with your PIN code and your card together (in one place);

3.4.3. Do not allow third parties to see the PIN code numbers you enter on the device keyboard (ATM, terminal);

3.4.4. Do not make mistakes when entering the PIN code numbers. If the PIN code is entered incorrectly (three times in a row), the limit on the number of attempts to enter the PIN code expires, the card is automatically blocked, and further card transactions are impossible. In this case, the cardholder is advised to contact the nearest Bank branch or the Bank's Contact Center to reset the number of incorrect PIN code entries.

3.5. Card transactions confirmed by entering the PIN code are considered by the Bank to have been made by the cardholder and cannot be disputed on the grounds of unauthorized access to the card account and/or fraud.

Chapter 4. Using the card at merchant outlets

4.1. Non-cash payment for goods, services, and works at merchant outlets (hereinafter – TSPs) is performed within the established card limit and the limit in the acquiring bank's device.

4.2. The maximum amount of a single operation and the number of operations per day in the Bank's and/or a third-party acquirer's device is determined by the Bank's Tariffs, the acquirer's policy, and payment system rules.

4.3. Payment for goods and services can be performed via:

- 4.3.1. reading the card's magnetic stripe and entering a PIN code;
- 4.3.2. reading the card's magnetic stripe without entering a PIN code;
- 4.3.3. reading the card chip and entering a PIN code;
- 4.3.4. reading the card chip without entering a PIN code;
- 4.3.5. reading a contactless chip via a contactless chip reader without entering a PIN code within established limits per the Tariffs of the Bank, the acquirer, and/or payment system rules;
- 4.3.6. reading a contactless chip via a contactless chip reader with PIN code entry for amounts exceeding the established limit per the Tariffs of the Bank, the acquirer, and/or payment system rules;
- 4.3.7. using a card token without entering a PIN code (within established limits) or with PIN code entry (for amounts exceeding the limit). Limits are regulated by the Bank's policy, the acquirer's policy, and/or payment system rules;
- 4.3.8. reading a QR code to perform a money transfer or non-cash payment for goods or services at TSPs.

4.4. Non-cash payment for goods and services at TSPs can be made either online or offline, depending on the settings of the acquiring bank's devices. The cardholder is responsible for conducting transactions in offline mode. At the same time, payment for goods and services in POS terminals belonging to the Bank in offline mode is prohibited by default.

4.5. Payment for goods and services, as well as cash withdrawals with a chip reading error in devices supporting chip technology, is prohibited (Fallback transactions).

4.6. Bank cards are issued with the possibility of making contactless payments (PayWave / NFC), which cannot be disabled at the cardholder's initiative due to the payment systems' requirement for mandatory support of contactless payment technology.

4.7. All transactions using the card at a merchant must be conducted in the presence of the cardholder. This is necessary in order to reduce the risk of unauthorized access to the cardholder's personal data specified on the card. Some merchants may request identification. Therefore, when paying for purchases with a card, the Bank recommends that you carry your passport or other identification document with you.

4.8. All TSPs are equipped with signs with payment system logos to inform cardholders about the possibility of servicing a particular card at this TSP, as well as the possibility of accepting payments using a QR code.

4.9. To perform card transactions, the cardholder must insert/tap the card or hold the mobile device (in case of card tokenization) to the device (ATM, payment terminal, POS terminal) or scan the QR code via the Bank's mobile application when paying via QR code.

4.10. To conduct card transactions through a TSP or the Bank, an employee of the TSP or the Bank performs authorization using a POS terminal. The card is placed in or tapped against the POS terminal reader.

4.11. Previously, the TSP or Bank employee enters the transaction amount on the POS terminal keypad. In some cases, for example, if the transaction amount limit allowed without a PIN is exceeded, the cardholder may be asked for a PIN code, which must be entered on a special keypad. 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 within a minimum distance of the POS terminal or ATM to perform a card transaction or scan the QR code through the Bank's mobile application when paying via QR code.

4.12. The cardholder is recommended to:

4.12.1. verify the correctness of the data specified in the receipt;
4.12.2. take one copy of the POS terminal receipt until the final settlement for this card transaction, as well as for the purpose of reconciling debit transactions on the card account.

4.13. For transactions confirmed by a PIN code, as well as contactless transactions conducted without entering a PIN code within the established limit, the cardholder's signature on the receipt is not mandatory.

4.14. Requirements for signing a receipt when conducting transactions in a third-party acquirer's network are determined by the policy of that acquirer.

4.15. The cardholder is prohibited from signing a commercial POS terminal receipt that does not specify the purchase amount (of the goods/service).

4.16. According to the rules of payment systems, TSPs are not entitled to inflate the cost of goods and services when accepting a card for payment compared to cash settlement. If such cases are identified, the cardholder is recommended to notify the Bank.

4.17. A refund for a purchase or service paid by card is made with the consent of the TSP. For this purpose, at the request of the cardholder, the TSP employee must initiate a "refund" transaction on the POS terminal. Refund of the purchase amount in cash is not provided for.

Chapter 5. Card use at ATMs

5.1. As a rule, cash is issued by card in the currency of the country of stay. Some acquiring banks may set an additional commission for cash withdrawals. Also, in some countries, the frequency and maximum amount of cash withdrawals by card may be limited by law.

5.2. Before using an ATM, it is necessary to inspect it for unusual devices: unevenly installed PIN pad, overlays in the card reader, the presence of mini-video cameras directed at the PIN pad, 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 to report it to the acquiring bank's Contact Center at the numbers indicated on the ATM.

5.3. To receive funds or other services at an ATM, you must insert the card into the ATM's card reader or bring the mobile device in case of card tokenization, enter the PIN code, select the appropriate menu, and follow the instructions on the screen.

5.4. To refuse a service, it is necessary to cancel the transaction by pressing the "Cancel" button.

5.5. When working with an ATM, it is not allowed to use physical force to insert the card into the ATM. If the card does not fit, you should refrain from using such an ATM.

5.6. When entering the PIN code, make sure that the PIN code is not seen by third parties. After 3 (three) attempts to enter an incorrect PIN code, the card is blocked and may be detained (seized) by the ATM.

5.7. After the command "TAKE YOUR CARD" appears on the screen, it is necessary to immediately take the card; otherwise, after 15-30 seconds, the card may be detained by the ATM.

5.8. After the command "TAKE YOUR MONEY" appears on the screen, it is necessary to immediately take the funds; otherwise, after 20 seconds, the funds will be detained by the ATM.

5.9. It is recommended to always take the receipt of the transaction through the ATM, as the receipt is a document confirming the transaction in case of dispute resolution. Due to the presence of information related to the cardholder in the receipt, it is recommended to take the receipt with you and not leave it near the ATM.

5.10. The reasons for unsuccessful card transactions at an ATM may be as follows:

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

5.10.2. the requested amount exceeds the single 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 operation several times;

5.10.3. the requested amount exceeds the available balance of the card account (including the Bank's and/or acquiring bank's commission). 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 transaction through the ATM menu.

5.11. In case of card seizure by an ATM, it is necessary to make sure that the card is indeed detained (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 them.

5.12. In case of card seizure by an ATM, the cardholder is recommended to immediately block the card in any convenient way: by contacting the Bank's Contact Center or independently through the Bank's mobile application. Subsequently, the Bank recommends issuing a new card with new details, as there is a risk of third parties accessing the card and/or card details when the card is seized.

5.13. If the card or funds are detained by an ATM, it is necessary to immediately contact the Bank or the acquiring bank at the phone numbers indicated on the ATM0.

Chapter 6. Card use on the Internet

6.1. Card transactions on the Internet are carried out within the established limit for Internet payments and the limit of the acquiring bank.

6.2. Payment for goods or services on the Internet is made without the physical presence of the card, but using card details, the mandatory ones of which are: card number, card expiration date, embossed name of the cardholder. Additionally, when making payments on the Internet, such card details as: CVV2, 3D Secure password may be requested 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.

6.3. The Bank issues cards with access to Internet payments "by default".

6.4. The cardholder can close access to Internet payments (except for card transactions carried out with the entry of a 3D Secure password and recurring payments). To do this, the cardholder is recommended to contact the Bank with a written application to disable access to Internet payments or independently disable access through the "ESB" mobile banking.

6.5. The Bank's VISA and Mastercard cards are connected to the 3D Secure service "by default". The 3D Secure protocol does not apply to transactions conducted via Elcard cards.

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

6.7. Card transactions on the Internet can be conducted in the following ways:

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

6.7.2. by linking card or token details to an Internet account, e-wallet, store, trading platform, Internet service, or other Internet resources in accordance with the requirements and terms of service of the Internet resource. If a card/token is linked, it becomes possible to make recurring payments. The cardholder is responsible for such transactions until the card details are unlinked or the token is deactivated. In this case, the cardholder is advised to keep proof of unlinking the card or deactivating the token from recurring payments, which may be required in the event of a dispute between the cardholder and the Internet resource.

6.8. Access to transactions on the Internet exceeding the limit established by the Bank's tariffs is carried out:

6.8.1. by the cardholder contacting a branch of the Bank and submitting a written application to change the current limits and restrictions on Internet payments.

6.9. Before performing a transaction on the Internet, the Bank recommends that the cardholder:
6.9.1. check the expiration date of the card and the absence of card blocking;
6.9.2. ensure there are sufficient funds on the card;
6.9.3. ensure that there is open access on the card to Internet payments and sufficient limits for this type of card operations;
6.9.4. ensure that security updates are installed in their browser;
6.9.5. make Internet payments only on verified sites with a positive reputation, as well as sites that support secure Internet payment technology (3D Secure);
6.9.6. refrain from performing operations on automatically redirected pages or pop-up windows to avoid "Phishing". In most cases of "Phishing", a fraudulent clone site to which redirection can be configured looks identical to the real one and may only slightly differ from the original site, for example, by part of the URL address;
6.9.7. to cancel an Internet payment, full or partial, the cardholder must first contact the customer support service of the online store to initiate a payment refund.

6.10. When booking services on the Internet in the Travel & Entertainment category (such as car rental, hotels, ticket purchases, etc.), the Bank has the right to block money on the cardholder's card account until the completion of full settlement with the TSP (Merchant). At the same time, the acquiring bank has the right to increase the amount of the final debit in the amount provided for by the rules of the corresponding payment system. The cardholder bears full responsibility for the payment of the added value for card operations related to the Travel & Entertainment category.

Chapter 7. Security measures for card handling

7.1. Card number, PIN code, CVV2 code, card expiration date, embossed cardholder name, client ID at the Bank, 3D Secure and OTP passwords, as well as the login and password for the Bank's mobile application, constitute card details and confidential information that provide access to the cardholder's funds and therefore fall into the category of protected information that must not be disclosed or transferred to third parties.

7.2. The cardholder is responsible for keeping the card details and confidential information safe. Card details and confidential information must not be disclosed to third parties. The cardholder is obliged to keep the card details and confidential information in a safe place that is inaccessible to third parties.

7.3. The use of the card, card details, confidential information (PIN code, 3D Secure and OTP passwords, login and password for the Bank's mobile application), as well as the use of a mobile device containing data about the tokenized card, by third parties is not permitted.

7.4. The cardholder is responsible for compliance with and the consequences of non-compliance with clauses 7.8-7.10 of these Rules. The cardholder agrees that any violation of clauses 7.8-7.10 of these Rules will result in the card being blocked by the Bank unilaterally.

7.5. The cardholder is prohibited from:
7.5.1. writing down any data from the card details, as well as the password/login for ESB mobile banking or mobile device passwords on the card itself, or storing them together with or near the card;
7.5.2. leave the card and/or its details, as well as a mobile device or other confidential information in places accessible for copying and/or recording and/or use by third parties;
7.5.3. disclose to third parties the card details (in whole or in part), one-time passwords, as well as the password/login for the Bank's mobile application, passwords for the mobile device.

7.6. 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 the ESB mobile banking app (including transactions made by scanning a QR code) or using a mobile device (including tokenized transactions) by third parties, shall be borne by the cardholder.

7.7. In the event of loss, theft, or suspicion of use of the card or its details by a third party, and/or if the cardholder receives an SMS/push notification with information about a card transaction that they did not make, as well as in the event of voluntary transfer of a mobile device or confidential information to third parties, or in the event of loss/ theft of a mobile device and/or compromise of a token, the cardholder is obliged to IMMEDIATELY contact the Bank through the official communication channels posted on the Bank's corporate website www.esb.kg, to block the card/token, or block the card independently via ESB mobile banking, selecting the appropriate reason for blocking, when this fact became known to the cardholder or the cardholder had suspicions about this fact. The cardholder is responsible for all card transactions and their actions or inactions and/or the actions or inactions of third parties until the card/ESB mobile banking is blocked

7.8. A lost/stolen card or a card with compromised details or confidential information shall be blocked and shall not be reissued or extended with the same card details. The cardholder must contact the Bank to have a new card issued with new card details. Further use and/or unblocking of lost/stolen/compromised cards is prohibited.

7.9. If a lost/stolen/compromised card has been unblocked at the cardholder's initiative, the cardholder shall bear full responsibility for any subsequent unauthorized charges made to the card. The cardholder shall lose the right to initiate a dispute process in accordance with the rules of payment systems.

7.10. The customer is obliged to comply with the following security requirements in order to prevent unauthorized transactions using the token:

7.10.1. Do not leave your mobile device unattended;

7.10.2. ensure an adequate level of security on the mobile device by using passwords and other possible methods of locking/unlocking the mobile device;

7.10.3. ensure that no fingerprints or other means of authentication of another person, including facial recognition, are registered on the mobile device;

7.10.4. not disclose the password for the mobile device to third parties;

7.10.5. delete all personal data and financial information from the mobile device if its use is discontinued;

7.10.6. immediately contact the Bank by calling the phone number provided on the back of the card or through the official communication channels listed on the Bank's corporate website www.esb.kg if you suspect any unauthorized use of the token, or if your mobile device has been hacked, lost, or stolen;

7.10.7. not block any security features provided on the mobile device to protect the token;

7.10.8. create a complex password and store only their biometric data (fingerprints, facial recognition, etc.) for use with the mobile device;

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

7.10.10. not subject the mobile device to operations that increase privileges/hack the device's operating system (jail break, rooting, etc.);

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

7.10.12. not verify the mobile payment service on mobile device(s) belonging to third parties.

7.11. The cardholder shall be fully liable for any losses incurred as a result of card transactions carried out within the framework of “Friendly Fraud” and/or as a result of ‘Phishing’ and/or “Social Engineering”.

7.12. The cardholder shall bear full responsibility for the sale/transfer of card details and confidential information to third parties, including for the execution of financial transactions using the card at the instruction and in the interests of third parties for the purpose of committing unlawful acts in accordance with the legislation of the Kyrgyz Republic.

7.13. In order to track card account transactions and respond promptly and block the card in case of unauthorized access to the card account, the cardholder is advised to activate the service of receiving SMS/push notifications about card transactions.

7.14. Cardholders are advised to check their card account balance at least once a month. To do

so, cardholders can generate a statement themselves via mobile banking or contact the Bank to request a card account statement.

Chapter 8. Processing Card Transactions

8.1. Card transactions within the framework of payment system rules are processed in two stages:

8.1.1. **Authorization** - Stage 1, which involves blocking funds on the cardholder's card account; at the authorization stage, the available balance of the card account is reduced by the amount of the successfully authorized card transaction.

8.1.2. **Posting** - Stage 2, which involves accepting the card transaction for accounting purposes, which is carried out after all documents for the card transaction have been received. At this stage, the final financial processing of the card transaction takes place, i.e., the debiting or crediting of funds to the cardholder's card account, depending on the type of card transaction (expense or income).

8.2. For the period between the date of authorization and posting of the card transaction, the amount of the card transaction (including fees) is blocked on the cardholder's card account and is finally posted within 33 (thirty-three) calendar days.

8.3. Blocking funds for successful card transactions at the authorization stage leads to a decrease or increase in the available balance of the card account, depending on the nature of the card transaction: expenditure or income. An outgoing card transaction always leads to a decrease in the available balance, while an incoming card transaction increases the available balance of the card account if this is provided for by the rules of the payment systems.

8.4. Transactions are posted after the Bank receives an electronic financial document from the acquiring bank through the relevant payment system.

8.5. If the acquiring bank fails to post the transactions by the deadline specified in clause 8.2. of these Rules, the amount of funds for the successful card transaction is automatically released from the block (unlocked) and becomes available to the cardholder for reuse.

8.6. If the Bank receives a late debit (posting of transactions within a period exceeding 33 calendar days) from the acquiring bank, the Bank shall be entitled to make a non-acceptance debit from the cardholder's card account in the amount of the previously unblocked amounts of successful card transactions.

8.7. At the authorization stage, when blocking the amount on the card account for successful card transactions conducted in a currency other than the currency of the card account, the Bank may apply a multiplier. Card transactions are posted without applying a multiplier.

8.8. Card transaction processing:

8.8.1. When conducting a card transaction in the Bank's acquiring network in a currency other than the card account currency, the card transaction is processed at the Bank's commercial exchange rate set on the day of authorization.

8.8.2. When conducting a card transaction in the acquiring network of a third-party Bank in a currency other than the currency of the card account, the card transaction is processed in EUR at the exchange rate of the payment system on the date of authorization of the card transaction.

8.8.3. In the event of a technical overdraft on the card account, this debt shall be accounted for at the rate of the Interbank Payment System (IPS) in effect at the time the debt was incurred.

8.9. When conducting card transactions in a currency other than the currency of the card account, the Bank shall convert the funds into the currency of the card account without acceptance in accordance with Chapter 12 of these Rules. The cardholder hereby authorizes the Bank to perform such non-acceptance conversion of funds on the card account based on these Rules and the Agreement and without any additional consent in any form from the cardholder.

8.10. A full refund of the amount of the card transaction previously debited from the card account shall be made at the initiative of the acquiring bank/TSP in the full amount and currency of the original card transaction. If the currency of the card account differs from the currency of the card transaction, the card transaction shall be fully canceled at the Bank's commercial

exchange rate set on the date of the original card transaction.

8.11. Partial cancellation of a card transaction is carried out at the initiative of the acquiring bank/TSP in the partial amount and currency of the original card transaction.

8.12. In the event of funds being credited to the card in the form of a credit card transaction (credit and/or credit adjustment, etc.) and/or a reversal card transaction (reversal) that results in an increase in the available balance of the cardholder's card account (hereinafter referred to as a credit/reversal card transaction), the Bank has the right to unilaterally block the card account and/or card for up to 30 (thirty) calendar days if the cardholder does not have documents confirming the validity of credit/reversal card transactions. In the event of a technical overdraft on the card account as a result of the acquiring bank revoking the amount of a previously received credit and/or refund card transaction, the cardholder is obliged to repay the resulting debt on the card account at the Bank's first request.

Chapter 9. Settlement of Disputes on Card Transactions

9.1. In the event of disputed card transactions (financial claims), the cardholder is advised to contact the Bank to submit a standard application for investigation (Application for a disputed transaction (hereinafter referred to as the “Application for disputing a transaction on a card/Bank device”), and, if necessary, provide documents confirming the cardholder's right to a refund for the disputed card transaction.

9.2. If the cardholder's claim is justified, the Bank shall initiate a financial claim against the acquiring bank on behalf of the cardholder in accordance with the rules of payment systems.

9.3. If the acquiring bank agrees with the cardholder's financial claim, the Bank shall refund the amount of the card transaction to the card account in accordance with the procedure and within the time limits established by the rules of the relevant payment systems and the Bank's internal procedures.

9.4. Payment systems impose penalty fees for unjustified financial claims, which may exceed the amount of the disputed card transaction. The Bank has the right to debit penalty fees and the amount of the unjustified financial claim from the card account without the cardholder's consent.

9.5. The following card transactions shall not be subject to dispute on the grounds of fraud or unauthorized access to the card account and shall be deemed to have been performed by the cardholder:

- 9.5.1. card transactions made with the entry of a PIN code, made with the physical presentation of the card, in which the card chip and/or magnetic strip data was read;
- 9.5.2. card transactions made without entering a PIN code, for contact/contactless (PayWave) payments made with the physical presentation of the card;
- 9.5.3. card transactions made with the entry of a 3D Secure password;
- 9.5.4. card transactions made in the ESB mobile banking app, including transactions using a QR code;
- 9.5.5. card transactions made using a card token.

9.6. A card transaction shall be deemed authorized by the cardholder if, within 120 (one hundred and twenty) calendar days from the date of its execution, the cardholder has not submitted an “Application for disputing a transaction on a card/device of the Bank” to the Bank due to unauthorized access to the card account.

9.7. The Bank has the right to refuse to accept an “Application for disputing a transaction on a card/Bank device” if the cardholder's application is submitted more than 120 (one hundred and twenty) calendar days after the date of the disputed card transaction.

9.8. In order to monitor card transactions on the card account and to respond promptly and block the card in case of unauthorized access to the card account, the cardholder is advised to activate the service of receiving SMS/ push notifications for card transactions, as well as regularly generate card account statements themselves in the Bank's mobile application or request them at Bank branches.

Chapter 10. Monitoring of Card Transactions and Card Blocking

10.1. The Bank monitors card transactions in order to identify suspicious, fraudulent, and/or unusual card transactions, with the aim of reducing the risk of unauthorized access to the

card accounts of the Bank's cardholders.

10.2. The Bank may block a card based on the results of monitoring in order to verify the cardholder's involvement in a card transaction, as well as:

10.2.1. if there is suspicion of fraud on the part of the cardholder or the cardholder's involvement in a fraudulent scheme;

10.2.2. if there is suspicion of transactions that fall under the financing of terrorist activities, financing the proliferation of weapons of mass destruction, and legalization ("laundering") of criminal illegal income, as well as if there is suspicion that the cardholder is included in the sanctions lists of the financial intelligence service and in the list of persons, groups, or organizations for which there is information about their involvement in the legalization (laundering) of criminal proceeds.

10.3. In the event of negative reviews of the cardholder by social media users or group members. The Bank shall block the card/account card unilaterally, and blocking for the reasons specified in clause 10.2. of these Rules may be carried out for a period of up to 30 (thirty) calendar days, with the Bank having the right to further extend the blocking period until all circumstances have been clarified.

10.4. If the Bank detects multiple unsuccessful card authorizations: 5 (five) or more unsuccessful card transactions within 2 (two) calendar days, for recurring payments due to closed access and/or insufficient funds and/or lack of communication with the cardholder to clarify participation in the card transaction and/or lack of replenishment of the card account and/or unsubscribing/unlinking the card from recurring payments, the Bank has the right to place the card on a stop list.

Chapter 11. Instructions for Payment via QR Code and Safety Rules

11.1. Instructions for paying with a QR code:

11.1.1. Step 1: Open the bank's mobile app.

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

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

11.1.4. Step 4: After scanning, make sure that the payment details (amount, recipient) match those specified. Check all payment/transfer details carefully.

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

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

11.2. Security rules when making payments/transfers using a QR code:

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

11.2.2. Enable transaction notifications in the bank's app to keep track of all transactions on your account.

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

11.2.4. Before paying/transferring money, verify the authenticity of the scanned QR code to eliminate the risk of QR code substitution (for example, make sure that the static QR code at the point of sale has not been replaced).

11.2.5. If you are redirected to a website when scanning a QR code for payment/transfer, make sure that the URL begins with "https://" and belongs to the official domain. Do not enter your personal or bank card details, including confidential information about your card or mobile app, on unverified or suspicious websites.

11.2.6. In case of an erroneous transfer, if you have transferred/paid the wrong amount via QR code, inform the seller; a conscientious merchant should immediately refund the excess money. All responsibility for payments/money transfers made using a QR code lies with the cardholder. Money transfers, including those made using a QR code, are considered voluntary and irrevocable.

Chapter 12. Currency Conversion

12.1. On the date of settlement with the MPS, the amount of the transaction made with the card is debited from the card account and credited by the payment system to the TSP account.

12.2. **Write-off for a transaction (payment for goods and services) using a Visa card:**

<table>
<tr><td rowspan="2">Card currency</td><td colspan="4">Transaction currency</td></tr>
<tr><td>KGS</td><td>EUR</td><td>USD</td><td>Other currencies</td></tr>
<tr><td>KGS</td><td>No conversion</td><td colspan="3">The transaction amount in a currency other than KGS is converted by the Visa IPS into KGS at the internal IPS exchange rate on the date the funds are debited from the card account.</td></tr>
<tr><td>EUR</td><td>The transaction amount in KGS is converted to EUR at the Bank's exchange rate on the date of debiting the card account.</td><td>No conversion</td><td colspan="2">The transaction amount in a currency other than EUR and KGS is converted by the Visa IPS into EUR at the internal IPS exchange rate on the date the funds are debited from the card account.</td></tr>
<tr><td>USD</td><td>The transaction amount in a currency other than KGS is converted by Visa to USD at the internal exchange rate of Visa on the date of debiting the card account, and then converted by the Bank from USD to KGS.</td><td>The transaction amount is converted by the Visa IPS into USD at the internal IPS exchange rate on the date the funds are debited from the card account.</td><td>No conversion</td><td>The transaction amount is converted by the Visa IPS into USD at the internal IPS exchange rate on the date the funds are debited from the card account.</td></tr>
</table>

12.3. **Write-off for transactions (payment for goods and services) using a Mastercard:**

<table>
<tr><td rowspan="2">Card currency</td><td colspan="4">Transaction currency</td></tr>
<tr><td>KGS</td><td>EUR</td><td>KGS</td><td>Other currencies</td></tr>
<tr><td>KGS</td><td>No conversion</td><td colspan="3">The transaction amount in a currency other than KGS is converted by the Visa IPS into KGS at the internal IPS exchange rate on the date the funds are debited from the card account.</td></tr>
</table>

EUR	The transaction amount in KGS is converted into EUR at the Bank's exchange rate **on the date of debiting** the card account.	No conversion	The transaction amount in a currency other than KGS and EUR is converted by the Mastercard IPS into EUR at the internal IPS exchange rate **on the date the funds are debited** from the card account.	
USD	The transaction amount in KGS is converted to USD at the Bank's exchange rate **on the date of debiting** the card account.	The transaction amount in EUR is converted by the Mastercard IPS into USD at the internal IPS exchange rate **on the date the funds are debited** from the card account.	No conversion	The transaction amount in a currency other than KGS and USD is converted by the Mastercard IPS into USD at the internal IPS exchange rate **on the date the funds are debited** from the card account.

These Rules are an integral part of the Agreement on Opening and Maintaining Bank Accounts (Card Accounts) (for individuals in national and foreign currencies) and are binding on the Cardholder.