TERMS OF USE OF BANK PAYMENT CARDS

Carefully read the Rules and be sure to keep it until the expiration date of the payment card issued to you

1. Terms and Definitions.

Authorization	Authorization of the Issuing Bank on banking operations with Bank payment card.
Card cancellation	Declaring the card invalid and withdrawing it from circulation.
Issuing bank	A bank, which is a member of the payment system, which issues (issuing) cards, as well as responsible for obligations to other banks-members of the payment system.
Bank-Acquirer	Hardware and software complex for issuing and receiving cash, cash withdrawal, recording of cash on the card, obtaining information on transactions made by the Cardholder, making non-cash payments and issuance of card check for all types of transactions performed. ATM is designed for independent fulfillment by a holder of operations with using the card without participation of the authorized employee of the Bank. Further can be found as ATM - Automatic Teller Machine.
Bank account (hereinafter card account)	Account opened by the Bank to the Cardholder for cash flow and execution of transactions by the Cardholder's card.
ATM	Hardware-software complex for issuance and reception of cash, recording of cash on the card, receipt of information on transactions made by the Cardholder, non-cash payments and issuance of card check on all types of transactions made. ATM is designed for independent performance of transactions by the Holder with the card without the participation of the Bank's authorized officer. Further can be found as ATM - Automatic Teller Machine.
Card blocking	Full or temporary prohibition of card transactions.
ATM statement	Card Account Statement generated by ATM at the request of the Cardholder. The ATM Statement covers a maximum of 10 (ten) recent transactions, made on the Cardholder's card account.
Bank payment card (hereinafter referred to as the card)	A payment instrument intended for payment for goods, works and services, transfers and other payments, as well as for receipt of cash within the balance of funds available on the card account. The card is valid only during the period specified on it. No transactions shall be performed with overdue cards no transactions shall be performed.
Cardholder	An individual who has the right to use the card in accordance with the terms of the Banking Services Agreement.
Additional card	Card issued under the card account to the Cardholder's proxy. The cardholder has the right to set a limit on the amount of money of card transactions on the additional card.
Indebtedness	All amounts payable by the Cardholder to the Bank in connection with the issue/reissue of the card/additional card, opening, maintenance (keeping), conducting card operations, closing of the card account, technical overdraft, as well as other amounts payable according to the Bank's tariffs.

Code word	The word (or combination of symbols), specified by the Cardholder in the Application-letter for issue of bank payment card and adherence to the terms of banking services for individuals, by which the Bank can identify the Cardholder and provide information on the status card accounts and cards over the phone.
Limit(s) cash limit	Limits set by the Bank on the maximum amount made by means of the card. The limit(s) may be set both for the amount and currency of a single transaction and for the amount of all transactions made within a certain time.
Interbank Processing Center (hereinafter referred to as IPC)	Hardware and software complex of the national payment system of the Kyrgyz Republic ELKARD, designed for processing transactions made with the use of bank payment cards ELKARD, VISA, Mir, as well as cards of other systems integrated with the IPC system.
Fraudulent transaction	Bank payment card transaction not authorized and not confirmed by the Cardholder.
Irreducible balance	Amount of cash of cash, determined by the Bank, which not subject to authorisation and is the Cardholder's pledge to the Bank.
Abnormal situation	A situation that cannot be resolved by the built-in automatic means of risk management of a separate payment system in accordance with the rules and technology of the system and requires specially organized activities of the operator's or participant's personnel to resolve it of this payment system.
Overdraft	A form of short-term credit, the granting of which enables To the cardholder to make payments by means of the card in excess of the amount ofown payment funds available on the card account.
PIN code	Personal Identification Number, a secret code assigned to each Cardholder and intended to identify such Cardholder. The PIN consists of a sequence of four digits.
Cash point	Cash point.
POS terminal	It is an electronic payment device installed by the Bank at the bank branches for cash withdrawal, in a trade and service enterprise, used when carrying out a card transaction of the Cardholder for payment for goods and services through the card.
TSE	A trade service enterprise with a POS terminal for accepting and card maintenance.

Stop list	List of cards in the Payment system prohibited by the Bank for acceptance asmeans of payment.
Statement of account (hereinafter referred to as "statement")	Report on the balance of funds on the Cardholder's card account, on movements of funds on the card account and transactions performed by means of the card for thespecified period.
Transaction	A card transaction involving the purchase of goods, services, currency exchange,or cash withdrawal that results in the debit or crediting of a card account for the amount of the transaction.
Technical overdraft	Indebtedness arising from excess of payments (expense)transactions) over the available balance on the card account.
Phishing	One of the types of Internet fraud that aims to gain access to confidential user data such as logins, passwords, personal accounts and bank card details. Mostly, it is a method of mass mailings on behalf of a bank, popular companies or organizations, which contain links to false websites that look indistinguishable from the real one,but are in fact fake. The emails politely ask you to update or confirm that your personal information is correct, often mentioning any data issues. You are then redirected to a fake site that looks indistinguishable from the real one, where you are asked to enter credentials. If attackers get hold of the necessary information, it could lead to thetheft of personal data or funds.
CVV code (card verification value 2)	Three-digit code to authenticate the card when paying online andother types of transactions printed on the back of the card.
3D Secure	This state-of-the-art card payment security technology enables to additionally identify the cardholder by entering a 3D Secure password and minimize the risk ofonline fraud using bank payment cards.

1. General Provisions.

1.1. The present Regulations on the Use of Bank Payment Cards (hereinafter referred to as the Regulations) determine the procedure of issuance and servicing of cards by the Bank, the procedure of transactions with the use of cards, as well as the rules for safe use of cards.

1.2. Legal relations between the Holder and the Bank on issue and maintenance of cards are regulated by the Banking Services Agreement, concluded between the Bank and the Cardholder by means of adherence of the Cardholder to the Terms of banking services for individuals of "BAKAI BANK OJSC" (hereinafter referred to as the Agreement).

1.3. It is prohibited to transfer the card to other persons for use or as a pledge. A card presented by an unauthorised person is subject to seizure.

1.4. The Card is the property of the Bank; upon expiry of the Card validity term, the Agreement or upon the first request of the Bank, the Card must be compulsory returned to the Bank.

1.5. These Rules and the Bank's tariffs shall be posted on the Bank's official website www.bakai.kg.

1.6. The Bank shall have the right to unilaterally amend these Regulations.

2. Card issuance procedure

2.1. The bank issues a card directly to the Holder, or to his authorized person. At reception of the card the Holder has to sign in the specially provided for this purpose field on the underside of the card.

2.2. The Card shall be issued together with the PIN code in the PIN envelope, the PIN code may be issued by the Bank in the PIN envelope or through remote banking service channels, if technically possible, the PIN code maybe assigned by the Cardholder himself/herself through a mobile application after authentication.

2.3. In order to protect the funds on the card account of the Cardholder, the Bank strongly recommends not to disclose the PIN-code to the third parties and not to keep it in paper form.

2.4. Upon receipt of the card, the cardholder must make sure that the Latin spelling of his name on the card to the letter coincides with the spelling of his name in the foreign passport, in case of absence of the foreign passport verifies by the ID passport. Otherwise, the Cardholder may have difficulties when paying for purchases abroad.

2.5. The Bank issues a card within 5 (five) business days in Bishkek and 13 (thirteen) business days in the regions ofthe Kyrgyz Republic according to the Bank tariffs.

2.6. In case of urgent issue of a card, it is issued within 2 (two) business days in Bishkek and 7 (seven) business daysin the regions of the Kyrgyz Republic according to the Bank's tariffs.

2.7. The Bank does not perform urgent issuance of a card until the urgent issuance fee is paid in full in accordance with the tariffs.

2.8. In case of issue of a card but the Cardholder's failure to come to the Bank to receive a card within more than 6 (six) months from the date of application, the Bank has the right to cancel the card and not to return to the Cardholder the paid by him commission for its issue and annual maintenance in full or in part.

2.9. On the front side of the Card are:

- the Bank's logo;
- payment system logo;
- built-in chip (microprocessor) - is considered a more reliable means of cardholder's information protection;
- Card number consisting of 16 digits;
- last name and first name (or initials of the first and last name) of the Cardholder (in Latin characters). In case ofpre-issued cards it is allowed to have no surname and first name on the card;
- card expiration date.

2.10. On the reverse side of the Card are:

- a dark-coloured magnetic stripe on which information about the Cardholder is recorded;
- a designated space for the Cardholder's signature;
- number of the 24-hour help line of the Bank and the IPC;
- a verification code (CVV2), which is used for online transactions.

2.11. To prevent damage to the magnetic stripe, it is necessary to observe the rules of card storage:

- Do not leave near sources of open flame;
- do not place near household or other appliances, the radiation of which may distort the information printed onthe magnetic strip of the card;
- Do not expose to mechanical impact;
- do not store in wallets with magnetic locks;
- Do not use as a cleaning agent to remove dirt and frost from car windshields.

2.12. If the magnetic stripe is damaged, the card is reissued at the Cardholder's expense.

3. Use of the PIN code.

3.1. At giving out to the Holder of the card together with the PIN-envelope, it is recommended to open the PIN-envelope at once after receipt, to remember the PIN-code and to destroy the insert and the envelope.

3.2. When issuing the card to the cardholder without the PIN-envelope, the cardholder himself/herself assigns the PIN-code via the Bank's mobile applications. For this, the Cardholder must enter all necessary information

about the card, such as card number, expiration date, assign the PIN-code. To activate the PIN-code, it is necessary to make the first transaction at an ATM entering the set PIN-code.

3.3. Change of PIN-code in ATM of the Bank is made according to the instruction (step-by-step action), described on the screen of ATM. To change PIN-code in ATM, you need to have the card and PIN-code.

3.4. Change of PIN-code via mobile applications of the Bank is made as usual change of PIN-code, but without checking the old PIN-code.

3.5. The combination of digits (4 digits) is chosen at the discretion of the Cardholder. The cardholder should not use obvious, easily assumed digital combinations, for example, the last digits of the phone number, date of birth, etc.

3.6. When entering the PIN-code, the digits on the displays of electronic devices are not specially highlighted, but are replaced by a conventional sign. It is important not to make any mistakes while entering. If an incorrect PIN-code is entered three times in a row (at any time interval, when using one or different electronic devices), the card will be automatically blocked and it will be detained at the ATM or may be confiscated at the service point until the circumstances are clarified.

3.7. Card Transactions confirmed with a set of PIN shall be deemed by the Bank to have been executed by the Cardholder.

4. Application of the map.

- Payment for goods and services in non-cash form in trade and service enterprises, which accept cards forpayment.
- Obtaining cash at banking institutions and through ATMs.
- Conducting transactions on the Internet.
- Conducting transactions through mobile applications and Internet banking.
- Transferring funds from card to card.
- Card account replenishment.

5. The process of paying by card in retail and service establishments.

5.1. All card service points are equipped with signs with the logos of ELKART/VISA PS to inform Cardholders about the possibility of card service at this point.

5.2. To pay for purchased goods or services, you have to show your card to the employee of the sales outlet.

5.3. All transactions with the use of cards in the trade and service enterprises must be carried out in the presence of the Cardholder. This is necessary in order to reduce the risk of unlawful obtaining of personal data of the Cardholder specified on the card.

5.4. In some trade and service organizations in case of large purchases, you may be asked to present your ID card. Therefore, when paying by card, the Bank strongly recommends to have your passport or other identification document.

5.5. The cashier, having accepted the card, performs Authorization with the help of the terminal. For this purpose he puts the card into the reader of the terminal, enters the amount of transaction on the keyboard, or reads it through the contactless chip-reader. The request is sent to the Bank via communication channels. If the Cardholder enters the correct PIN-code and there is enough money on the card account, a receipt is printed in two copies, confirming the transaction. One copy of the receipt shall be given to the cardholder. It is necessary to check the correctness of the data indicated in the cheque. Depending on the adopted technology, the printed receipt may becertified by the signatures of the Cardholder and the cashier.

5.6. It is forbidden to sign a receipt if it does not contain the amount, which will be further debited from the card account with the Bank, or if other details of the transaction (e.g. date) are missing. If inaccuracy in the specified information is detected, it is necessary to refuse to put a signature and ask to cancel the performed operation. If the transaction is cancelled, a cancellation slip must be received.

5.7. The Bank strongly recommends keeping copies of receipts received as proof of payment for goods and services with the card. Keeping these documents guarantees against inaccurate debiting of the card account.

5.8. The Bank recommends that you pay by card only in those trade and service enterprises which you can trust; it is especially important to keep this in mind when travelling to countries with a high level of fraud (Africa, South-East Asia, Latin America, Eastern Europe, Turkey, USA).

6. The process of paying by card online.

6.1. Payment for goods or services on the Internet by payment card includes the types of payments that do notrequire the physical presence of the card at payment, but using the card details, obligatory of which are - the card number, card expiration date, embossed name of the Cardholder (name and surname as indicated on the card). Additionally, when making payments on the Internet, card details such as CVV2, 3D Secure password may be requested in accordance with the terms of service of the Internet resource. To complete the payment, after entering the necessary data, press "Pay".

6.2. By default the client has access to 3D Secure on VISA cards, therefore access to internet transactions on VISA cards is activated by default.

6.3. On cards of national payment system ELKART access to Internet transactions is opened on the basis of the Cardholder's Application.

6.4. All responsibility for the possible consequences of such access, in particular, the risk of unauthorized transactions by third parties on the bank payment card via the Internet shall be borne by the Cardholder. At that,

the Bank has the right not to accept the Applications for refund and/or claim work on these transactions.

6.5. The main issue of ensuring security when making payments in the Internet by means of payment cards is the identification of the Cardholder making the payment. CVV2/CVC2 code is used to make payment in the Internet - shop or other provider of services in the Internet.

6.6. CVV2/CVC2 is a three-digit code printed on the back of the card.

6.7. The Bank recommends making purchases only from verified websites of reputable companies.

6.8. To ensure secure Internet transactions, the Bank recommends making payments on websites supporting 3D Secure security technology. Cards are automatically connected to 3D Secure technology. The cardholder may clarify information on the status of card connection to 3D Secure technology by contacting the Bank. The 3D Secure protocol is not applicable to transactions made by means of the national payment card ELKART.

6.9. When carrying out an operation in the Internet that supports 3D Secure technology, the Cardholder is offered to enter a password that is received via SMS to the number specified by the Cardholder at the time of cardissuance. The SMS password is a one-time password and is valid for only one purchase.

6.10. Prior to carrying out an Internet transaction, the Cardholder must:

- Keep your browser updated and install security updates in a timely manner;
- Check the validity period of the card, no blocking, etc;
- Make sure there are enough funds on the card to make a payment;
- Refrain from making transactions on automatically redirected pages or pop-ups;
- For payment and order confirmation, the Cardholder must clearly follow the instructions of the site;

6.11. Possible reasons for payment refusal:

- There are not enough funds on the card;
- Internet payments are not allowed on the card or other restrictions are set;
- The card has expired;
- The cardholder has not entered a 3D Secure password;
- The card is blocked;
- The bank may have imposed a ban on prohibited transactions;
- When opening the card, wrong/lost phone number was specified and a message with 3D Secure code is sent to the wrong number;
- The site or country is blacklisted and considered high risk;
- Not allowed by browsers cookies;

For clarification of the reasons the Cardholder should contact the Bank.

6.12. In order to cancel the payment, in full or in part, the Cardholder has to contact the customer service of the onlineshop to initiate refunding the payment.

6.13. It is necessary to carefully analyze the website address (URL) to which a redirect is sent. In most phishing cases, even though the site looks identical to the real one, the URL may be different from the original (for example, ending in. com instead of. gov).

6.14. The Client has the right to refuse access to making payments via Internet, for this purpose he/she should applyto the Bank with his/her passport for execution of application to disable access to Internet operations.

7. Obtaining cash from an ATM.

7.1. Before using the ATM, you should inspect it for the presence of uncharacteristic devices: unevenly mounted PIN-keyboard, overlays above the ATM screen and other suspicious devices. In case of presence of suspicious devices, you should refrain from making transactions at such ATM, if possible, inform the Bank employees about your suspicions by the phone number indicated on the ATM or by calling the Contact Center.

7.2. Receipt of cash from ATM is confirmed by PIN-code and is made by the Cardholder in self-service mode, according to the instructions described on the screen of ATM.

7.3. In order to cancel the service, it is necessary to cancel the operation by clicking "Cancel" /"Cancel."

7.4. When entering the PIN-code, make sure that no unauthorized person can see it. In case you enter incorrect PINcode three times, the card will be blocked and can be withdrawn by ATM.

7.5. Do not accept assistance offered by third parties for transactions.

7.6. In accordance with the Regulation "On bank payment cards in the Kyrgyz Republic", the amount of a single transaction withdrawn by the Cardholder through an ATM must not exceed 250 (two hundred and fifty) settlement indexes in national currency or its equivalent in foreign currency. In ATMs of different banks the single amount of cash withdrawal can differ.

7.7. Simultaneously with the cash withdrawal, the ATM will return the card and print a receipt.

7.8. It is advisable to save the receipts you receive via an ATM, as they are authenticated with a PIN and serve as proof of transaction.

7.9. When the message "Pick up your card" appears on the screen - you should immediately pick up your card, otherwise it will be confiscated by ATM.

7.10. It is necessary to retrieve the cash dispensed by ATM within 20 (twenty) seconds, otherwise the security system will be activated and ATM will retrieve it back. This is provided in order to minimize the risks of cash withdrawal from ATMs.

7.11. In case of seizure of a card or funds by an ATM, the Cardholder should not leave immediately, but should make sure that they are really seized. Otherwise, after the Cardholder moves away from the ATM, he/she may return the card or give out the money.

7.12. The card transaction for a valid card when the correct PIN code is entered may be rejected for the following reasons:

- The requested amount may not be dispensed with banknotes available in the cash drawers of the ATM. The requested amount shall be a multiple of the minimum denomination of banknotes specified in the ATM manual;
- The requested amount exceeds the single withdrawal limit determined by the dimensions of the cash withdrawal device of the ATM. It is necessary to split the requested amount into parts and repeat the operation several times;
- The requested amount exceeds the amount of money available to the Cardholder. It is possible to request a smaller amount, the amount of which can be clarified by calling the function of printing out the balance of money on the card account.
- The requested amount exceeds the daily limit available to the cardholder on the device. It is necessary to applyto the bank branch, where the account is opened, for withdrawal of the required amount through the bank's cash desk.
- When withdrawing cash from ATM, make sure that ATM serves cards of the payment system you need (usually, ATMs bear the logos of payment systems that are served by the ATM).

8. Transferring funds from card to card.

8.1. You can transfer funds from one card to another using the "CardEX" money transfer service via ATMs, according to the instructions described on the screen of the ATM. Note: it is necessary for ATM to support this functionality. Transfers can be made to any ELCART and VISA cards supported in "MPC" processing

8.2. Transfer via Mobile Banking/Internet Banking of the Bank is made in the Transfers section.

8.3. Translation via other mobile applications.

8.4. In order to transfer money using these services, you need to know the full card number, in some cases the expiry date of the recipient's card, and indicate the transfer amount.

9. Card account replenishment.

9.1. You can replenish your card account by one of the following ways

- in cash at any branch or savings bank of the Bank;
- by wire transfer from other Banks. It is necessary to find out card account details in advance;
- in the Bank's payment terminals free of charge;
- in the Bank's payment terminals, as well as in QuickPay, Megacom, Pay24 terminals in accordance with the tariffs;
- by wire transfer via mobile applications.

10. Card withdrawal cases.

10.1. Causes of ATM card hijacking:

- putting the card on a hard stop list by the issuing bank;
- if the PIN-code of the card has been entered incorrectly more than 3 (three) times;
- expiration of the card;
- communication failure;
- ATM malfunction.

10.2. If the card is withdrawn by an ATM, the following instructions must be followed:

- first of all, it is necessary to make sure that the card is really captured and the ATM will not issue the card to the next customer;
- in case the ATM has actually withdrawn the card, you should contact the bank which installed the ATM. The bank's coordinates and telephone numbers are usually listed on the ATM itself or near the location of the ATM;
- by contacting the bank, which operates the ATM, to explain the situation and clarify the time and ways of card return;
- if it was not possible to identify the bank servicing the ATM, you should call to the issuing bank and inform the country, city, street and house number where the ATM is located. The Bank's specialists will give you necessary advice on further actions;
- You must bring your ID card in order to receive the card.

11. What to do if the card is lost/stolen.

11.1. If the card is lost or stolen, immediately contact the Bank (or the Processing Centre or any branch of the Bank at its location) with a verbal or written request to block the card (application):

Call - center MPC: **+996 (312) 63 76 96; +996 (312) 66 43 25.**

- during working hours Call-center of the Bank: **+996 (312) 61-00-61.**

11.2. The sooner you inform the Bank about the lost/stolen card, the less likely it is that unauthorized persons may usethe funds on the card.

11.3. The cardholder bears responsibility for the card transactions, carried out before the entry into force of the blocking of the card and is released from it from the moment of the entry into force of the blocking of the card.

11.4. If a card previously reported as lost or stolen is discovered by the Cardholder himself/herself, the Bank must be

notified immediately. One should not try to use this card, as it will be withdrawn by ATM. It is necessary to apply to the Bank to unblock or re-issue the card.

11.5. The Bank strongly recommends that you check your card account statement in the following months to ensure that no unauthorised transactions have been made on the card.

12. Abnormal situations in the payment system.

12.1. The following abnormal situations may occur in the payment system:

- power outages;
- communication link failures;
- system hardware and software failures;
- force majeure circumstances (fire, flood, earthquake, etc.)

12.2. In case of occurrence of these situations in the payment system, the Bank shall not be liable for performance ofobligations under the Agreement.

12.3. The Bank takes all possible measures to ensure uninterrupted operation of equipment and systems involved inthe process of providing services on card transactions.

13. Suspicious card transactions.

13.1. If you find any disputable operation in the card account statement, you need to contact an employee of the Bank to clarify the amount spent. In case of unauthorized use of card funds, it is necessary to write a claim application.

13.2. In case of suspicion of fraudulent/uncharacteristic actions on the card, the Bank has the right to block the card until clarification/confirmation with the Cardholder.

13.3. The claim application on correctness of operation is submitted within 45 (forty five) working days from the moment of operation fulfillment. After expiration of the given term the Bank has the full right not to accept the claim application from the Holder.

13.4. On VISA cards the minimum amount of dispute on international transactions is 15 (fifteen) US dollars or the equivalent in local currency.

–

13.5. The dispute resolution process is as follows:

- after providing a written application of the Cardholder, the Bank shall investigate the claim transaction for compliance with the validity of the transaction. The Bank has the right to request additional documents (check atpayment, check at withdrawal of money from ATM), confirming the fact of transaction;
- in case of confirmation of incorrect write-off of funds not through the fault of the Cardholder, the Bank makes a refund.
- the time for consideration of the claim and decision making by the Bank depending on the reasons may take up to (2) two months.

13.6. The Bank rejects the Cardholder's claims regarding the shortage(s) when receiving money from ATM in case of absence of surplus in ATM, determined by means of ATM cash revision/ recalculation, made on the basis of the Cardholder's written application.

13.7. The Bank shall timely inform the authorized body according to the current legislation of the Kyrgyz Republic in case of revealing the fact of suspicious transactions, including fraudulent ones, on the Card Holder's card.

14. Security rules for Cardholders to prevent card fraud.

14.1. It is prohibited to transfer the card to a third party, except for the transfer of the right to use the card by proxy, in accordance with the current legislation of the Kyrgyz Republic.

14.2. Keep your card in a safe place. You should not leave the card in places where someone can take it and/or copy the card number/signature/CVV code and other card data.

14.3. To avoid damage to the magnetic stripe, do not keep the card in close proximity to sources of electromagnetic radiation (cellular phones, TV sets, microwave ovens, audio and video equipment, etc.). Be careful when makingpayments in places where magnetic coding of goods is used - it may lead to refusal to process the card or to incorrect processing of the card at ATMs and POS-terminals. The use of the card by a third party is considered by the Bank as a gross violation of these Rules and may entail termination of the Agreement at the initiative of the Bank.

14.4. The Bank rejects the Cardholder's claims regarding the shortage(s) when receiving money from ATM in case of absence of surplus in ATM, determined by means of ATM cash revision/ recalculation, made on the basis of the Cardholder's written application.

14.5. It is necessary to keep the PIN-code in secret. Communication of the PIN-CODE to the third person (relative, colleague, friends etc.) can lead to unauthorized use of the card, i.e. to the spending of the money belonging to the Holder. The transactions conducted with the PIN-CODE input shall be recognized as made by the Cardholder and shall not be disputed.

14.6. It is prohibited to keep the card near the PIN code, it is prohibited to write the PIN code on the card itself or in the documents stored near the card.

14.7. When making a purchase, you must not lose sight of the card. It is necessary to pick up the card immediately after completing the transaction and verify the authenticity of the card.

14.8. All transactions with the card shall be performed in the presence of the Cardholder at the Points of sales.

14.9. Prior to ATM transactions, pay attention, if there are no any external signs of ATM malfunction, having found

any extraneous devices near or on ATM, inform the bank servicing that ATM and use another ATM.

14.10. It is not recommended to use those ATMs, which display a message asking to switch to other ATMs. Banks do not post such messages.

14.11. If possible, try to use ATMs with which the Cardholder is already familiar. In other cases, choose ATMs in well-lit and convenient locations.

14.12. While at an ATM, the Cardholder must not allow anyone to distract him/her.

14.13. It is recommended that you keep all receipts for later tracking of expenses and do not throw receipts in the wastebin in a public place.

14.14. The Bank strongly recommends not to enter card data (printed on the card itself) when requesting dubious internet sites, as well as when requesting any mobile phone manufacturers (in case of uncertainty or limited/ lack of information), as otherwise there is a risk of theft or withholding of funds without the Cardholder's knowledge.

14.15. If possible, it is advisable to use ATMs during daylight hours and at night to choose well-lit areas and make sure that unauthorised persons are not standing too close when making a transaction.

14.16. When entering the PIN, make sure that no unauthorised person sees the PIN.

14.17. 14.17. To ensure control of card transactions, it is recommended to use the service "SMS notification". The service is activated by the Bank based on the Cardholder's application.

14.18. It is necessary to update the contact information provided to the Bank, so that the Bank has an opportunity tocontact the Cardholder by phone/email/ SMS, for example, in case of a suspicious card transaction.

14.19. You should follow safe online behaviour and not click on links sent in suspicious or obscure emails or through Facebook.

14.20. You should not download attachments from emails that the Cardholder did not expect.

14.21. The cardholder must keep his/her passwords secure and not disclose them to anyone else.

14.22. The cardholder must not disclose his personal data to anyone - whether by phone, in person or in an e-mail message.

14.23. It is necessary to carefully analyze the website address (URL) to which the Cardholder was redirected. In most phishing cases, even though the site looks identical to the real one, the URL may be different from the original (for example, ending in .com instead of .gov).

14.24. You need to keep your browser updated and install security updates in a timely manner.

14.25. In accordance with the Law of the Kyrgyz Republic "On Prohibition of Gambling Activities in the Kyrgyz Republic", the Bank introduced a ban on banking operations related to gambling activities, betting shops and casinos (including Internet space) and other prohibited types.

15. Card Restrictions.

15.1. To reduce the risk of unauthorized card transactions the Bank is entitled to establish restrictions and limits on card transactions. The Bank independently determines the amount of restrictions and limits, as well as the conditions, terms and procedure of their establishment. The Bank establishes daily card limits. The Cardholder may carry out Transactions with the Card within the limits of daily limits, the list of which is available on the Bank's website www.bakai.kg.

15.2. The standard restrictions set by the Bank may be changed upon the Cardholder's written application to the Bank.

15.3. The Bank has imposed additional restrictions on contactless cards:

- carrying out transactions without entering PIN-code within the set limits according to the Bank's tariffs;
- carrying out transactions by entering PIN-code in excess of the set limits according to the Bank's tariffs.

16. Card validity period and termination of the Agreement.

16.1. The expiry date (month and year) is indicated on the card. The card is valid until the end of the last day of the month indicated on it. All expired cards shall be blocked and surrendered to the Bank.

16.2. The Cardholder may close the Card and terminate the Agreement unilaterally by submitting an application forcancellation of the Card.

16.3. The Bank shall be entitled to block/annul the Card and terminate the Agreement with the Cardholder in case of the Cardholder's failure to comply with the terms of these Rules and the Agreement.

16.4. Upon termination of the Agreement the Cardholder shall repay the existing debt and surrender all the cards issued on his/her card account.

16.5. In case of termination of the Agreement on the initiative of either party, the annual service fee and other fees paid by the Cardholder shall not be refunded.

16.6. The card account balance shall be issued if there is no debt to the Bank.

17. Other terms and conditions.

17.1. The cardholder must notify the Bank within 5 (five) days of all changes in the data specified in the application-letter for the card issue and adherence to the terms of banking service and other documents related to the card issue by providing the Bank with the documents containing the changes. The Bank shall not be liable for consequences of untimely notification of changes of these data.