RULES FOR USING BANK PAYMENT CARDS

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

1. Terms and Definitions.

Authorization	Authorization Issuing bank for realization of banking operations using the Bank payment card.
Canceling a card	Declaring the FIC card invalid and withdrawing it from circulation.
Issuing bank	Bank, which is member of payment system,(issuing) IFC cards, as well as responsible for obligations to other banks-participants of the payment system.
Bank-Equalizer	The bank authorized to carry out acquiring, the owner of the network of peripheral devices, which provides the ability to carry out 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.
Bank account (hereinafter card account)	Card Hasan account opened by the Bank to the Cardholder for cash flowfunds and transactions on the card of the IFC cardholder.
ATM	Hardware-software complex for issuing and accepting cash, recording cash on the FIC card, obtaining information on the transactions made by the Cardholder, making non- cash payments and issuing a card check on all types of transactions made. ATM is designed for the Cardholder to make transactions using a card independently without the participation of an authorized employee of the Bank. Further can be found as ATM - Automatic Teller Machine.
Blocking a card	Full or temporary ban on transactions with the IFC card.
ATM statement	Card Account Statement generated by ATM at the request of the Cardholder. The ATM statement covers a maximum of ten (10) 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 term specified on it. By no transactions are performed on overdue cards.
Cardholder	An individual entitled to use the IFC card in accordance with the terms and conditions of the Banking Service Agreement.
Additional	IFC card issued under the card account to the Cardholder's proxy IFC. The IFC cardholder has the right to set a limit on the amount of money of cardtransactions on the additional card of the IFC.
Indebtedness	All amounts to be paid by the IFC Cardholder to the Bank in connection with the issue/reissue of the card/additional card, opening, maintenance (keeping), conducting card operations, closing the card account, technical overdraft, as well as other amounts payable according to the Bank's rates.
Code word	The word (or combination of symbols) specified by the Cardholder in the Application- letter for the issue of a bank payment card and adherence to the terms of banking services for individuals, by which the Bank can identify the Cardholder and provide information about the status card accounts and cards over the phone.
Limit(s) cash limit	Limits set by the Bank on the maximum amount made through the card. The limit(s) can 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 operation	Bank payment card transaction not authorized and not confirmed by the Cardholder.
Irreducible balance	Amount of money funds, determined by Bank, which not subject to authorization and is a pledge of the Cardholder to the Bank.
Abnormal situation	A situation that cannot be solved by 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.
IFC	Islamic window - "Islamic Financial Center" BAKAI BANK OJSC
PIN code	Personal Identification Number, a secret code assigned to to each Cardholder and intended to identify such Cardholder. The PIN consists of asequence of four digits.
Cash point	Cash point.
POS terminal	This is an electronic payment device installed by the Bank in the bank branches for cash withdrawal, in trade and service enterprises, used when carrying out a cardtransaction of the Cardholder to pay for goods and services through the card.
STE	Service and trading enterprise with a POS terminal for accepting and card service.
Stop list	List of cards in the Payment system prohibited by the Bank for acceptance as means of payment.
Statement of Account (hereinafter referred to as a statement)	Report on the balance of funds on the card account of the cardholder, on the movements of funds on the card account and transactions made by means of the card for the specified period.
Transaction	Transaction with the use of the card in the purchase of goods, services, currencyexchange or cash receipt, which results in debiting or crediting the card account for the amount of the transaction.
Technical overdraft	Indebtedness arising from the excess of payments (expenditures transactions) over the available balance on the card account.
Phishing	One of the types of Internet scams that aim to gain access to confidential user data, such as logins, passwords, account and bank card data. Basically, this method is used to send mass newsletters on behalf of a bank, popular companies or organizations, which contain links to false websites that look indistinguishable from the real ones, 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. Then you are redirected to a fake site that looks indistinguishable from the real one, where you are asked to enter your credentials. If attackers get their hands on the necessary information, it may lead to the theft of personal data or funds
CVV code (card verification value 2)	A three-digit code to verify the authenticity of the card when paying online and other types of operations on the back of the card.
3D Secure	This is a modern technology of card payments security in the Internet, allows you to further identify the cardholder by entering a 3D Secure password, and minimize the risk of online fraud with the use of bank payment cards.

2. General Provisions.

2.1. These Rules for the use of bank payment cards of IFC (hereinafter referred to as the Rules) determine the procedure for issuance and servicing of IFC cards (hereinafter referred to as the cards) by the Bank, the procedure for transactions using the cards, as well as the rules for the safe use of the card.

2.2. 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 Card Holder by the Cardholder's accession to the Terms and Conditions of banking services for individuals of the Islamic Window - "Islamic Financial Center" BAKAI BANK OJSC (hereinafter referred to as the Agreement) and these Rules.

2.3. Transferring the card to other persons for use or as collateral is prohibited. A card presented by an unauthorizedperson is subject to confiscation.

2.4. The card is the property of the Bank, upon expiry of the card, the Agreement or at the first request of the Bank,the card must be mandatorily returned to the Bank.

2.5. These Rules and the Bank's tariffs are posted on the Bank's official website www.bakai.kg, www.ifcenter.kg.

2.6. The Bank has the right to unilaterally amend these Rules by posting a new version on the Bank's official websitewww.bakai.kg, www.ifcenter.kg.

3. Card issuance procedure

3.1. The bank issues the card directly to the Holder, or to his authorized person. At reception of the card the Holder should sign in the specially provided for this purpose field on the back side of the card.

3.2. The card is issued together with the PIN code in the PIN envelope, the PIN code can be issued by the Bank inthe PIN envelope or through remote banking channels, if technically possible the PIN code can be assigned by the Cardholder through a mobile application after authentication.

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

3.4. 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 the absence of a foreign passport check with the ID passport. Otherwise, the Cardholder may have difficulties when paying for purchases abroad.

3.5. The Bank issues the card within 5 (five) business days in Bishkek, and 13 (thirteen) business days in the regionsof the Kyrgyz Republic according to the Bank's tariffs.

3.6. In the case of urgent production, the card is issued within 2 (two) working days in Bishkek, and 7 (seven) working days in the regions of the Kyrgyz Republic, according to the Bank's tariffs.

3.7. The bank does not issue a card until the urgent issuance fee is paid in full according to the tariffs.

3.8. 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 fee paid by him for its issue and annual maintenance in full or in part.

3.9. On the front side of the Card are:

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

3.10. On the back side of the Card are:

- a dark-colored magnetic strip on which the information about the Cardholder is recorded;
- a designated place for the Cardholder's signature;
- number of the round-the-clock reference telephone number of the Bank and the IPC;
- A verification code (CVV2), which is used for online transactions.

3.11. 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 devices, the radiation of which can distort the information printed on themagnetic strip of the card;

- Do not expose it to mechanical impact;
- do not store in wallets with magnetic locks;
- Do not use as a means of cleaning the windshields of cars from dirt and frost.

3.12. If the magnetic strip is damaged, the card is reissued at the expense of the Cardholder.

4. Using the PIN code.

4.1. When the card is issued to the cardholder with the PIN-envelope, it is recommended immediately upon receipt to open the PIN-envelope, memorize the PIN-code and destroy the insert and the envelope.

4.2. When issuing the card to the Cardholder without a PIN-envelope, the Cardholder himself assigns a PIN-code through mobile applications of the Bank. For this, the Cardholder must enter all necessary information about thecard, such as the card number, expiration date, assign the PIN code. To activate the PIN-code, it is necessary to make the first transaction at an ATM by entering the set PIN-code.

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

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

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

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

4.7. Card transactions confirmed by the set of PIN-code are considered by the Bank as made by the Cardholder.

5. Application of the card.

- Payment for goods and services in cashless form in trade and service enterprises that accept cards, FIC, except for purchases in establishments whose activities are prohibited by Shariah (specialized institutions such as alcohol, tobacco stores, entertainment facilities, casinos, betting shops, sites with obscene and shameful content,etc.).
- Receiving cash in banking institutions and through ATMs.
- Conducting transactions on the Internet.
- Conducting transactions via mobile applications and Internet banking.
- Transferring money from card to card.
- Replenishment of the card account.

6. The process of payment by card in sales and service enterprises.

6.1. All card service points are equipped with signs with the logos of ELKARD/VISA PS to inform Cardholdersabout the possibility of card service at this point.

6.2. To pay for purchased goods or rendered services, you need to show the employee of the sales outlet a card.

6.3. 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 to reduce the risk of unlawful obtaining of personal data of the Cardholder specified on the card.

6.4. In some retail and service organizations in case of large purchases, you may be asked to show proof of identity. Therefore, when paying by card, the Bank strongly recommends that you have your passport or other identity document.

6.5. The cashier, after accepting the card, performs authorization with the help of the terminal. To do this, he puts thecard into the reader of the terminal, types in the amount of transaction on the keyboard, or reads through a contactless chip-reader. The request is received by the Bank through communication channels. If the Cardholderdials the correct PIN-code and there is enough money on the card-account, a receipt is printed in two copies, confirming the transaction. The cardholder is given one copy of the check. It is necessary to check thecorrectness of the data specified in the check. Depending on the adopted technology, the printed receipt may be certified by the signatures of the Cardholder and the cashier.

6.6. It is forbidden to sign the receipt if it does not contain the amount, which will be later debited from the card account at the Bank, or if other details of the transaction (e.g., date) are missing. If you find inaccuracies in

the specified information, you should refuse to put a signature and ask to cancel the performed operation. If the transaction is cancelled, a receipt of cancellation is required.

6.7. The bank strongly recommends keeping copies of receipts received as proof of payment for goods and services by card. Keeping these documents guarantees against inaccurate write-off of funds from the card account.

6.8. The bank recommends that you pay by card only in those merchants that inspire confidence, it is especially important to keep this in mind when traveling to countries with high levels of
fraud (African countries, Southeast Asian countries, Latin American countries, Eastern European countries,Turkey, USA).

7. The process of paying by card on the Internet.

7.1. 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 with the use of 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".

7.2. By default on VISA cards the client has access to 3D Secure, in this regard, access to Internet transactions on VISA cards is connected by default.

7.3. For cards of the national payment system ELKARD access to Internet transactions is opened on the basis of the Cardholder's Application.

7.4. 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. In this case, the Bank has the right not to accept applications for refunds and / or claim work on these transactions.

7.5. The main issue of security when making payments on the Internet with the help of payment cards is the identification of the Cardholder making the payment. CVV2/CVC2 code is used to make payment in the Internet
- store or other provider of services in the Internet.

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

7.7. The bank recommends making purchases only on trusted sites of reputable companies.

7.8. To ensure secure online transactions, the Bank recommends making payments on sites that support 3D Secure security technology. Cards are connected to 3D Secure technology automatically. To clarify the status of the card's connection to the 3D Secure technology, the cardholder may contact the Bank. The 3D Secure protocol does not apply to transactions made by means of the national payment card ELKARD.

7.9. When conducting an operation on the Internet that supports 3D Secure technology, the Cardholder is offered to enter a password that comes via SMS to the number specified by the Cardholder at the time of card issuance.The SMS password is a one-time password and is valid for only one purchase.

7.10. Before making an operation on the Internet, the Cardholder must:
- Keep your browser updated and install security updates on time;
- Check the validity of the card, no blocking, etc;
- Make sure you have enough money on your 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;

7.11. Possible reasons for payment refusal:
- There are not enough funds on the card;
- The card prohibits payments on the Internet or other restrictions;
- The card has expired;
- The cardholder did not specify a 3D Secure password;
- The card is blocked;
- The bank may have imposed a ban on prohibited transactions;
- When you opened the card, you entered a wrong/lost phone number and the message with the 3D Secure codecomes to the wrong number;
- The site or country is blacklisted and considered high-risk;
- Not allowed by browsers cookies;

To find out the reasons, the Cardholder should contact the Bank.

7.12. To cancel the payment, in full or in part, the Cardholder should contact the customer service of the online

store to initiate a refund.

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

7.14. The client has the right to refuse access to make payments through the Internet, to do this, you must contact the
Bank with your passport to draw up an application to disable access to Internet transactions.

8. Getting cash from an ATM.

8.1. Before using the ATM, you should inspect it for the presence of uncharacteristic devices: unevenly mounted PIN-keyboard, overlays over 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.

8.2. 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.

8.3. In order to cancel the service, you must cancel the operation by clicking
"Cancel" /"Cancel".

8.4. When entering the PIN-code, make sure that no one else can see it. If you enter the PIN-code incorrectly threetimes, the card will be blocked and can be withdrawn by the ATM.

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

8.6. 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. The single withdrawal amount may be different in ATMs of different banks.

8.7. The ATM will return the card and print a receipt at the same time as it dispenses cash.

8.8. It is recommended to save the receipts received through the ATM, as it is certified by a PIN code and is a confirmation of the transaction.

8.9. When the inscription "Pick up your card" appears on the screen - you must immediately pick up the card, otherwise it will be detained by the ATM.

8.10. It is necessary within 20 (twenty) seconds to take the money given out by ATM, otherwise the security system will be triggered and ATM will take it back. This is provided in order to minimize the risks of receiving money from ATMs.

8.11. If a card or funds are seized by an ATM, the Cardholder should not immediately walk away, but should verify that they have actually been seized. Otherwise, after the Cardholder moves away from the ATM, the Cardholdermay return the card or cash.

8.12. A card transaction for a valid card when the PIN code is correct may be rejected for the following reasons:

- The requested amount cannot be dispensed with the banknotes available in the ATM cassettes. You should request the amount multiple of the minimum denomination of banknotes, specified in the instruction to this ATM;
- The requested amount exceeds the one-time withdrawal limit determined by the dimensions of the ATM cash withdrawal device. 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 printout function of the balance of moneyon the card account.
- The requested amount exceeds the daily limit available to the cardholder on the device. You should contact the bank branch where the account is opened to withdraw the required amount through the bank's cash desk.
- When cashing out money at an ATM, make sure that the ATM serves the cards of the payment system you need (usually ATMs have the logos of the payment systems that are served by the ATM).

9. Transferring money from card to card.

9.1. 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: you need to have an ATM that supports this functionality. Transfers are available to any of the ELCARD and VISA cards supported in IPC processing

9.2. Transfer via mobile banking/Internet banking of the Bank is carried out in the Transfers section.

9.3. Translation via other mobile applications.
9.4. To transfer money through these services, you need to know the full card number, in some cases the expirationdate of the recipient's card, and specify the amount of the transfer.

10. Replenishment of the card account.

10.1. You can replenish your card account in one of the following ways:
- in cash at any branch or savings bank of the Bank;
- by wire transfer from other Banks. You need to know the details of the card account beforehand;
- in the Bank's payment terminals free of charge;
- in the Bank's payment terminals, as well as in QuickPay, Megacom, Pay24 terminals according to the tariffs;
- by wire transfer via mobile applications.

11. Cases of card withdrawal.

11.1. Causes of card hijacking by an ATM:
- putting the card on a hard stop list by the issuing bank;
- If the PIN-code of the card is entered incorrectly more than 3 (three) times;
- expiration of the card;
- communication failure;
- ATM malfunction.

11.2. If the card is withdrawn by an ATM, the following instructions must be followed:
- first of all, you need to make sure that the card is really captured and the ATM will not give the card to the next customer;
- In case the ATM has actually withdrawn the card, you should contact the bank that installed the ATM. The bank's coordinates and phone numbers are usually listed on the ATM itself or near the location of the ATM;
- by contacting the bank that services the ATM, it is necessary to explain the situation and clarify the time and ways to return the card;
- If it was not possible to identify the bank that services the ATM, you should call the issuing bank and report the country, city, street and house number where the ATM is located. Bank specialists will give the necessary advice on further actions;
- You must have your ID card in order to receive the card.

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

12.1. If your card is lost or stolen, you must immediately contact the Bank (or the Processing Center or any branch of the Bank at your location) with a verbal or written request to block your 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.**

12.2. The sooner you inform the Bank about the loss/theft of the card, the less likely it is that unauthorized persons can use the funds on the card.

12.3. The cardholder is responsible for the card transactions carried out before the entry into force of the blocking of the card and is exempt from it from the entry into force of the blocking of the card.

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

12.5. The bank strongly recommends that you check your card account statement in the following months to make sure that no unauthorized transactions have been made on the card.

13. Abnormal situations in the payment system.

13.1. The following abnormal situations can occur in the payment system:
- power outages;
- communication channel failures;
- system hardware and software failures;
- force majeure (fire, flood, earthquake, etc.).

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

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

14. Suspicious card transactions.

14.1. If you find a disputable transaction in the card account statement, you need to contact an employee of the Bank to clarify this or that amount carried out. In case of unauthorized use of funds on the card, it is necessary to writea claim application.

14.2. In case of suspicion of fraudulent/uncharacteristic actions on the card, the Bank has the right to requestadditional information and documents. In case of failure to provide the information and documents requested by the Bank, the Bank has the right to block the card until the clarification/provision of confirmations from the Cardholder.

14.3. 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.

14.4. On VISA cards, the minimum amount of dispute on international transactions is fifteen (15) U.S. dollars or the equivalent in local currency.

14.5. The dispute resolution process is as follows:

- after providing a written application of the Cardholder, the Bank carries out an investigation of the claim transaction for compliance with the validity of the transaction. The Bank has the right to request additional documents (check at payment, check at withdrawal of money from ATM), confirming the fact of transaction;
- in the case of confirmation of the incorrect withdrawal of funds through no fault of the Cardholder, the Bank makes a refund.
- the period of consideration of the claim and decision-making by the Bank, depending on the reasons, may take up to (2) two months.

14.6. The Bank refuses to satisfy the Cardholder's claims regarding the shortage(s) when he/she receives money from the ATM if there is no surplus in the ATM, determined by the inspection/ recount of the ATM cash, made on thebasis of the Cardholder's written application.

14.7. The Bank must promptly report information to the authorized body, according to the current legislation of the Kyrgyz Republic in case of detection of suspicious transactions, including fraudulent, on the card of theCardholder.

15. Security rules for Cardholders to prevent card fraud.

15.1. It is forbidden to transfer the card to a third party, except for the transfer of the right to use the card by proxy, in accordance with applicable law of the Kyrgyz Republic.

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

15.3. To avoid damaging the magnetic stripe, do not keep your card in close proximity to sources of electromagnetic radiation (cellular phones, televisions, microwave ovens, audio and video equipment, etc.). Be careful when making payments in places where magnetic coding of goods is used - it can lead to refusal in processing or incorrect processing of the card in 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 on the initiative of the Bank.

15.4. The Bank refuses to satisfy the Cardholder's claims regarding the shortage(s) when he/she receives money fromthe ATM if there is no surplus in the ATM, determined by the inspection/ recount of the ATM cash, made on thebasis of the Cardholder's written application.

15.5. It is necessary to keep the PIN-code in secret. Informing of PIN-CODE to the third person (relative, colleague, friends and etc.) can lead to unauthorized use of a card, i.e. expenses of money belonging to the Holder. Transactions carried out with PIN-CODE input are recognized as made by the Cardholder and are not subject to contestation.

15.6. It is forbidden to keep the card near the PIN-code, it is forbidden to write the PIN-code on the card itself or inthe documents stored near the card.

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

15.8. At points of sale all transactions with the card must be made in the presence of the Cardholder.

15.9. Before you make a transaction at the ATM, pay attention, if there are no external signs of ATM malfunction, ifyou find any foreign devices near or on the ATM, inform the bank servicing that ATM and use another ATM.

15.10. It is not recommended to use those ATMs which display a message asking to switch to other ATMs.

Banks donot post such messages.

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

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

15.13. It is recommended that you keep all receipts for future reference and do not throw receipts in the trash can in a public place.

15.14. The Bank strongly recommends not to enter card data (printed on the card itself) when requesting dubious Internet sites, as well as when requesting the manufacturers of any cell phones (in case of uncertainty or limited/unavailable information), as otherwise there is a risk of theft or withholding money without the knowledge of the Card Holder.

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

15.16. When entering the PIN-code, make sure that the PIN-code is not seen by unauthorized persons.

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

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

15.19. It is necessary to follow the principles of safe behavior on the Internet and do not click on links sent insuspicious or incomprehensible emails or through Facebook.

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

15.21. The cardholder must ensure the protection of his passwords and not give them to anyone.

15.22. The cardholder should not give out his or her personal information to anyone - whether by phone, in person, or in an email message.

15.23. It is necessary to carefully analyze the site 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).

15.24. You need to keep your browser updated and install security updates on time.

15.25. 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.

16. Card Restrictions.

16.1. In order to reduce the risk of unauthorized card transactions the Bank is entitled to establish restrictions and limits on card transactions. The amount of restrictions and limits, as well as the conditions, terms and procedure of their establishment shall be determined by the Bank independently. The Bank establishes daily limits oncards. The Cardholder has the opportunity to carry out transactions using the Card within the daily limits, a listof which is provided on the Bank's website www.bakai.kg, www.ifcenter.kg.

16.2. The standard restrictions set by the Bank may be changed upon written request of the Cardholder to the Bank.

16.3. The bank has set additional restrictions on contactless cards:

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

17. Card validity period and termination of the Agreement.

17.1. The expiration date (month and year) is indicated on the card. The card is valid until the end of the last day ofthe month indicated on it. All overdue cards are blocked and must be returned to the Bank.

17.2. The cardholder has the right to close the card and terminate the Agreement unilaterally by submitting anapplication for cancellation of the card.

17.3. The Bank has the right to block / cancel the card and terminate the Agreement with the Cardholder in case of theCardholder's failure to comply with the terms of these Rules and the Agreement.

17.4. Upon termination of the Agreement the Cardholder must repay the existing debt and surrender all the cardsissued on his card account.

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

17.6. The balance of funds on the card account is issued in the absence of debt to the Bank.

18. Other terms and conditions.

18.1. 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 services and other documents related to the card issue by providing the Bank with the documents containing the changes. The Bank bears no responsibility forthe consequences of untimely notification about the changes of these data.