Security measures while using banking cards

1. General security measures and minimization of risks

1.1. Upon receipt of a card, make sure to put your signature on it.

1.2. A PIN-code (personal identification number) is a combination of digits, containing 4 characters and meant for identification of a Cardholder as well as protection against unauthorized usage of the card. **Only you must know information about the PIN-code. Nobody has the right to ask you to give the PIN-code of the card.**

1.3. Don't keep the PIN-code and the Card in one place, don't write the PIN-code on the card itself. Remember the PIN-code or keep it apart from the card in the place inaccessible for other.

1.4. Don't give your card to other people for conduct of any operations.

1.5. In order to reduce the risk of fraudulent operations when visiting the countries with the high level of fraud (the countries of Africa, the countries of South-east Asia, the countries of Latin America, Moldova, Ukraine, Turkey, USA) carefully observe all security measures specified in this Instruction.

1.6. Keep receipts confirming payment for goods and services within a year from the day of an operation with the card. If the deal for some reasons has not gone through, keep the receipts of unsuccessful operations with the Card and/or alternative payment (cash payment, with another card) in the event of its conduct. The specified documents can be required in order to confirm lawfulness of the operation carried out with the card or to settle disputable situations.

1.7. **On a regular basis (at least once a month) check statements from a bank account. If there are questions connected with conducted operations on the account (unauthorized writing-offs or faulty accruals) immediately approach the branch of CJSC "KICB" (hereinafter the Bank).**

1.8. In order to control the state of the bank account and the list of operations, you can use the i-bank service – the system of remote bank service of CJSC "KICB" and/or a statement that you can obtain in the Bank.

1.9. In order to ensure control over operations with the Card, you can use the service "SMS notification". Using this service you can receive information about available balance after conduct of an operation with the Card, notifications about receipt of the funds to the account and withdrawal operations on the account.

The services specified in cl. 1.8. and 1.9., are enabled based on an application of a cardholder.

1.10. In order to minimize financial losses from conduct of fraudulent operations with your card, you have an opportunity to establish limits on the amounts of operations with the card (for each operation, for operations within 24 hours) either separately for operations of cashless payment for goods (works, services) and/or operations of cash receipt or for all operations. For the same purpose the Bank can establish the limit on receipt of cash in ATMs during a day.

1.11. Upon receipt of any requests (by e-mail, phone or in another way) asking to confirm personal data and information about your card, don't provide information about your card **(a PIN-code, a number of the card, expiry date of the card, CVV2 – a security code)**, as these messages are used by malefactors in order to obtain confidential information for subsequent use for fraudulent purposes. Be attentive: messages can be similar to genuine official messages (can have a business letter style, contain references to current sites or sites that are well disguised as the sites of well-known organizations, informing can be made in automatic mode using "e-voice"), and also can transfer harmful programs that are computer viruses allowing obtaining personal information illegally. Upon receipt of such information (requests) immediately contact with the "Call center" of the Bank by phone. For information interaction with the Bank use the communication facilities (telephones/faxes, internet-baking, usual and electronic mail), details of which are stipulated in the documents obtained directly in the Bank.

1.12. In order to use Internet resources safely, use the addresses of official web-sites. These measures are connected with appearance of the websites in the Internet network imitating internet-representatives of the Banks of the Kyrgyz Republic. The domain names (addresses where a company provides its services through the Internet network) and the style of these sites design, as a rule, are similar to the names of genuine web-sites of the banks. The use of such details is connected with the risk and can lead to undesirable sequences (including financial losses). If you reveal a false web-site of the bank yourself or receive such kind of information by e-mail or in another way, immediately contact by phone (312) 97 67 97 or 62 01 01 with the Call center of the Bank.

2. Precaution measures while conducting operations with the card

2.1. Carry out all operations with the card in the trade and service companies only in your presence. Don't let the employees of the trade and service companies take your card to another room and don't lose the view of your card during conduct of operations, as in such events the information from your card can be copied using special equipment and used for production of a fake card in order to receive access to your bank account.

2.2. Before putting your signature on the receipt, make sure that all data about a carried out operation is correctly indicated in the document. If something is inaccurate in the specified information, refuse to put your signature and ask to cancel the conducted operation. In the event of cancelation of the operation it is necessary to receive a receipt of cancelation of the operation.

2.3. Don't leave empty receipts with the imprint of your card in the trade and service companies, i.e. the receipts where there is no your signature or the amount of the operation. The empty as well as "**defective**" receipts must be destroyed by an employee of the trade and service company at once in your presence.

2.4. Don’t throw away and don’t leave payment documents on operations with the card in the trade and service companies as the full number of the card can be printed on them.

2.5. When entering your PIN-code during the operation in the trade and service company, pay attention to the fact that it is input on a special device (a PIN-pad or through the POS-terminal itself), directly connected with the cash machine or the POS-terminal. Don’t agree with the proposal to enter a PIN-code twice on different devices in one and the same place except for repeated payment or cancellation of the operation.

2.6. We would like to draw your attention to the fact that an employee of the bank or the trade and service company when conducting an operation with the card shall be entitled to request your identifying document.

2.7. The card can be taken from you on the Bank’s request by an employee of the bank or the trade and service companies where you make payment for goods/services using the card. In this case you need to obtain an act of the card withdrawal and immediately contact with the Bank for blocking of the card.

2.8. Don’t forget to take your card back after completion of the operation, making sure that the card returned belongs to you.

2.9. Present the card for payment only in the trade and service companies that you have confidence in. Be very careful while conducting operations with the card in the following trade and service companies:

- entertainment centers
- jewelry shops
- travel agencies
- internet services (booking of tickets, payment for goods/services, booking of hotels, etc.)

It is very important to remember about it during trips to the countries of Eastern Europe, the Asian-Pacific region, to the countries with the high level of fraud, specified in cl. 1.5.

2.10. In order to minimize the risks of your card, don’t withdraw cash in the trade and service companies that besides sales of goods are involved into cash withdrawal. Use for these purposes cash withdrawal points or ATMs located in safe places (subdivisions of the bank, government institutions, big trade complexes, hotels, airports, etc.).

2.11. Before carrying out an operation via ATM/terminal, examine it. If you find the devices that arouse your suspicion (an overlay on the card-reader, an overlay on a keyboard for input of a PIN-code, an overlay on the face of ATM or near it, where a camera can be mounted and so on), wires and outside things, don’t insert the card into the reader. As far as possible contact with the organization that has installed ATM/terminal in order to notify about found suspicious devices.

2.12. In order to prevent fraudulent operations and according to recommendations of the international payment systems, the Bank shall install special standard blue inhibitors on ATMs allowing avoiding unauthorized copying of data from the magnetic stripes of the cards. If there is information on the ATM screen about the appearance of the fraudulent device inhibitor in order to ensure additional security, compare the appearance of the existing inhibitor with the proposed image. If you reveal discrepancy, contact with the Call center by phone.

2.13. If you notice some suspicious people near ATM it is recommended to carry out the operation via another ATM installed in a well-illuminated and a safe place or in the cash withdrawal point.

2.14. We would like to draw your attention to the following: the banking card reader for ensuring access to the special closed premises where ATMs and other terminals are installed must not require entering a PIN-code. If at the entrance to the premise the device is installed that requires entering a PIN-code don't use it.

2.15. While carrying out the operation with input of a PIN-code, see that the PIN-code entered on a keyboard is not visible to others, for this, for example, shield a keyboard with your hand to avoid possible video-recording of your actions and viewing of information about the entered PIN-code from the side. Don't use somebody's help while carrying out operations with the cards.

2.16. If ATM/self-servicing device takes your card due to technical problems, immediately contact with the bank that supports ATM/self-servicing device in order to clarify information when and where the card can be obtained. It is recommended to temporarily suspend the card (to block the card temporarily) by contacting with the Call center of the bank by phone.

2.17. In case of failure to receive the whole or the part of the requested amount in ATM or problems while carrying out deposit operations (in devices with the function of cash acceptance) approach the Bank in order to complete an application about the occurred problem.

- **In the events when it seems to you that your PIN-code has become known to other people, you have suspicions of illegal use of your card, the card has been lost, stolen or taken by ATM, you have to immediately contact with the Call center of the bank by phone or to go to the bank and to ask to block your card and to order a new card.**

3. Security measures while carrying out operations of cashless payment for goods (works, service) through the Internet network, a telephone/fax, mail.

3.1. While carrying out operations of cashless payment for goods/services through the internet network, a telephone/fax, mail, you can be asked to indicate CVV2 (three digits of a security code). It is located on the back of

the card (three last digits printed on the stripe for signature or on the right of it in a special field) and serves for additional check of the client by the bank.

3.2. The input of the PIN-code for identification of the holder is supposed only while carrying out operations with the card in the presence of the Holder itself via the terminals with the function of card data reading and only using a special device – a PIN-pad: a keyboard, connected to the payment terminal or a cash machine. In the event of operations of cashless payment for goods/services through the Internet network, a telephone/fax, mail, the provision of information about the PIN-code should be excluded.

3.3. While carrying out operations in the Internet shops, make sure that the shop has published liabilities for protection of the client's data, is certified by VISA payment system and has contact details of an organization on the site. If it is possible, make sure that the address and the telephone indicated on the site are correct. The input of required data shall be through the secure channel using the HTTPS-protocol.

3.4. Be attentive, the web-sites can be used by frauds in order to obtain confidential information (for order of goods/services the clients are offered to fill in electronic forms and to specify the details of bank accounts, cards including the PIN-code). There are for example such kinds of frauds as a **twin-site** of the well-known Internet shop; «a short-lived shop»; the site that represents an organization that does not exist in reality and so on. **Be careful with operations through the Internet network and provision of your personal information and information about your cards.**

3.4**.** In order to avoid fraud with your banking card, the Bank advises you after the use of the banking card in one of the following countries, approach CJSC "KICB" for blocking of a card or re-issuing of a new card:

• **Thailand**	• **Mexico**	• **Vietnam**
• **Malaysia**	• **Nigeria**	• **India**
• **Taiwan**	• **Ukraine**	• **China**
• **Brazil**	• **Turkey**	• **Australia**
• **Hong Kong**	• **USA**	• **UAE**
• **Indonesia**	• **Russia**	• **Singapore**
• **Bulgaria**	• **Spain**	• **Moldova**

It shall be remembered:

- **The bank in not responsible for transaction caused by skimming (fraud) card.**
- **The bank is not responsible for transactions made on the fraudulent sites.**
- **The client is responsible for all operations made with the card (including Internet operations) made using the card details as well as for all amounts written off from the client's account.**
- **The client bear all risks related to conduct of internet operations.**
- **The bank is not responsible if the operation fails for the reasons beyond the bank.**