KSB COMMERCIAL BANK

MEMBER OF A SWISS FINANCIAL GROUP

Card Holder's Memo

A bank card is a convenient and modern tool for paying for goods and services in non-cash form, as well as for storing and transporting money. It is important to know how to protect your funds without falling for the tricks of scammers.

Due to the increasing incidence of fraud with payment cards, we remind you of the importance of saving personal card data. To minimize risks and ensure the safety of your funds, it is important to adhere to the following recommendations:

1. Do not transfer the card to a third party, with the exception of transferring the right to use the card under Power of Attorney in accordance with the current legislation of the Kyrgyz Republic.

2. Do not leave the card in places where someone can take it and/or copy the card number/ specimen signature/CVV code and other card data.

3. The cardholder must not communicate his/her personal data to anyone – neither by phone, in person or in an email message, even if the person introduces him/herself as a bank employee: neither SMS code, nor confirmation code from mail, card number, expiration date or CVV -code on its reverse side, credentials for logging into the bank's personal account. Bank employees will never request this information from its clients due to its confidential nature.

4. To avoid demagnetization of the magnetic stripe, do not keep the card in close proximity to sources of electromagnetic radiation (cell phones, TVs, microwave ovens, audio and video equipment, etc.). Be careful when making payments in places where magnetic encoding of goods is used – this may lead to refusal to process or incorrect processing of the card at ATMs and POS terminals.

5. The cardholder must ensure reliable protection of his/her passwords for logging into personal accounts on Internet resources and not disclose them to anyone.

6. The PIN must be kept secret: do not write it on the card or keep the card near the written PIN. Communicating the PIN code to a third party (relative, colleague, friends, etc.) may lead to unauthorized use of the card and expenditure of funds belonging to the cardholder. Operations carried out by entering a PIN code are recognized as completed by the cardholder and are not subject to challenge.

7. Before performing an operation at an ATM, pay attention to whether there are any external signs of a malfunction of the ATM. If you find any foreign objects near or on the device, notify the bank that provides ATM service. It is not recommended to use devices that display a message on the screen asking you to switch to other ATMs.

8. At retail outlets, all transactions with the card must be carried out in the presence of its owner. When making a purchase, you should not lose sight of it, and after completing the transaction,the card must be immediately collected after making sure of its authenticity.

9. Delete suspicious messages and do not distribute them further. If you nevertheless follow the offered link to an unknown website, under no circumstances enter your card details to pay for anything.

10. You should never download attachments from email messages that you did not expect. You should not click on suspicious or incomprehensible links on the Internet sent via email, instant messengers, chats or social networks from strangers.

11. It is necessary to carefully analyze the website address (URL) to which the cardholder can be redirected. In most phishing cases, although the website looks identical to the real one, the URL may be different from the original (for example, ending in .com instead of .gov).

12. Update the contact information provided to the bank so that you can contact the cardholder by phone/email/SMS (for example, in the event of a suspicious card transaction).

13. You must keep your browser updated and install security updates promptly.

Double-check any doubtful information by contacting the bank by phone numbers listed on the official website. The Contact Center, as the first line of assistance to customers, always has latest data and can promptly provide consultation to you.

www.ksbc.kg
bank@ksbc.kg
+996 (312) 54 34 24
+996 (755) 54 34 24
+996 (705) 54 34 24
+996 (222) 54 34 24