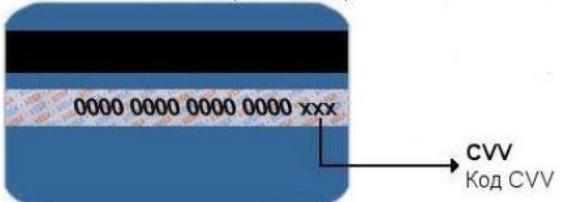


Safety measures during online transactions (purchases) using a bank card

- When making non-cash payment transactions for goods /services online (via the Internet), by phone/fax, post, you may be asked to enter CCV2 (three security code digits). This number is located on the back of the card (three last digits printed on the signature strip or to the right of it in a special field) and serves as an additional means of verification of the client by the Bank.A diagram of a blue credit card. The back of the card is shown, featuring a horizontal signature strip with three black horizontal bars above it. Below the bars, the last four digits of the card number ('xxxx') are printed. To the right of the card, an arrow points from the text 'CVV' to the three-digit number 'xxx' on the card.
- When carrying out transactions in online (Internet) stores, please check that the store has published obligations to protect customer data, is certified by the payment system and that the site contains contact details of the organization. If possible, make sure that the address and the phone number indicated on the site are valid. The required data should be entered via a secure channel using the HTTPS protocol.
- Pay attention. Websites can be used by fraudsters to obtain confidential information (to order a good/ service customers are asked to fill out an electronic form and indicate their bank account and card details, including PIN-code). There are, for example, such types of fraud as twin websites of a well-known online store; a ‘one-day store’; a website representing a nonexistent organization, etc.
- Be careful when conducting transactions over the Internet and providing your personal data and information about your cards.
- Always activate the ‘SMS Notification’ service.

Attention!

If you are subscribed to the ‘SMS Notification’ service and receive an SMS-message about a transaction that you did not perform, you need to **immediately block your card**.

- ✓ Please remember that the Client bears responsibility for all transactions performed with the card, including online transactions made by using card details, as well as for all amounts deducted from the client’s account.
- ✓ The Bank is not responsible for transactions made on fraudulent websites.

Telephone numbers:

- Call Center of the Bank **0 (312) 61 00 61**
- Interbank Processing Center CJSC **0 (312) 66 43 25, 66 50 83**.

You can also contact us by e-mail at **fraud@bakai.kg**