# RECOMMENDATIONS
# FOR SAFE USE OF PAYMENT CARDS

Compliance with these recommendations will ensure the maximum safety of the payment card, payment card details, the PIN and other data, also to reduce possible transactions risks in the using the payment card at the ATM, when making cashless payments for purchase of goods and services, including via the Internet.

## General recommendations

1. Do not reveal information about your PIN to any third party, including relatives, friends, bank employees, trade organizations (service), law enforcement officials and people who help you in using a payment card. Do not pass information about your PIN by phone or by email. Only holders of payment cards should know their PIN code.

2. It is necessary to remember the PIN-code, or if it is difficult, try to keep it separate from the payment card, at inaccessible place for third parties (including relatives).

3. Do not pass the payment card to the third parties including relatives for use. If there are the first and the last name of the individual on the the payment card then only this individual has a right to use the payment card.

4. Upon receiving the payment card sign it on the back in a place designed for signature of the card holder if it is envisaged. This will reduce the risk of using the payment card without your consent in the case of a loss.

5. Prevent the mechanical damage of the payment card by the following: strain, pollution, high and low temperatures, magnetic fields, direct sunlight, moisture, colourants, solvents, harmful chemicals and other adverse factors that may lead to card inefficiency.

6. Payment card issuer bank phone number (the bank that issued the payment card) is printed on the back of the payment card. You should always have the contact numbers of the issuer bank and your payment card number written at the other media: your notebook, mobile phone and / or other media, but not next to the PIN code.

7. Order the service of receiving text messages about transactions on your payment card - this would allow you to promtly receive information about transactions being processed on your payment card: payments for goods and services, viewing of the balance at the ATM, cash withdrawing information. In case it is a paid service, issuer bank should notify you before connecting to the service. In addition, for the purpose of prevention the illegal actions of withdrawing all money from the bank account it is advised to fix daily limit on the amount of transactions on the payment card.

8. In case of receiving a request (personally or by phone) including from the bank employees to provide your personal data or information about the payment card (including PIN-code) withhold this information. Call issuer bank and notify bank employees about that fact.

9. In case of receiving text message from the bank about your payment card and account number locking and with request to provide your personal data (PIN-code, your card's full number, validity period, CVV2/CVC2 codes) withhold this information as well and call issuer bank and notify bank employees about this fact.

10. Ignore the emails that are sent on behalf of the issuer bank with request to provide your personal data. Do not follow the "links" specified in the email (including issuer bank's site links), as they may lead to spoof websites.

11. In order to interact with issuer bank it is recommended to use only communications that are indicated in the documents received from the issuer bank (mobile and fixed-line phones numbers, fax numbers, interactive websites/portals, and e-mail addresses and etc).

12. Remember in case of the disclosure of your personal data, the PIN-code or loss of the payment card may occur the risk of illegal actions with money on your bank account form the third parties.

When discovering the loss (theft) of the payment card, card details, the PIN-code information or upon incurrence of the suspicion that the payment card, card details, the PIN-code information was available for intruders, and when appearance of the risk of illegal use of the payment card and (or) its details or the PIN-code, you should immediately contact the issuer bank's customer service and follow the instructions given by the bank employee. Before addressing the issuer bank you bear the risk related to illegal debiting of the funds from your bank account.

13. It should be taken into account that the specific character of making transactions with the payment card involves the time lag between the time of the transaction made by the holder and a reflection of the operation at the account. Duration of a period between the day of the transaction and the day of reflection at the account depends on the place transaction was made (in the Republic of Kazakhstan or abroad), technical infrastructure premising (issuer bank or other bank), the time of the transaction (night or day, working days, weekends, holidays).

## Recommendations for payment card transactions using ATM

1. When choosing an ATM for payment card transaction, it is recommended to avoid obscure and solitary places. Use the ATMs installed in the safe places (for example, government agencies, banks offices, shopping malls, hotels, airports, etc.). Do not use devices that require a PIN for access to the premise where the ATM is installed.

2. Before using the ATM, inspect it for any hanging electrical conductors or additional equipment that is inadequate for ATM design and located in a place designed for PIN code entering or located in the card insertion slot (for example, irregular fixed PIN entry key pad). In that case, please do not use such ATM.

3. It is recommended to conduct the transactions using ATMs equipped with videotaping and surveillance systems which operate at the time of the transaction. The equipment should be located above the ATM and not near the PIN entry key

pad.

4. In case if the keyboard or card insertion slot are equipped with additional devices inadequate to ATM design, please desist from using this ATM and inform about your suspicions bank employees using the phone number written on the ATM.

5. Do not apply pressure to insert the payment card into the ATM. If the payment card is not being inserted, please refrain from using such ATM.

6. Enter your PIN in a manner that people around you would not see your PIN code. While entering the PIN-code cover up the key pad by hand. Do not listen to the third parties' advices, and refuse from their assistance in carrying out transaction with your payment card at the ATM.

7. If the ATM is not working correctly (for example, is on standby mode for long period, spontaneously reloads the program), it is advised not to use this ATM, cancel the current operation by pressing the keyboard button "Cancel", and wait for payment card return.

8. After receiving cash from the ATM you should recalculate each banknote, standing as close to the ATM as possible, make sure that the payment card was returned, wait for a receipt (if requested) and only then move away from the ATM.

9. You should keep the printed ATM receipts for verification with payment card account statement.

10. If during the conducting the transactions using the ATM the cash machine does not return the payment card, call the bank by phone number written on the ATM, and explain the circumstances of the incident. Also you should address the issuer bank of unreturned card and then follow the instructions of the bank employee.

## Recommendations for payment cards using for non-cash payment for goods and services

1. Do not use payment cards at the incredible trade and service organizations.

2. Demand for all your payment card transactions be conduced only in your presence. This is necessary to reduce the risk of illegal acquisition of your personal data.

3. When using the payment card for goods and services, the cashier may require the payment card holder's passport (or identification card) for identification, to sign a receipt or enter the PIN code. Before entering the PIN code, make sure that the surrounding people will not be able to see it.

4. Before signing a check, make sure that the amount, currency, number of the payment card (part of it), date of operation, type of operation, the name of trade (service) organization and other information specified in the receipt, are correct.

5. Keep all documents related to the payment card operations (slips, checks, ATM receipts) not less than 30 days from the date of the transaction.

6. In case of "unsuccessful" transaction while trying to pay with the payment card, save a copy of the receipt issued by the terminal for further check with payment card account statement.

7. Try do not use your payment cards in the fraud high level countries, such as: Argentina, Australia, Azerbaijan, Bahrain, Brazil, United Kingdom, Venezuela, Haiti, Guatemala, Gibraltar, Honduras, Hong Kong, Indonesia, Iran, Iraq, Colombia, Costa Rica, Malaysia, Mali, Mexico, Pakistan, Peru, Philippines, Poland, Saudi Arabia, Singapore, Taiwan, Thailand, Ukraine, Uruguay, the Philippines, Sri Lanka, Chile, Ecuador, Japan, in African countries.

## Recommendations for transactions over the Internet with using the payment card

1. Do not use the PIN code when ordering goods or services over the Internet, or by phone/fax.

2. Never share your personal information or your payment card information (such as the PIN code, passwords for access to the bank resources, the validity of the payment card, credit limits, transactions history, personal data) over the Internet.

3. In order to prevent illegal actions of withdrawing all amount of money from your bank account it is recommended to make purchases over the Internet using a separate payment card (virtual card) with an ultimate limit, intended only for the stated purposes and which does not allow to make transactions using it in the organizations of service and trade.

4. To make purchases over the Internet it is recommended to use Internet sites of known companies which use special software to protect information about client’s payment cards.

5. When you enter a web address into your browser, make sure that it's correct, because there are similar web sites which can be used for illegal purposes.

6. It is recommended to make purchases only using your own computer in order to preserve the confidentiality of personal data and (or) information on the payment card.

If a purchase is made using someone else's computer, it is not recommended to save your personal data and other information in that computer, and after all operations completion you should ensure that the personal data and other information are not saved (reload the browser of web-seller page).

7. Install on your computer licensed software, including anti-virus, and regularly update it. This will help to protect your computer from viruses and other destructive programs and unauthorized access to your personal data.