RULES FOR USING BANK PAYMENT CARDS

(HEREINFORE – RULES)

These rules for using bank payment cards (hereinafter referred to as the Rules) are part of the current (settlement) bank account agreement, access to which is provided through the use of a bank payment card, the current (settlement) bank account agreement of an individual with basic service conditions, and (or) other payment instruments (hereinafter referred to as the Agreements), concluded between JSC Belagroprombank (hereinafter referred to as the Bank) and an individual (hereinafter referred to as the Client), determine the rights, obligations, and other conditions for the Bank and the Client and are posted on the official website of the Bank in the global computer network Internet at the address: [www.belapb.by](http://www.belapb.by) .

1. Funds from a current (settlement) bank account, access to which is provided through the use of a bank payment card, a current (settlement) bank account of an individual with basic service conditions and (or) other payment instruments (hereinafter referred to as the account), are used for settlements on transactions carried out using all bank payment cards (hereinafter referred to as cards) (or their details) issued under the Agreement, including for payment of remuneration to the Bank.

2. When maintaining an account in foreign currency:

if the debt under the Agreement is repaid by the Client by depositing foreign currency in cash at the Bank's cash desk and the portion of the funds required for repayment is less than the minimum denomination of the banknote of the relevant foreign currency, then the Client deposits an amount of foreign currency that exceeds the portion of the funds required for repayment, and the Bank purchases from the Client the difference between the minimum denomination of the banknote of the relevant foreign currency and the portion of the funds to be repaid at the exchange rate for the purchase of foreign currency in cash established at the time of the transaction in the Bank Subdivision in which the transaction is carried out;

if, when closing an account in foreign currency, the portion of the funds required to be issued to the Client is less than the minimum denomination of the banknote of the corresponding foreign currency, the Bank shall purchase from the Client a portion of the funds less than the minimum denomination of the banknote of the corresponding foreign currency at the exchange rate for cash foreign currency established at the time of the transaction by the Bank Division in which the transaction is carried out.

In this case, currency exchange transactions are executed in accordance with the legislation and legal acts regulating the procedure for carrying out currency exchange transactions involving individuals.

3. The account may be replenished by another individual (hereinafter referred to as another individual) in compliance with the requirements of the law.

4. The Bank has the right to establish for the Client an incentive in the form of Money- back (income paid by the Bank as a percentage of the amount of non-cash payment for goods, works and services) or other types of incentives for card payments within the framework of loyalty and bonus programs.

The Bank has the right to provide the Client with additional services and facilities for certain types of cards (concierge service, Premium Card , etc.).

In case of cancellation/return of a non-cash payment transaction for goods, works and services, made with the payment of a reward in the form of Money - back, the Bank has the right to write off the previously credited amount of income from the Client's account.

The rules of loyalty and bonus programs are published by the Bank on the official website of the Bank in the global computer network Internet at www.belapb.by. Amendments (additions) to the rules of loyalty and bonus programs, suspension, closure of loyalty and bonus programs are carried out by the Bank unilaterally.

5. The Client instructs the Bank to write off from his Account by the Bank's payment order 0.3% of the amount of each non-cash transaction made using a card issued within the framework of the charity project “Touch” and (or) its details, and to transfer the specified amount quarterly to the local charity fund “Touch of Life”.

For the purposes of implementing part one of this paragraph, non-cash transactions include payment transactions for goods, works and services in OTS, transactions without presentation of a charity card, namely payment transactions for goods, works and services via the global computer network Internet. The following do not apply to non-cash transactions defined in part one of this paragraph: receipt of cash from ATMs and cash dispensing points (cash desks); transactions conducted at cash dispensing points (cash desks), ATMs, self-service terminals and RBSS of the Bank and other banks; transfers of funds from a charity card; crediting of funds to a charity card; debiting of remuneration from the account by the Bank.

In case of cancellation of a non-cash transaction, the amount debited as a donation is returned to the Account in full. In case of refund of funds due to the cardholder's refusal to pay for the goods, work, service, including at the request of the Client, the amount debited as a donation is not returned to the account.

6. The Client is aware that income received by him as part of advertising games and promotions, as well as other advertising events in the form of a gift, is subject to personal income tax in accordance with current legislation.

PROCEDURE FOR ACTIVATION AND USE OF A BANK PAYMENT CARD

7. The card is the property of the Bank (except for the PayRing payment ring) and must be returned to the Bank upon expiration of its validity (except for the virtual card and the PayRing payment ring). The PayRing payment ring is the property of the Client and is transferred to the Client (his representative), the holder of the additional card after the remuneration has been paid from the moment he puts his own signature in the application form under the mark on the issuance of the PayRing payment ring .

The details of the virtual card are displayed to the Client in the remote banking systems determined by the Bank, the security code (CVV2/CVC2/KPP2 code) is sent by SMS message to the Client’s mobile phone number specified in the application form.

Together with the card (except for the virtual card), the Client (the holder of the additional card) is given a sealed envelope with a PIN code, which is generated automatically during the process of personalizing the card and is used to authenticate the client, the holder of the additional card, when conducting transactions.

The card may be issued by the Bank without forming an envelope with a PIN code, with subsequent provision of the PIN code to the Client (card holder) using e-PIN technology by sending an SMS message to the mobile phone number of the Client (additional card holder). In this case, to record the received PIN code on the card microprocessor, it is necessary to perform any successful operation with the PIN code input (receiving cash, viewing the balance (available balance) of the card) at an ATM of the Bank or another bank connected to JSC Banking Processing Center.

The card (except for the virtual card) is activated when the PIN code is generated using the e-PIN technology or, if the said technology was not used (the PIN code was issued on paper), by the Client (additional card holder) independently upon performing the following successful transactions using the card, confirmed by entering the PIN code correctly: withdrawing cash; viewing the balance (available balance) on the card; paying for goods and services; changing the PIN code. The card is not activated if the PIN code check is successful during the transaction, but the transaction itself is rejected (for example, due to insufficient funds or limits being set on the card for non-cash transactions and/or for receiving cash); if the PIN code is entered incorrectly; the card is on the stop list (card is blocked); when an account replenishment transaction is performed using the card.

The contactless interface of the card is activated after a successful financial transaction on the card using a contact microprocessor with the entry of the correct PIN code (cash withdrawal, payment, etc.) at an ATM (infokiosk) located on the territory of the Republic of Belarus, or a terminal installed in a Bank or trade (service) organization on the territory of the Republic of Belarus.

When applying for a card, the Client specifies a code word (mother's maiden name). If the code word needs to be clarified or changed, the Client should contact the Bank branch with an identity document.

The Client, the holder of an additional card, undertakes to keep the card details and/or their PIN code secret, and to store the PIN code separately from the card, since entering the PIN code replaces their signature. The card may only be used by the Client, the holder of an additional card, whose name, surname and/or signature are written on the card. It is prohibited to transfer the card for use by third parties.

When receiving a card with a PIN code sent via SMS message using e - PIN technology, the PIN code is sent to the phone number registered with the Bank.

8. The card or its details must not be used for illegal purposes, including the purchase of goods (works, services) prohibited by the legislation of the Republic of Belarus, as well as the legislation of the state in which the card is used.

All transactions using cards or their details must be carried out by clients, holders of additional cards within the limits of the balance of funds in the account and within the established limits for carrying out transactions, as well as in compliance with other restrictions that are established or may be established by the Bank in accordance with these Rules, the Agreement.

Confirmation of the transaction performed using a card or its details are card checks and (or) other documents (including account statements) stipulated by the rules of the payment system and (or) LPA. Card receipts and other documents that are confirmation of the transactions performed using a card or its details may be drawn up on paper and (or) in electronic form.

When performing transactions using a card or its details, the means of authentication of the Client, the holder of an additional card are the PIN code, and (or) the signature of the Client, the holder of an additional card on the card receipt, and (or) other means of authentication of the Client, the holder of an additional card, provided for by the rules of the payment system, the Bank and (or) the acquiring Bank. In cases provided for by the rules of the payment system, it is possible to perform transactions on the card without authorization.

When conducting a transaction using a card, the Bank or a representative of the OTS has the right to require the Client, the holder of an additional card, to present an identity document.

When performing transactions using cards with a contactless interface, it is possible to perform transactions without authentication.

The amounts of all transactions made using the card or its details are reflected in the account.

Carrying out a spending transaction using a card includes card authorization and reflection of the transaction on the account.

The moment of the transaction, as a rule, does not coincide with the moment of reflection of the transaction on the account.

9. Transactions at ATMs and other self-service devices are performed only by entering a PIN code. By signing card receipts (entering a PIN code), the cardholder acknowledges the correctness of the amount indicated in them and thereby instructs the Bank to perform a transaction on the account. Only three attempts to enter an incorrect PIN code are allowed when performing a transaction. If lost, the PIN code cannot be restored.

CARD VALIDITY

10. The card is issued for the period specified in the application form for the issue (reissue) of the card. The card expires upon the expiration of the last day of the month and year indicated on the card, after which it must be returned to the Bank. The virtual card and the PayRing payment ring cannot be returned to the Bank .

In this case, the Bank has the right to continue servicing the card after its expiration without carrying out the replacement procedure. The Bank informs the Client about the actions taken in relation to the card's validity period by sending an SMS message.

If the client expresses a desire to reissue the card due to its expiration, the specialist fills out an application form and carries out the necessary actions to replace it.

11. If, before the expiration of the card, an inscription indicating the invalidity of the card appears on the special strip for storing a signature sample (if any), located on the back of the card (" VOID " for cards of international payment systems (hereinafter referred to as IPS) and "INVALID" for cards of the BELKART payment system), the Client, the holder of an additional card, must contact the Bank to reissue the card. The Client, the holder of an additional card must keep in mind that the OTS representative has the right to refuse to accept for payment a card that has an inscription indicating its invalidity.

INFORMATION AND CONSULTING SUPPORT

12. The Bank’s Contact Center provides the following information by calling 136:

cost of issuing and reissuing Bank cards;

reward for transactions made using the Bank's cards;

exchange rates established for the execution of currency exchange transactions using the Bank's bank payment cards;

about the services provided to Bank cardholders;

information support in non-standard situations that arise when using the card;

about the location of the Bank's ATMs and information kiosks.

13. The 24-hour service department of JSC Bank Processing Center (hereinafter referred to as the service (support) department) provides the following services:

adding a card to a stop list (blocking) in case of its loss, theft, or suspected unauthorized use of the card or its details by phone +375 17 299 25 26;

removing a card from a stop list, unblocking a card after exceeding the number of incorrect attempts to enter a PIN code, providing information and reference consultations, managing the token life cycle by phone +375 17 299 25 25;

Providing information on the available amount on the card by phone: +375 17 299 25 23.

METHODS OF OBTAINING INFORMATION ABOUT OPERATIONS CARRIED OUT USING THE CARD

14. The Bank provides the Client with information on transactions carried out using the card in the form of a paper statement (account statement) upon the Client’s personal visit to the Bank.

Additionally, the Bank offers the following methods of obtaining information about transactions carried out using the card:

“ SMS -informing” service – allows you to receive information about transactions made using the card via Push / SMS / Viber messages;

mini-statement – a statement generated by the Client independently in self-service devices, Internet banking, Mobile Internet banking systems, containing information on the latest authorization requests for the card (no more than 13 requests), excluding balance viewing, for a certain number of days (no more than 9);

account statement in the RBSS – an account statement generated by the Client independently in the Internet Banking and Mobile Internet Banking systems;

monthly sending of an account statement by the Bank to the Client's email address specified in the application form for the card issue when opening the account.

15. The method of obtaining information about transactions carried out using the card is specified by the Client in the application form, which is an integral part of the Agreement. In the event of detection of an unauthorized transaction, the Client is obliged to immediately block the card.

The date of receipt by the Client of information about transactions carried out using the card in the event of the Client disputing the transaction shall be considered to be the earliest of the following dates (determined on the basis of information registered in the Bank's information systems or the service (support) department, depending on the method of notification chosen by the Client):

the date of sending by the Bank to the Client a text message to the mobile phone number within the framework of the SMS -informing service connected by the Client;

date of receipt by the Client of a mini-statement from an ATM, information kiosk, via the Internet banking and Mobile Internet banking systems;

date of receipt by the Client of a statement generated independently in the Internet Banking and Mobile Internet Banking systems;

the date the Client receives a paper account statement upon personal application to the Bank (if the Client has not applied for a statement – the first day of the month following the reporting month);

date of sending the account statement by the Bank to the Client's email address.

16. If a discrepancy is found between the transactions reflected in the statement and the transactions actually carried out, the holder of the card payment instrument or the Client has the right to demand that the completed payment transaction be recognized as unauthorized in cases determined by law and the National Bank of the Republic of Belarus.

An application for recognition of a transaction carried out using a card payment instrument as unauthorized must be submitted by the holder of the card payment instrument or the Client to the Bank on paper within one month from the date of discovery of the fact of an unauthorized transaction, but no later than 70 calendar days from the date of reflection of this transaction on the account.

The Bank has the right to establish a list of documents to be provided by the card payment instrument holder or the Client along with the application for an unauthorized transaction depending on the nature of the disputed transaction, and also to request additional documents in the process of considering the application of the card payment instrument holder or the Client. Failure by the card payment instrument holder or the Client to provide the documents requested by the Bank shall be grounds for refusing to conduct an inspection.

The period for considering an application for recognizing a transaction carried out using a card payment instrument as unauthorized shall be calculated from the day following the day of registration of the application with the Bank. If the last day of the application review period falls on a non-working day, the first working day following it shall be considered the day of expiration of the period.

The Bank shall inform the holder of the card payment instrument or the Client of the results of the review of the application for recognition of the transaction carried out using the card payment instrument as unauthorized within a period not exceeding 90 calendar days from the date of registration of the application with the Bank, by sending the holder of the card payment instrument or the Client a notice on paper or in electronic form. The notice of the results of the review of the application shall, among other things, include:

information on the decision taken by the Bank to recognize (not recognize) a transaction carried out using a card payment instrument as unauthorized;

grounds established by legislation in the field of payment systems and payment services for refusing to recognize a transaction carried out using a card payment instrument as unauthorized (if a corresponding decision is made);

the specific date of execution of the decision to reimburse the amount of the unauthorized transaction (if the relevant decision is made);

the amount of money due to the holder of the card payment instrument or the Client as compensation.

17. The holder of a card payment instrument or the Client has the right to demand that a transaction carried out using a card payment instrument by a person who is not the holder of the card payment instrument be recognized as unauthorized if the implementation of this transaction became possible due to the compromise of the card payment instrument as a result of illegal access to the software and hardware of banks, foreign banks and (or) processing centers and, as a consequence, to the card details and (or) information that allows the unauthorized use of cards.

The holder of the card payment instrument or the Client shall submit to the Bank an application containing a request to recognize the transaction carried out using the card payment instrument as unauthorized in accordance with the first part of this paragraph, on paper or in electronic form. There is no time limit for submitting such an application.

If the Bank has information about the compromise of a card payment instrument in the case specified in the first part of this paragraph, the application containing the requirement to recognize the transaction carried out using the card payment instrument as unauthorized shall be subject to mandatory satisfaction by the Bank in terms of the transactions carried out using the compromised card payment instrument, provided that the details of the compromised card (authentication data) declared by the card payment instrument holder or the Client correspond to the details (authentication data) available to the Bank for each specific case of compromise of the card payment instrument, and the Bank has no information about the involvement of the card payment instrument holder or the Client in organizing illegal access to the software and hardware of banks, foreign banks and (or) processing centers.

In the event that the holder of the card payment instrument or the Client, on his initiative, has cancelled the blocking of the compromised card payment instrument, carried out by the Bank unilaterally due to the compromise of the card payment instrument in the case specified in the first part of this paragraph, the application containing the requirement to recognize the transaction carried out using the card payment instrument as unauthorized, is subject to satisfaction in terms of the transactions carried out using the compromised card payment instrument before the cancellation of the blocking of the compromised card payment instrument initiated by the holder of the card payment instrument or the Client.

In the event that a transaction carried out using a card payment instrument, specified in the first part of this paragraph, is recognized as unauthorized, the Bank shall not charge a fee (compensation) for filing and reviewing the application, including carrying out all necessary procedures in accordance with the rules of the payment system within the framework of which the card payment instrument was issued.

The holder of the card payment instrument or the Client shall be informed about the results of the application review in accordance with paragraph 16 of these Rules.

Reimbursement of the amount of an unauthorized transaction is carried out by initiating a non-cash payment by the Bank in favor of the Client.

Reimbursement of the amount of an unauthorized transaction is carried out without the Bank charging a fee (commission) for the necessary procedures and settlement transactions carried out to ensure reimbursement.

18. Information about the available amount on the card can be obtained by the Client, the holder of an additional card, from the service (support) department by phone +375 17 299 25 23, as well as in the RBSS.

LOSS OF CARD OR PIN CODE, CHANGE OF PIN CODE, BLOCKING OF CARD

19. If the card is lost, stolen, the card details and/or PIN code become known to an unauthorized person, or if unauthorized transactions or details are detected using the card, the Client, holder of an additional card must immediately block the card with the service (support) service by phone +375 17 299 25 26(25), and then notify the Bank of this within three days to put the card on a hard stop list by submitting a paper application.

A card that has been transferred or information about which has been transferred to the Bank by third parties who are not clients, holders of additional cards (a found card), is subject to mandatory blocking by a Bank employee through the service (support) service by phone +375 17 299 25 26.

20. The Client, holder of an additional card, can change the PIN code of the card by contacting any Division or independently in the RBSS. In this case, the PIN code will be sent to the cardholder via SMS message when using e - PIN technology.

Also, the Client, the holder of an additional card, can change the PIN code of the card (except for cards in form factor format) at the Bank's ATMs.

For changing the PIN code, the Bank charges a fee established by the Collection of fees (remuneration) for transactions carried out by the Bank.

It is also possible to request CVV 2/ CVC 2/KPP2 of a virtual card in the RBSS.

21. The Bank issues a new card based on an application form for the issue (reissue) of a card, completed by the Client on paper or using the RBS, in accordance with the Bank's rules. For reissuing a card, the Bank charges a fee established by the Collection of fees (fees) for operations carried out by the Bank.

22. The Client, holder of an additional card, is obliged to provide information at the Bank's request to investigate the circumstances of the loss of the card. If the Bank has information that the illegal use of the card occurred with the knowledge of the Client, holder of an additional card, then the Client, holder of an additional card, shall be responsible for the transactions performed using the card.

If a card previously reported stolen or lost is found, the use of such card is strictly prohibited.

23. If the card is blocked at the initiative of the Bank or the Client, the holder of the additional card, due to its compromise, then the Client, the holder of the additional card has the right to demand that the Bank unblock the card in order to resume the possibility of its use. In the event of such a request from the Client, the holder of the additional card, the Bank will unblock the card.

FEATURES OF PERFORMING CURRENCY EXCHANGE OPERATIONS

24. Before conducting currency exchange transactions, the Client expresses his consent to the use of the exchange rates established by the Bank in the following ways:

when performing a transaction using the RBSS – by confirming the transaction using exchange rates after reviewing them;

when performing a transaction at an ATM or information kiosk of the Bank – by pressing a button or selecting an interface element that initiates the execution of the corresponding transaction;

when performing other operations:

if, when performing a transaction, the Client is authenticated – by performing actions to authenticate the Client;

if the Client is not authenticated when performing a transaction – by performing actions to initiate the relevant transaction or actions to grant third parties the right to initiate the relevant transaction.

If the transaction currency does not match the account currency, as well as in some cases provided for by payment systems, a currency exchange transaction is carried out. Currency exchange transactions are carried out at the rates set by the Bank at the time of the transaction, taking into account the cross rates of the Mir payment system and the VISA and Mastercard international payment systems. Separate exchange rates are set for transactions using the Bank's cards, which differ from the rates for transactions with cash. Currency exchange rates for transactions using cards may be changed during the working day in accordance with the Bank's LPA regulating the establishment of exchange rates for transactions using cards. Information on the exchange rates set by the Bank for transactions with cards is posted on the main page of the Bank's corporate website, in the remote banking systems for customer service (Internet banking, mobile banking), as well as in the Bank's divisions in a place generally accessible to the Client.

Information on exchange rates set by payment systems is posted on the websites of the VISA, Mastercard and Mir payment systems.

For transactions performed outside the Republic of Belarus or in the devices of banks not connected to the JSC Bank Processing Center (hereinafter referred to as BPC), the moment of the foreign exchange transaction is determined on the basis of the settlement information received from the payment system. In the event that the payment system does not indicate the time of the transaction in the settlement information, the currency exchange rates established by the latest order for that date are used to perform such a transaction.

For transactions carried out in the devices of the Bank or banks connected to the BPC, the moment of the foreign exchange transaction is determined based on the date and time of the transaction.

Upon completion of a currency exchange transaction by the Client, the Bank generates a document confirming the execution of the currency exchange transaction. The document is generated (printed or output to the device interface) using the Bank's device in which the Client conducts the currency exchange transaction. This document contains information stipulated by law.

25. Processing of transactions using cards is carried out in two systems. Initially, in the authorization request processing system, in which the available amount on the card changes in real time (increases or decreases by the transaction amount), and then in the clearing system, in which settlement information is generated. Only as the Bank processes the settlement information is the transaction amount reflected in the Client's account.

Since exchange rates are set by the International Payment System daily and updated taking into account the situation on the foreign exchange market, the amount of the transaction in the account currency at the authorization stage and at the stage of reflecting the transaction on the account may differ (up or down).

26. When paying in OTS outside the Republic of Belarus, the cashier may ask the client to select the payment currency in which the transaction will be made. The currency of the account to which the card is issued is also indicated among the proposed currencies. It is necessary to take into account that during such transactions, in addition to the rates of the issuing bank and the IPS, the rates of the acquiring bank servicing OTS are also used, which actually increases the cost of the purchase. For example, if, when making a payment transaction in Poland with a card in US dollars, the US dollar is selected as the payment currency, the purchase amount in zlotys will be converted into US dollars at the rate of the acquiring bank servicing OTS, which is usually less favorable than the IPS rate. In order to avoid unnecessary expenses, we recommend that when paying in OTS, we select the currency of the country in which the payment is made.

27. When returning funds to an account for a foreign exchange transaction using a card, the procedure for applying foreign exchange rates depends on the type of transaction and the date of the transaction, which are specified by the acquiring bank servicing the OTS.

28. When crediting funds received via bank transfer in a currency other than the account currency to an account, the Bank carries out currency exchange transactions at the rates established for transactions using cards at the time the transactions are carried out.

FEATURES OF PERFORMING OPERATIONS IN THE GLOBAL COMPUTER NETWORK INTERNET

29. Terms:

3 D - Secure – additional authentication technology when making a payment transaction for goods, works and services in the global computer network Internet using cards, on the basis of which the International Payment System has developed special programs – Verified by VISA and Mastercard SecureCode ; the BELKART payment system has developed a similar technology – BELKART- InternetPassword, and the Mir payment system has also developed the MirAccept technology.

CVV 2/ CVC 2/КПП2 – a three-digit card authentication code that is applied to the signature strip and is used as a security element when conducting transactions on the global computer network Internet.

30. The Bank provides the Client, the holder of an additional card issued by the Bank, with the opportunity to perform transactions for payment of goods, works and services in the global computer network Internet using the card details, taking into account the following features:

The Bank provides the Client, the holder of an additional card, with the opportunity to use 3D - Secure and BELKART- InternetPassword technologies;

CVV 2/ CVC 2/KPP2 is usually used, however, when making repeated (signed) payments in the same OTS, the absence of CVV 2/ CVC 2/KPP2 confirmation is allowed.

In accordance with the technology developed by the Mastercard International Payment System for downloading data using the automatic data update program (Automatic Billing Updater – ABU), mandatory for all participating banks, the Bank is obliged to transfer the details of issued (reissued) cards (except for CVC 2/ CVV 2/КПП2 code) to the system that ensures updating of card details in online stores and services. The Client, the holder of an additional card, may refuse to transfer the details of the issued (reissued) card by submitting a written application of any form, by contacting any Subdivision.

The Bank has the right to set restrictions on the execution of transactions for payment of goods, works and services in the global computer network Internet (including the use of 3D - Secure and BELKART- InternetPassword technologies) when using cards.

31. The client, the holder of an additional card, is responsible for transactions made using his card or its details on the global computer network Internet (hereinafter referred to as Internet payments), as well as for all amounts debited from the account as a result of Internet payments.

The client, the holder of an additional card, bears all risks associated with making Internet payments and performing other actions related to entering and saving card details on Internet sites.

The Client, the holder of an additional card, cannot make claims to the Bank regarding transactions carried out on the global computer network Internet using the card, in the event of a violation of these Rules.

The Bank shall not be liable if the Client, the holder of an additional card, is unable to make Internet payments due to circumstances beyond the control of the Bank.

Entering the correct card details, CVV 2/ CVC 2/КПП2 code and/or 3D - Secure verification code is proper and sufficient authentication of the cardholder to reflect on the Account the transaction made using the card and its details.

31-1. Disclosure of information in accordance with Article 23 of the Law of the Republic of Belarus dated 19.04.2022 No. 164-Z "On Payment Systems and Payment Services" is carried out by the Bank by posting the Rules of the payment system of JSC Belagroprombank on the official website of the Bank in the global computer network Internet at: www.belapb.by.

RECOMMENDATIONS FOR SAFE USE OF THE CARD

32. General recommendations.

32.1. When receiving the card, sign on its reverse side in a special field, if any. Having a signature on the card will reduce the risk of its use by other people in case of its loss or theft. If there is no signature on the card or the signature does not match the sample on the card and the identity documents, the transaction may be refused and the card may be confiscated.

32.2. Save the phone number of the Bank's card service (support) in an easily accessible place (for example, in the memory of your mobile phone or a notebook); this information may be useful for blocking the card in the event of its loss or theft.

32.3. To carry out each type of operation (daily and/or regular operations, payments on the global computer network Internet, operations during foreign trips), issue separate cards for different accounts. To carry out payments abroad, it is advisable to issue several cards of different payment systems for one account and store the cards separately from each other.

Remember that you should not keep large sums of money on cards that you use irregularly: for example, a card for payment on the global computer network Internet should be replenished with exactly the amount that you plan to spend, and immediately before making a payment.

32.4. Ensure storage conditions for the card that exclude the possibility of its loss, damage, copying of data, unauthorized and illegal use. Avoid mechanical damage to the card, deformation, contamination, exposure to high and low temperatures, electromagnetic fields, direct sunlight, moisture, dyes, solvents, harmful chemicals and other adverse factors that may result in the card becoming inoperative.

32.5. Do not pass the card to third parties. Only the person whose personal data is indicated on the front side of the card has the right to use the card, unless the Agreement and the rules of the payment system stipulate that the cardholder's last name and first name may not be indicated. If you need to provide access to your account to other persons, you can contact the Bank to issue additional cards to the account.

32.6. Keep confidential card data secret from other persons: the card number and expiration date, the three-digit card authentication code (if any) indicated on the back, the PIN code, which must be remembered or, if this is difficult, stored separately from the card in an inconspicuous form (for example, by rewriting it on a piece of paper among other groups of numbers or any other information). Never disclose the PIN code to other persons, including relatives, acquaintances, bank employees, OTSs, or law enforcement officials. Do not transmit the PIN code either by telephone or by e-mail. Only the Client, the holder of the additional card, must know their PIN code.

32.7. We strongly recommend using the "SMS -Informing" service, which provides prompt receipt of information about transactions made with the card. The "SMS -Informing" service allows you to promptly inform about the account status and changes in the account balance via a text message to your mobile phone. If you receive a Push / SMS / Viber message about a transaction that you did not make, you must immediately block the card and contact the Bank.

If, despite the connected service " SMS -informing", messages from the Bank about the transactions carried out have stopped arriving on your mobile phone, you must contact the Bank to clarify the reasons in order to exclude the possibility of interception of Push / SMS / Viber messages by third parties. If the received Push / SMS / Viber message raises any doubts or concerns, promptly contact the Bank for clarification.

32.8. To interact with the Bank, use only the details of the means of communication (mobile and landline phones, faxes, Internet sites, regular and e-mail) that are specified in the documents received directly from the Bank.

32.9. If the card is lost, stolen, left in an ATM or other self-service device, confiscated by an OTS cashier, the card is compromised (if confidential card data becomes known to third parties) or if such suspicions arise, you must immediately block the card (for example, by calling the service (support) service, or via the RBSS) and contact the Bank.

32.10. Keep card receipts and other documents on card transactions for reconciliation with the account statement. Try to check the account status regularly, at least once a month, and also after foreign trips in which the card was used. If you find discrepancies between the transactions actually performed and those reflected in the statement, contact the Bank to clarify the validity of the transactions.

32.11. Use the Bank's options for setting transaction limits. It is recommended to disable or limit the ability to pay by card on the Internet, as well as to make transactions abroad, if you do not plan to make these transactions in the near future.

33. Carrying out transactions using a card at ATMs and information kiosks.

33.1. When choosing an ATM or information kiosk where you are going to conduct a transaction using a card, it is advisable to avoid poorly lit and deserted places. The safest places to conduct transactions are the premises of bank offices, while street ATMs in tourist areas are less safe.

33.2. To perform regular transactions, try to use the same ATM, located in a well-lit place: it will be easier for you to detect the fact that third-party equipment has been installed on it, which can be used by fraudsters to steal information from cards.

33.3. Before servicing, inspect the front panel of the ATM. Some banks' ATMs offer to compare the image of the ATM on the monitor with the one in front of you. Pay special attention to the card reader slot: fraudsters can install an overlay on it that is not provided for by the ATM design. Before using the ATM or other self-service device, touch the panels, try to move them: fake overlays and keyboards usually do not hold well and, as a rule, even with minor impact, wobble, move away or even fall off. Fraudsters often leave noticeable traces: cracks, glue smudges and chips. It is better not to use an ATM whose card reader looks like someone picked at it with a screwdriver or poured glue on it.

Sometimes fraudsters make fake panels with video cameras, which are then attached to the ATM: on the money dispenser, under the visor, under the screen, or even in the stand for advertising brochures. These cameras can look like black dots from a distance.

If the keyboard protrudes unnaturally, wobbles, or has a different tone, looks new, while the ATM itself already shows obvious signs of wear, this is also a reason to refuse to use such a self-service device.

33.4. Do not use excessive physical force to insert the card into the ATM (infokiosk). If the bank card does not insert without additional force, refrain from using this ATM (infokiosk).

Some ATMs (info kiosks) may use special devices that prevent fraudsters from copying card data – jitters. In such ATMs (info kiosks), the process of accepting cards by the device may differ from other ATMs (info kiosks) – the card vibrates when it is accepted by the device.

33.5. If you find outside equipment (e.g., a cover plate), do not try to remove it yourself, refrain from performing transactions, and report the detected cover plate to the bank servicing the device. If doubts about the correct operation of the ATM or other self-service device arise after the card is inserted into the card reader , do not enter the PIN code. Press the button to cancel the transaction and take the card. If you notice outside equipment after the end of servicing, be sure to block the card immediately in any available way.

33.6. Make sure that the ATM or other self-service device you have selected accepts the card you have. The logo on your card and on the screen of the software and hardware device and/or on its body must be the same. If you insert a card into an ATM or other self-service device that is not accepted by the device, the card will be returned to you, and information will appear on the screen about the impossibility of performing the transaction.

33.7. If there are people near an ATM or other self-service device that you are suspicious of, you should choose another time to use the device or use another ATM or self-service device.

33.8. Be especially careful if strangers offer you assistance in using your card at an ATM or other self-service device. In case of difficulties arising when using your card, do not listen to the advice of strangers, and to contact the Bank, use only the telephone numbers that are indicated directly on the card or that you received from reliable, verified sources or directly from the Bank.

33.9. Pay attention to the people standing behind you in the queue at an ATM or other self-service device; if necessary, ask them to move to a distance from which they cannot see the PIN code you are entering. When entering the PIN code, stay as close to the ATM or self-service device as possible, while covering the keypad with the palm of your free hand.

33.10. When using the card, carefully study the information displayed on the screen of the ATM or other self-service device and check the accuracy of the data entered. If the PIN code is repeatedly entered incorrectly, the card is blocked and may be seized by the ATM or other self-service device. If the card is seized (regardless of the reason) by the ATM or other self-service device, immediately block it (for example, by contacting the service (support) or using the RBSS).

33.11. Do not allow anyone to distract you while you are performing a transaction, as you may accidentally perform an incorrect transaction. In addition, if you do not take any action within the time set for this device, it may seize your card and/or money.

33.12. After receiving cash from an ATM, you should make sure that the card has been returned by the ATM, wait for the card check to be issued (if requested), and only then leave the ATM. It should be remembered that the sequence of issuing cash and returning the card in ATMs of different banks may differ. The ATM may first return the card and then issue the requested amount of money. It is necessary to take into account this specific feature of ATM operation and not leave the device until you receive the card, card check (if requested), and money.

33.13. If an ATM or other self-service device does not operate correctly (e.g., is in standby mode for a long time, reboots spontaneously), you should stop using such a device, cancel the transaction by pressing the appropriate button on the keyboard, and wait for the card to be returned. If the device does not return the card, you should immediately block the card in any available way and contact the Bank.

33.14. Do not leave the card receipt you requested in an ATM or other self-service device, as the check may indicate the transaction amount or the balance of funds. This may attract a robber or fraudster.

34. Receiving cash and conducting non-cash payment transactions using a card at bank branches.

34.1. All actions of the bank employee with the card must take place under your supervision. Do not allow the bank employee to leave with the card to another room.

34.2. When receiving cash or making a non-cash payment, pay special attention to the correspondence between the indicated amount and the amount contained in the card check (slip).

34.3. A bank employee has the right to demand presentation of an identity document to identify the cardholder and process the transaction.

34.4. When conducting transactions at a POS, pay special attention to the actions of the bank employee if he or she tries to swipe your card through the equipment reader more than once. This will prevent unauthorized transactions. Be sure to inquire about the reason why the employee needs to swipe the card through the equipment reader again.

33.5. Before entering your PIN code, carefully study the information presented on the terminal screen and make sure that the amount and currency of the transaction are correct.

34.6. Enter the PIN code, covering the keyboard with the palm of your free hand. Never, under any circumstances, disclose the PIN code to bank employees.

34.7. Before signing the card check, make sure that the amount and currency of the transaction, the date of the transaction, the type of transaction and other data indicated on the card check are correct.

35. Carrying out non-cash payment transactions using a card in OTS.

35.1 Use cards in OTS that inspire confidence.

35.2. When conducting transactions in restaurants, bars, shops, when giving the card to the service personnel, do not let it out of your sight. If necessary, follow the OTS employee to the terminal. This will prevent unauthorized copying of the information indicated on the card.

35.3. When performing a transaction using a printer or payment terminal (POS- terminal), the cashier may require entering a PIN code or signing a card check in accordance with the requirements established by the rules of the payment systems within which the cards are issued, as well as providing an identity document for the purpose of identifying the cardholder.

35.4. When making a payment transaction at OTS, pay special attention to the actions of the cashier if he/she tries to swipe the card through the equipment reader more than once. This will prevent unauthorized transactions. Be sure to inquire about the reason why the cashier needs to swipe the card through the equipment reader again. If, as a result of an unsuccessful card transaction, you paid for the purchase in another way (for example, in cash or with another card), save the confirmation document and check whether the funds for the unsuccessful transaction have been debited from the account.

35.5. Enter the PIN code, covering the keyboard with the palm of your free hand. Before entering the PIN code, make sure that people in your immediate vicinity cannot see it. Never, under any circumstances, disclose the PIN code to OTS employees.

35.6. Before signing the card check, make sure that the amount and currency of the transaction, card number (part of it), transaction date, transaction type, OTS name and other data indicated in the card check are correct.

35.7. If you decide to cancel the purchase after the transaction has been successfully completed, request that the transaction be cancelled. Be sure to keep the card receipt for the cancellation transaction until you verify the statement for the account to which the card was issued.

35.8. Contactless transactions are carried out in the “self-service” mode: The Client, the holder of an additional card, does not hand over the card or other payment instrument used for payment (for example, a bracelet, keyring, mobile phone or other device) to the cashier, but independently applies the card or other payment instrument to the terminal’s reading device to carry out the transaction.

36. Carrying out non-cash payment transactions using a card on the global computer network Internet.

36.1. Do not use cards with large amounts of money on them for online payments. It is better to create a separate card (to a separate account) for such purposes and transfer money there only as needed. When using a virtual card, we recommend not using it to store funds, but to top up the card as needed.

36.2. To ensure the highest level of transaction security, connect the transaction confirmation service using 3D - Secure and/or BELKART-InternetPassword technology. These technologies allow you to request additional confirmation of transactions performed on the global computer network Internet, using a one-time password sent to the phone (via Push / SMS / Viber message), specified when connecting the service.

The website of an online store that accepts payments using 3D - Secure and BELKART- InternetPassword technologies, as a rule, must place the logos of the corresponding payment system programs.

36.3. Do not respond to emails that, allegedly from the Bank or other organizations, or from individuals, ask for personal information, including card details, for the purpose of updating or registering them. Try to find out the legitimacy of such offers by contacting the Bank at a reliably known phone number (for example, the one you received directly from the Bank when you received the card).

Provide your card information only to pay for your purchase. Never send your card details via email, as information sent via email is not fully protected from interception and use by third parties. All reputable stores use data encryption technology on their websites to protect your personal information when making a purchase.

Never show your card number as proof of reaching a certain age, although sometimes some sites may ask you to do so. The card number cannot indicate that you have reached any age.

36.4. Attackers often distribute viruses through various Internet resources - from social networks to regular news sites. A client whose computer is infected, when trying to log into their personal account, may be quietly redirected to a "phishing" site, which outwardly is practically no different from the genuine sites of Internet banks, online stores or other payment services. To avoid this, try to make the most of the security features of your browser and email client. To do this, you need to enable additional functions in the browser and email client options. For example, "Block pop-up windows", "Protection from phishing and malware", "Open files based on content, not extension", etc. Also, do not use the preview window in the email client you use.

In addition, it is recommended to always enter the bank's web address ("Internet banking") into the browser's address bar yourself instead of using any hyperlinks, especially from suspicious messages.

36.5. Make purchases from online stores that you know or first make sure that they have a good reputation and are reliable. Check the correctness of the addresses of the Internet sites that you connect to make a purchase, as similar addresses can be used to carry out illegal actions. If you have any suspicions about the Internet page or do not want to provide personal or card data, then leave the page and make a purchase elsewhere.

When making a card payment on the global computer network Internet, make sure that the web address fragment " http " in the address bar of the web browser has changed to " https " - this will mean that the session is encrypted. Most browsers additionally visualize such a change with an image of a padlock, by clicking on which you can view certificates confirming the security of payments through this site.

36.6. Before making a payment for a product (service), carefully study the terms of the proposed agreement, in particular, all rules for the provision of services, terms of delivery, return, replacement of goods, as well as the procedure for canceling an order. Read especially carefully the terms of transactions related to gambling (casinos, lotteries), as they may provide for automatic subscription, which will entail the write-off of funds on a regular basis. Separately evaluate the advisability of making a transaction if information about the terms of purchase is presented in an unfamiliar language. Find the phone number or email address of OTS and write them down in case you have questions.

36.7. Keep records of transactions made on the global computer network Internet, including the addresses of websites of online stores. Many online stores send customers electronic messages with summary information about transactions - save or print them. Save any electronic documents, email correspondence concerning attempts to resolve a dispute with OTS, as these documents may be very important for protecting your rights. If you are unable to resolve a dispute yourself, contact the Bank.

36.8. Some OTSs (e.g. hotels, car rentals) have the right to request authorization by card before selling goods, performing work and rendering services as a guarantee of the solvency of the cardholder. As a result of authorization, the requested amount is blocked on the card of the Client, the holder of the additional card and becomes unavailable.

36.9. If a hotel reservation was made via the Internet site, but for some reason it is not planned to be used, be sure to cancel the reservation via the same Internet site in accordance with the procedures specified there. Receipt by the Client, the holder of an additional card of the hotel reservation cancellation code is proof that the reservation has actually been cancelled. Otherwise, for late cancellation of the reservation, the hotel has the right to write off from the account an amount of money in the amount established by it.

36.10. Never give your PIN code when ordering goods by phone or mail and do not enter it anywhere on the Internet. The PIN code is never used to perform such transactions.

36.11. Make sure that the transactions you are conducting comply with the law. If the website of an online casino or other gambling websites contains logos of payment systems, this does NOT mean that the operations related to participation in gambling are legal. If you have any questions or doubts about the legality of the transactions you are conducting, contact the Bank.

36.12. Make purchases only from your devices, do not use Internet cafes and other publicly accessible places where spyware programs may be installed that remember the confidential data you enter.

36.13. Install licensed software on your devices, including antivirus software and firewalls (firewalls /brandwalls) and update them regularly. This will help protect your devices from viruses and other destructive programs, as well as from unauthorized access to your confidential data. Even if you are confident in your software, you should not open or download email attachments from unknown or dubious recipients.

36.14. Connect to the Bank’s services that allow you to exercise operational control over your card expenses (“Internet banking”, “Mobile Internet banking”, “SMS notification”, etc.).

36.15. If you suspect that money has been written off unlawfully, we recommend that you immediately block your card and contact the Bank.

37. Using RBSS.

37.1. Keep confidential card data secret from other persons: the card number and expiration date, the three-digit card authentication code (if any) indicated on the back, as well as information related to accounts in the RBSS: logins, passwords, access codes, data from Push / SMS / Viber messages, etc.

37.2. When using the Internet banking system, pay attention to the presence of a secure HTTPS protocol on the service page. Before entering the system, it is recommended to verify the authenticity of the certificate and the site. As a rule, to do this, you need to click in the Internet address bar field (the field with the lock or sheet of paper icon) and check the information in the block. If the data present does not match the actual information about the Bank, you should immediately leave the page.

37.3. Do not forget to change your password periodically (and also if your password has become known to third parties). Try to make it as complex and unique as possible. To do this, use uppercase and lowercase letters, numbers and symbols in your password. Do not use the same password in different systems (e-mail, Internet banking systems of other banks, social networks, etc.). Try to avoid your date of birth, name and other available information about you in your password. Under no circumstances disclose your password to anyone, including bank employees.

37.4. Be careful when visiting sites with questionable content: they are usually the source of the newest viruses.

37.5. After finishing your session with the Internet Banking system, be sure to correctly log out of the system using the appropriate option.

38. Carrying out transactions using applications and Mobile Internet Banking.

38.1. Install mobile applications (including Bank applications) only from known sources (Google Play, Windows Store, App Store or AppGallery). It is recommended to use an antivirus for mobile devices.

38.2. Please remember that the Bank does not send its Clients, holders of additional cards, links or instructions for installing applications via Push / SMS / Viber / MMS / e - mail messages.

38.3. Do not install the Bank's mobile applications on a mobile phone (device) on which root rights (superuser rights) have been obtained. It is also not recommended to use such phones and devices to receive messages from the Bank (for example, SMS with a code (one-time password) for authentication).

38.4. If you lose your mobile phone (device) on which the Bank’s mobile application is installed ( Push / SMS / Viber messages with confirmation one-time passwords are received), or if the SIM card suddenly stops working, you should block the SIM card as soon as possible .

39. Features of conducting operations when using a card.

39.1. It is necessary to take into account that the specifics of performing transactions using a card presupposes the presence of a time gap between the date of the transaction and the reflection of this transaction on the account. The duration of the period between the day of the transaction and the day of reflection of the transaction on the account depends on the place of the transaction (in the territory of the Republic of Belarus or abroad), the affiliation of the technical infrastructure (to the Bank or another bank), the time of the transaction (night or daytime, working or weekends, holidays).

39.2. Depending on the country of residence and the bank, an additional fee may be withheld when performing a transaction using a card. It is advisable to inquire about the amount of this fee from the employee serving you before performing the transaction or by studying the bank's information on its official website in advance. Such information may also be displayed on the screen of an ATM or self-service device when performing the transaction.

39.3. If you have suffered from fraud, you must immediately block the card and contact the Bank. In case of fraud, you must file a complaint with law enforcement agencies.

39.4. When making payments for goods, works and services, or withdrawing cash abroad, it is worth paying attention to the availability of the Dynamic service currency conversion (DCC), which means "dynamic currency exchange". This service offers an additional conversion step, which usually results in an additional fee: the amount to be paid is converted into the currency of the country in which the card was issued, at the rate set by the bank offering the DCC service. It is necessary to carefully monitor the information presented on the terminal screen, as well as check the terms of the transaction specified in the card receipt (in particular, it is worth paying attention to the presence of the abbreviation DCC). In case of disagreement with the terms of the transaction, insist on canceling the transaction and conducting it without using dynamic conversion. In case of disagreement of the organization's employees to cancel the transaction using dynamic conversion, it is worth contacting the police without leaving the organization.

WARRANTY SERVICE OF PAYRING PAYMENT RING

40. When registering a PayRing payment ring, the ring is covered by a 12-month warranty. The warranty period begins from the moment the PayRing payment ring is handed over to the Client, the holder of the additional card, which is confirmed by the Client, the holder of the additional card, putting his or her signature in the application form under the note on receipt of the card.

Warranty cases include the failure of the PayRing payment ring to function during transactions due to a manufacturing defect.

Upon expiration of the warranty service period, the PayRing payment ring is reissued in accordance with the Fee Guide for transactions carried out by the Bank.

The warranty service for the PayRing payment ring does not apply to:

natural wear and tear and aging (scratches, chips);

damage resulting from careless use (impacts, dents);

damage from interactions with aggressive liquids, including cosmetics (solvents, antiseptics, products containing lead, etc.);

damage from interaction with powerful electromagnetic and magnetic fields;

damage caused by immersion in water to a depth of more than 3 meters.