УТВЕРЖДЕНО
Протокол правления
ОАО «Белагропромбанк»
20.06.2013 № 41
(в редакции протокола
Правления
ОАО «Белагропромбанк»
26.09.2024 № 70)

# RULES FOR USE OF BANK PAYMENT CARDS
(hereinafter referred to as 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, an agreement for a current (settlement) bank account of an individual with basic terms of service, 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 on the global computer network Internet at: 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 terms of service and (or) other payment instruments (hereinafter referred to as the account), are used for settlements on transactions performed 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 repayment of debt under the Agreement is carried out by the Client depositing cash foreign currency into the Bank's cash desk and part of the funds required for repayment is less than the minimum denomination of a banknote of the corresponding foreign currency, then the Client deposits an amount of foreign currency that exceeds the part of the funds required for repayment, and the Bank buys from the Client the difference between the minimum denomination of a banknote of the relevant foreign currency and the part of the funds to be repaid at the exchange rate for the purchase of cash foreign currency established at the time of the transaction in the Bank Division in which the transaction is carried out;

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

At the same time, currency exchange transactions are formalized in accordance with the legislation and LLA, governing the procedure for carrying out currency exchange transactions with the participation of individuals.

3. The account can 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 incentives for the Client 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 premium programs.

The Bank has the right to provide the Client with additional services 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 incentives 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 premium programs are published by the Bank on the official website of the Bank on the global Internet computer network at www.belapb.by. Amendments (additions) to the Rules of loyalty and premium programs, suspension, closure of loyalty and premium programs are carried out by the Bank unilaterally.

5. The Client instructs the Bank to debit from his Account using a Bank payment order 0.3% of the amount of each non-cash transaction made using a card issued as part of the "Touch" charity program and (or) its details, and quarterly transfer the specified amount to the local Charitable Foundation "Touching Life".

For the purpose of fulfilling part one of this paragraph, non-cash transactions include transactions for payment for goods, works and services in TSO, transactions without presenting a charity card, namely transactions for payment 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: receiving cash from ATMs and cash dispensing points (cash desks); operations carried out at cash dispensing points (cash desks), ATMs, information kiosks and RBSS of the Bank and other banks; money transfers from a charity card; crediting 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 the event of a refund if the card holder refuses to pay for goods, work, services, 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 promotional games and promotions, as well as other promotional 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 upon expiration of its validity period must be returned to the Bank (except for the virtual card and 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 payment of the reward from the moment he puts his handwritten signature in the application form under the mark on the issuance of the

PayRing payment ring .

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

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

The card can be issued by the Bank without generating an envelope with a PIN code and then providing the Client (card holder) with a PIN code 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's microprocessor, it is necessary to perform any successful operation with entering the PIN code (receiving cash, viewing the balance (available balance) of the card) at an ATM of the Bank or another bank connected to JSC "Bank Processing Center".

Activation of a card (except for a virtual card) is carried out at the moment of generating a PIN code using e-PIN technology or - if the specified technology was not used (the PIN code was issued on paper) - by the Client (additional card holder) independently when making the following transactions using the card successful transactions confirmed by correct entry of the PIN code: cash withdrawal; viewing the card balance (available balance); payment for goods and services; change PIN code. The card is not activated if the PIN code verification was successful during the transaction, but the transaction itself was rejected (for example, due to insufficient funds or limits on the card for conducting non-cash transactions and (or) receiving cash); in case of incorrect PIN code entry; finding the card in the stop list (blocking the card); when performing a top-up operation using a card.

Activation of the contactless card interface is carried out after a successfully completed financial transaction on the card using a contact microprocessor with entering the correct PIN code (cash withdrawal, payment, etc.) at an ATM (info kiosk) located on the territory of the Republic of Belarus, or at a terminal installed in Bank or trade (service) organization on the territory of the Republic of Belarus.

When registering a card, the Client indicates a code word (mother's maiden name). If it is necessary to clarify or change the code word, the Client should contact the Bank with an identification document.

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

Upon receipt of a card with a PIN code sent via SMS message using e - PIN technology, the value of 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 (work, services) prohibited by the legislation of the Republic of Belarus, as well as the legislation of the state in whose territory the card is used.

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

Confirmation of the transaction performed using the card or its details is a card receipt and (or) other documents (including account statements) provided for by the rules of the payment system and (or) LLA. Card receipts and other documents that confirm transactions performed using the card or its details can be drawn up on paper and (or) electronically.

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 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 card transactions without authorization.

When conducting a transaction using a card, the Bank or a representative of TSO has the right to require the Client, the holder of an additional card, to present an identification 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 an expense transaction using a card includes authorization on the card and reflection of the transaction on the account.

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

9. Transactions at ATMs and other self-service devices are carried out only by entering a PIN code. By signing card receipts (by entering a PIN code), the card holder acknowledges the correctness of the amount indicated on them and thereby instructs the Bank to carry out transactions on the account. When performing a transaction, only three attempts to enter the PIN code incorrectly are allowed. If lost, the PIN code is not restored. Transactions at ATMs and other self-service devices cannot be performed using a virtual card.

## CARD VALIDITY

10. The card is issued for the period specified in the application form for the issue (re-issue) of the card. The card validity expires after 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 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 a replacement procedure. The Bank informs the Client about the actions taken regarding the validity period of the card by sending an SMS message.

If the Client expresses a desire to reissue the card due to the expiration of its validity period, the specialist fills out an application form and takes the necessary actions to replace it.

11. If before the expiration of the card, an inscription indicating the invalidity of the card ("VOID" for cards of international payment systems (hereinafter referred to as IPS) and "INVALID" for cards of the BELKART payment system) appears on a special strip for storing a sample signature (if any) on the back of the card, 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 TSO 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 phone 136:

cost of issuing and re-issuing Bank cards;

remuneration for transactions made using Bank cards;

exchange rates established for carrying out foreign exchange transactions using bank payment cards of the Bank;

on services provided to Bank card holders;

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

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

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

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

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

providing information about the available amount on the card by phone. +375 17 299 25 23.

## WAYS TO OBTAIN INFORMATION ABOUT OPERATIONS CARRIED OUT USING THE CARD

14. The Bank provides information about transactions carried out using the card to the Client in the form of a paper statement (account statement) when the Client personally contacts the Bank at the place where the account was opened.

Additionally, the Bank offers the following ways to obtain information about transactions carried out using the card:

SMS -informing" service – allows you to receive information about transactions performed 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 about the latest authorization requests for the card (no more than 13 requests), excluding viewing the balance, for a certain number of days (no more than 9);

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

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

15. The method of obtaining information about transactions carried out using the card is indicated by the Client in the application form, which is an integral part of the Agreement. If an unauthorized transaction is detected, 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 that the Client protests the operation is 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 information chosen by the Client):

the date the Bank sent a text message to the Client’s mobile phone number as part of the “SMS -informing” service activated by the Client;

date of receipt by the Client of a mini-statement at an ATM, information kiosk, through the “Internet banking”, “Mobile Internet banking” systems;

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

the date of receipt by the Client of an account statement on paper upon personal contact with the Bank (if the Client did not apply for a statement - the first day of the month following the reporting month);

the date the Bank sent the account statement to the Client’s email address.

16. If a discrepancy is identified between those reflected in the statement and the transactions actually carried out, the Client has the right to demand recognition of the completed payment transaction as unauthorized in cases determined by law and the National Bank.

An application to recognize a transaction carried out using a card as unauthorized must be submitted by the Client to the Bank on paper within one month from the date of detection 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 Client along with an 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 Client’s application. Failure by the Client to provide the documents requested by the Bank is grounds for refusal to conduct an inspection.

The period for consideration of an application to recognize a transaction carried out using a card as unauthorized is calculated from the day following the day of registration of the application with the Bank. If the last day of the application consideration period falls on a non-working day, then the first working day following it is considered the expiration date.

The Bank informs the Client about the results of consideration of the application to recognize the transaction carried out using the card as unauthorized

within a period not exceeding 90 calendar days from the date of registration of the application with the Bank, by sending a notice to the Client on paper or electronically. Notification of the results of consideration of the application, among other things, includes:

information about the decision taken by the Bank to recognize (non-recognize) the transaction carried out using the card as unauthorized;

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

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

the amount of money due to the Client as compensation.

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

The client, the holder of the additional card, submits to the Bank an application containing a requirement to recognize the transaction carried out using the card as unauthorized in accordance with part one of this paragraph, on paper or in electronic form. There is no time limit for filing such an application.

If the Bank has information about the compromise of cards issued by it in the case specified in part one of this paragraph, the application containing the requirement to recognize the operation carried out using the card as unauthorized is subject to mandatory satisfaction by the Bank in relation to the operations carried out using the compromised card, subject to compliance the details of the compromised card declared by the Client, the holder of the additional card to the details available to the issuing bank for each specific case of compromise of the cards of the issuing bank.

If the Client, the holder of an additional card, on his initiative, canceled the blocking of a compromised card, carried out by the Bank unilaterally due to the compromise of cards issued by him in the case specified in part one of this paragraph, a statement containing a requirement to recognize the operation carried out using the card as unauthorized, is subject to satisfaction in terms of transactions carried out using a compromised card until the moment of cancellation of the blocking of the compromised card initiated by the Client, the holder of the additional card.

If the transaction carried out using the card, specified in part one of this paragraph, is recognized as unauthorized, the Bank does not charge a fee (remuneration) for filing and reviewing the application, including carrying out all necessary procedures in accordance with the rules of the payment system under which the card was issued.

The Client, the holder of the additional card, is informed about the results of consideration of the application in accordance with paragraph 16 of these Rules.

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 25, as well as in RBSS.

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

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

20. The Client, the holder of an additional card, can change the PIN code of the card by contacting any Division or independently at RBSS. In this case, the PIN code will be sent to the cardholder via SMS message 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 Fee Guide for operations carried out by the Bank.

It is also possible to request CVV2 of a virtual card in RBSS.

21. The Bank issues a new card on the basis of an application form for the issue (re-issue) of a card, drawn up by the Client on paper or using RBSS, in accordance with the rules of the Bank. For reissue of the card, the Bank charges a fee established by the Fee Guide for operations carried out by the Bank.

22. The client, the holder of the additional card, is obliged to provide, at the request of the Bank, information 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, the holder of the additional card, then the Client, the holder of the additional card, is responsible for the transactions performed while using the card.

If a card that has previously been 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 an additional card due to its compromise, then the Client, the holder of an additional card has the right to demand that the Bank unblock the card in order to resume the possibility of its use. If such a request is received from the Client, the holder of an additional card, the Bank unblocks the card.

## SPECIAL ASPECTS OF CURRENCY EXCHANGE OPERATIONS

24. If the transaction currency does not coincide with 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 established 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 IPS. For transactions using Bank cards, special exchange rates are established that differ from the rates for cash transactions. Currency exchange rates for transactions using cards can be

changed during the working day in accordance with the Bank's LLA, which regulates the fixing of exchange rates for transactions using cards. Information about the exchange rates established by the Bank for card transactions is posted on the main page of the Bank's corporate website, in remote banking customer service systems (Internet banking, mobile banking), as well as in the Bank's divisions in a place publicly accessible to the Client.

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

For transactions performed outside the Republic of Belarus or in bank devices not connected to JSC Bank Processing Center (hereinafter referred to as BPC), the moment of the currency exchange transaction is determined on the basis of 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 fixed by the last order for that date are used to carry out such a transaction.

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

25. Processing of transactions when using cards is carried out in two systems. Initially - in the system for processing authorization requests, 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, the transaction amount is reflected in the Client's account.

Since exchange rates are set by the IPS on a daily basis and are 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 account transaction may differ (round up and down).

26. When paying at the TSO outside the Republic of Belarus, the cashier may offer the client to choose the payment currency in which the transaction will be completed. Among the offered currencies, the currency of the account for which the card was issued is also indicated. It must be taken into account that during such operations, in addition to the rates of the issuing bank and the IPS, the rates of the acquiring bank servicing the TSO are also used, that 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, then the purchase amount in Polish zloty will be converted into US dollars at the rate of the acquiring bank servicing the TSO, which, as a rule, is less favorable than the rate MPS. To avoid unnecessary expenses, we recommend choosing the currency of the country in which the payment is made when paying via TSO.

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

28. When crediting funds received via bank transfer to an account in a currency different from the account currency, the Bank carries out currency

exchange transactions at the rates fixed for transactions using cards at the time of the transactions.

## SPECIAL ASPECTS OF OPERATIONS ON THE GLOBAL COMPUTER NETWORK INTERNET

29. Terms:

3 D - Secure - an additional authentication technology when making payments for goods, works and services on the global computer network Internet when using cards, on the basis of which special programs have been developed by the IPS - 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.

CVV2/CVC2/KPP2 is 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 carry out payment transactions for goods, works and services on the global computer network Internet using 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;

to confirm a transaction on the global Internet CVV2/CVC2/KPP2 is usually used, however, when making repeated (signed) payments in the same TSO, the absence of confirmation of CVV2/CVC2/KPP2 is allowed.

In accordance with the technology for downloading data developed by IPS Mastercard 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 (with the exception of CVC 2/ CVV 2/KPP2 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 (re-issued) card by submitting a written application in any form by contacting any Bank Division.

The Bank has the right to establish restrictions on transactions for payment for goods, works and services on the global computer network Internet (including using 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 making Internet payments.

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

The Client, the holder of an additional card, cannot make claims to the Bank for transactions carried out on the global computer network Internet when using the

card in case of violation of these Rules.

The Bank is not responsible if the Client, the holder of an additional card, is unable to make Internet payments due to circumstances beyond the Bank's control.

Entering the correct card details, CVV2/CVC2/KPP2 code and/or 3D - Secure verification code is proper and sufficient authentication of the card holder to reflect on the Account the transaction made using the card and its details.

## RECOMMENDATIONS FOR SAFE USE OF THE CARD

32. General recommendations.

32.1. When receiving a card, sign on the back of it in the special field, if available. Having a signature on the card will reduce the risk of it being used by others in the event 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 identification documents, the operation may be refused and the card 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 address book); this information may be useful for blocking the card if it is lost or stolen.

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

Please, remember that you should not store large sums of money on cards that you use irregularly: for example, a card for payment on the global computer network Internet should be topped up with the exact amount you plan to spend, and immediately before making a payment.

32.4. Provide card storage conditions that exclude the possibility of its loss, damage, data copying, unauthorized and illegal use. Avoid card mechanical damage, deformation, contamination, and exposure to high and low temperatures, electromagnetic fields, direct sunlight, moisture, dyes, solvents, harmful chemicals and other unfavorable factors that may cause the card malfunction.

32.5. Do not give the card to third parties. The right to use the card has only the person whose personal data is indicated on the front side of the card, unless the Agreement and the Rules of the payment system stipulate that the last name and first name of the cardholder 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 for your account.

32.6. Keep confidential card data secret from other persons: card number and expiration date, indicated on the back side, three-digit card authentication code (if available), PIN code, which must be remembered or, if this is difficult, stored separately from the card in an implicit form (for example, by copying it onto a piece of paper among other groups of numbers or any other information). Never give your PIN code to other people, including relatives, friends, bank employees, TSO employees, and law enforcement officials. Do not give out your PIN code over the phone or by email. Only the Client, the holder of the additional card, must know his PIN code.

32.7. We strongly recommend using the “SMS -informing” service, which ensures prompt receipt of information about card transactions. The “SMS -informing” service allows you to promptly inform about the account status and changes in the account balance via a text message to a mobile phone. When receiving an Push/SMS/Viber message about a transaction that you did not perform, you must immediately block the card and contact the Bank.

If you have the “SMS -informing” service activated, messages from the Bank about ongoing transactions stop 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 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 communication details (mobile and landline phones, faxes, Internet sites, regular and e-mail) that are indicated in the documents received directly from the Bank.

32.9. If the card is lost, stolen, left at an ATM or other self-service device, withdrawn by an TSO cashier, the card is compromised (if confidential card data has become known to unauthorized persons), or if such suspicions arise, you must immediately block the card (for example, by calling the service (support) department, or through RBSS) and contact the Bank.

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

32.11. Use the opportunities offered by the Bank to set transaction limits. It is recommended to disable or limit the ability to pay by card on the global computer network Internet, as well as perform transactions abroad, if you do not plan to perform these transactions in the near future.

33. Conducting transactions when using the card at ATMs and information kiosks.

33.1. When choosing an ATM or information kiosk where you are going to carry out an operation using a card, it is advisable to avoid poorly lit and deserted places. Bank offices are the safest places to conduct transactions, but street ATMs in tourist areas are less secure.

33.2. To carry out 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 is 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. ATMs of some banks offer to compare the image of the ATM on the monitor with the one in front of you. Pay special attention to the slot of the card reader: fraudsters can install an overlay on it that is not provided for by the design of the ATM. Before using an ATM or other self-service device, touch the panels, try to move them: fake pads and keypads usually do not hold well and, as a rule, even with minor impact, become loose, move away, or even fall off. Often, scammers leave noticeable marks: cracks, adhesive smudges and chips. It's best not to use an ATM whose card slot looks like

someone has poked around with a screwdriver or poured glue on it.

Sometimes scammers 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 a stand for advertising brochures. These cameras can look like black dots from a distance.

If the keyboard protrudes unnaturally, is wobbly, or has a different tone that looks new, while the ATM itself already has 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 a card into an ATM (information kiosk). If the bank card cannot be inserted without additional effort, refrain from using this ATM (information kiosk).

Some ATMs (information kiosks) have special devices that prevent fraudsters from copying card data - jitters. In such ATMs (information kiosks), the process of accepting cards by the device may differ from other ATMs (information kiosks) - the card vibrates at the moment it is accepted by the device.

33.5. If you find foreign equipment (for example, a cover), do not try to remove it yourself, refrain from performing operations, and inform the bank servicing the device about the detected cover. If doubts regarding the correct operation of an ATM or other self-service device arise after the card is placed in the card reader, do not enter the PIN code. Press the button to cancel the operation and take the card. If you notice foreign equipment after the end of the service, be sure to immediately block the card using any available method.

33.6. Make sure an ATM or other self-service device you choose 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 inserted a card into an ATM or other self-service device that is not accepted by this device, the card will be returned to you, and information about the impossibility of completing the transaction will appear on the screen.

33.7. If there are people close to an ATM or other self-service device that make you suspicious, you should choose a different time to use that device or use another ATM or self-service device.

33.8. Be especially careful if strangers offer to help you use your card at an ATM or other self-service device. In case of difficulties that arise when using the 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 received by you from reliable, verified sources or directly from the Bank.

33.9. Pay attention to the people standing behind you in line at an ATM or other self-service device, if necessary, ask them to move away to a distance from which they will not be able to see the PIN code you enter. When entering your PIN code, be 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 a card, carefully study the information displayed on the screen of an ATM or other self-service device and check that the data entered is correct. If you repeatedly enter the PIN code incorrectly, the card is blocked and can be withdrawn by an ATM or other self-service device. If the card is withdrawn (regardless of the reason) by an ATM or other self-service device, immediately block

it (for example, by contacting the service (support) department or using RBSS).

33.11. Do not allow anyone to distract you during the operation as you may accidentally perform an incorrect operation. In addition, if there is no action on your part within the time limit set for this device, it may confiscate your card and/or money.

33.12. After receiving cash from an ATM, you should make sure that the card was returned by the ATM, wait for the card receipt to be issued (if requested), and only then leave the ATM. It should be noted that the sequence of cash dispensing and card return at ATMs of different banks may differ. An ATM may first return the card and then dispense the requested amount of funds. It is necessary to take into account this specific operation of ATMs and not leave the device until you receive the card, card receipt (if requested) and money.

33.13. If an ATM or other self-service device does not work correctly (for example, it is in standby mode for a long time or reboots spontaneously), you should stop using such a device, cancel the operation being performed 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 at an ATM or other self-service device, as the receipt may indicate the amount of the transaction or the remaining funds. This may attract a burglar or scammer.

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

34.1. All actions of a bank employee with a card must be carried out 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 of the indicated amount and the amount contained in the card receipt (slip).

34.3. A bank employee has the right to require the presentation of an identification document to identify the card holder and complete the transaction.

34.4. When conducting transactions at a point of sale, pay special attention to the actions of a bank employee if he tries to swipe your card through the equipment reader more than once. This will prevent unauthorized transactions. Be sure to ask the reason why the employee needs to re-swipe the card through the equipment reader.

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

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

34.7. Before signing the card receipt, make sure that the amount and currency of the transaction, date of transaction, type of transaction and other information specified in the card receipt are correct.

35. Conducting non-cash payment transactions when using a card in TSO.

35.1. Use cards in TSO 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 sight. If necessary, follow the TSO employee to the terminal. This will prevent unauthorized copying of the information on the card.

35.3. When performing a transaction using a printer or payment terminal (POS terminal), the cashier may require you to enter a PIN code or sign a card receipt in accordance with the requirements established by the rules of the payment systems within which cards are issued, as well as provide an identification document, for the purpose of identifying the card holder.

35.4. When conducting a payment transaction at TSO, pay special attention to the actions of the cashier if he tries to swipe the card through the equipment reader more than once. This will prevent unauthorized transactions. Be sure to ask the reason why the cashier needs to re-swipe the card through the equipment reader. If, due to an unsuccessful card transaction, you paid for the purchase in another way (for example, cash or another card), save the supporting document and check whether the funds for the unsuccessful transaction were debited from your account.

35.5. Enter your PIN code while covering the keyboard with the palm of your free hand. Before entering your PIN code, you should make sure that people in your immediate vicinity would not be able to see it. Never and under any circumstances, give your PIN code to TSO employees.

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

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

35.8. Contactless transactions are carried out in “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, key fob, mobile phone or other device) to the cashier, but independently applies the card or other payment instrument to the reader terminal device for carrying out the operation.

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

36.1. Do not use cards on which you have large sums of money to pay online. For such purposes, it is better to have a separate card (to a separate account) and transfer money there only as needed. When using a virtual card, we recommend not using it to store funds, but replenishing the card as needed.

36.2. To ensure the highest level of transaction security, activate the transaction confirmation service using 3D - Secure technology and/or BELKART-InternetPassword. 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 number (via Push/SMS/Viber message) specified when connecting to the service.

An online store website that accepts payments using 3D - Secure and

BELKART- InternetPassword technologies , as a rule, must display the logos of the corresponding payment system programs.

36.3. Do not respond to emails in which, allegedly on behalf of the Bank or other organizations, as well as citizens, are asked to provide personal information, including card details, for the purpose of updating them or for registration. Try to find out the legality of such offers by contacting the Bank using a reliably known phone number (for example, you received directly from the Bank when receiving the card).

Provide your card information only to pay for a purchase. Never send card details by email, as information sent by email is not completely secure from interception and use by third parties. The websites of all well-known trustworthy stores use data encryption technology, which protects your personal information when making a purchase.

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

36.4. Attackers often distribute virus programs 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 in appearance 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 your browser and email client's security capabilities. To do this, you need to enable additional functions in your browser and email client options. For example, “Block pop-up windows”, “Protection against 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 address bar of your browser 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 are reputable and reliable. Please check that the addresses of the Internet sites you connect to to make a purchase are correct, as similar addresses may be used for illegal activities. If you have any suspicions about the Internet page or do not want to provide personal or card information, then leave the page and make a purchase elsewhere.

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

36.6. Before making a payment transaction for a product (service), carefully study the terms of the proposed agreement, in particular, all the 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 and conditions for transactions related to gambling (casinos, lotteries), as they may provide for

automatic subscription, which will entail debiting funds on a regular basis. Separately, evaluate the reasonability of completing a transaction if information about the terms of purchase is presented in an unfamiliar language. Find TSO's phone number or email address and write it down in case you have questions.

36.7. Keep records of transactions performed on the global computer network Internet, including addresses of online store sites. Many online stores send emails to customers summarizing transactions - save or print them. Save any electronic documents or email correspondence regarding attempts to resolve a dispute with TSO, as these documents may be very important for protecting your rights. If you are unable to resolve the dispute yourself, contact the Bank.

36.8. Some TSO (for example, hotels, car rental points) have the right to request authorization on the card before selling goods, performing work and providing services as a guarantee of the card holder's solvency. As a result of authorization, the requested amount is blocked on the card of the Client, the holder of the additional card, and becomes inaccessible.

36.9. If you made a hotel reservation through the Internet site, but for some reason you do not plan to use it, be sure to cancel the reservation through the same Internet site according to the procedures specified on it. Receipt by the Client, the holder of the additional card, of the hotel reservation cancellation code is proof that the reservation is indeed cancelled. Otherwise, for untimely cancellation of the reservation, the hotel has the right to write off the amount of funds in the amount established by it from the account.

36.10. Never give out your PIN code when ordering products by phone or mail, or enter it anywhere online. A PIN code is never used to perform such transactions.

36.11. Make sure that your transactions comply with the law. If payment system logos are present on the website of an online casino or other gambling sites, this does NOT mean that transactions related to participation in gambling are legal. If you have any questions or doubts about the legality of your transactions, please contact the Bank.

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

36.13. Install licensed software on your devices, including anti-virus software, and firewalls 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 unfamiliar or dubious recipients.

36.14. Connect to the Bank’s services, which allow you to quickly control expenses on your card (“Internet banking”, “Mobile Internet banking”, “ SMS notification”, etc.).

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

37. Use of RBSS.

37.1. Keep confidential card data secret from other persons: the card number and expiration date, the three-digit card authentication code indicated on the reverse

side (if available), as well as information regarding accounts in 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 logging in, 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 icon of a lock or a sheet of paper) and check the information available in the block. If the data present does not correspond to real information about the Bank, you should immediately leave the page.

37.3. Do not forget to periodically (and also if your password becomes known to unauthorized persons) change your password. Try to make it as complex and unique as possible. To do this, use upper and lower case letters, numbers and symbols in your password. Do not use the same password in different systems (email, Internet banking systems of other banks, social networks, etc.). Try to avoid your date of birth, name and other information available about you in your password. Under any circumstances, do not disclose your password to anyone, including bank employees.

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

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

38. Conducting transactions using applications and Mobile Internet Banking.

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

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

38.3. Do not install the Bank’s mobile applications on a mobile phone (device) that has root rights (superuser rights). 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 (you receive Push/SMS/Viber messages with confirmation one-time passwords), or the SIM card unexpectedly stops working, you should block the SIM card as quickly as possible .

39. Features of operations when using a card.

39.1. It must be taken into account that the specifics of performing transactions when using a card assume 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 the transaction is reflected on the account depends on the location of the transaction (on the territory of the Republic of Belarus or abroad), the ownership of the technical infrastructure (Bank or another bank), the time of the transaction (night or daytime, workdays or weekends, holidays).

39.2. Depending on the country of residence and the bank, when carrying out

a transaction using a card, an additional fee may be withheld, the amount of which is advisable to ask the employee serving you before making the transaction or by learning the bank's information in advance on its official website. Also, such information can be displayed on the screen of an ATM or self-service device when performing a transaction.

39.3. If you do suffer from fraud, you must immediately block the card and contact the Bank. In case of fraud, you must file a report with law enforcement bodies.

39.4. When making payments for goods, works and services, or withdrawing cash abroad, please pay attention to the availability of the Dynamic service currency conversion (DCC), which means "dynamic currency exchange". This service offers an additional conversion step, which, as a rule, leads to the payment of an additional commission: the amount payable is converted into the currency of the country in which the card is issued, at the rate established by the bank offering the DCC service. It is necessary to carefully monitor the information presented on the terminal screen, and check the conditions for the operation indicated on the card receipt (in particular, you should pay attention to the presence of the abbreviation DCC). If you disagree with the terms of the operation, insist on canceling the operation and carrying it out without using dynamic conversion. If the organization's employees do not agree to cancel the operation using dynamic conversion, you should contact the police without leaving the organization.

## PAYRING PAYMENT RING WARRANTY SERVICE

40. When registering a PayRing payment ring, the ring is subject to warranty service for a period of 12 months. The calculation of the warranty period begins from the moment of transfer of the PayRing payment ring to the Client, the holder of the additional card, about which a handwritten signature is affixed in the application form under the mark on receipt of the card by the Client, the holder of the additional card.

Warranty cases include the inoperability of the PayRing payment ring when performing transactions due to a manufacturing defect.

After the warranty period expires, the PayRing payment ring is reissued in accordance with the Fee Guide for operations carried out by the Bank.

Warranty service PayRing payment ring does not apply to:

natural wear and tear (scratches, chips);

damages resulting from careless use (impacts, dents);

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

damages when interacting with powerful electromagnetic and magnetic fields;

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