TERMS AND CONDITIONS OF THE AGREEMENT ON CURRENT (SETTLEMENT) ACCOUNT TO WHICH THE BANK PAYMENT CARD IS ISSUED (FURTHER – THE TERMS AND CONDITIONS)

1. The Bank issues the Card to the Customer following the payment of the fee set by the Bank, the deposit of the minimum balance (if applicable), unless otherwise provided for by the agreement on cashless money transfer to personal accounts concluded between the Bank and the enterprise (organization) by which the Customer is employed, or other documents.

2. The terms and conditions are applicable to all Cards issued.

3. The funds held in the account shall be used for payment operations performed using all Cards (or their details) issued within the Agreement, including for fee payments to the Bank.

4. In accordance with the LRLA of the Bank, the minimum amount of funds on the account (minimum balance) may be required which cannot be used by the Customer (Cardholder) during the entire period of the validity of the Agreement. On the Agreement's validity start date, the minimum balance amount on the non-resident's account is as follows:

For Cards Visa Classic, MasterCard Standard - _____ Bel. rub., _____ US Dollars, _____ Euros, _____ Russian rubles;

For Cards Visa Gold, MasterCard Gold - _____ Bel. rub.., _____ US dollars, _____ Euros, _____ Russian rubles;

For Cards Visa Platinum - _____ Bel. rub., _____ US Dollars, _____ Euros, _____ Russian rubles.

5. When account is held in foreign currency:

If redemption of indebtedness under the Agreement is carried out by depositing of foreign currency cash by the Customer at the Bank's counter, and the portion of funds to be redeemed is less than the lowest denomination of the banknote of the relevant foreign currency, then the Customer shall deposit foreign currency in the amount exceeding the portion of funds to be redeemed and the Bank shall purchase from the Customer the difference between the lowest denomination of the banknote of the relevant foreign currency and the portion of funds to be redeemed at the exchange rate for purchase of cash foreign currency determined at the time of the transaction by the Bank's branch in which the transaction was performed;

If upon the closure of the account in foreign currency the portion of funds required to be given to the Customer are less than the lowest denomination of the relevant foreign currency banknote, the Bank shall purchase from the Customer the remaining portion of funds less than the lowest denomination of the relevant foreign currency banknote at the foreign currency cash exchange rate determined at the time of the transaction by the Bank's branch in which the transaction was performed.

In addition, currency exchange transactions shall be executed in accordance with the legislation of the Republic of Belarus and the LRLA governing the procedure for currency exchange transactions that involve individuals.

6. Accounts of individuals may be topped up by individuals who are not account owners (further – other individuals), subject to the requirements of the legislation of

the Republic of Belarus in relation to the transfer of funds between resident individuals, between resident individuals and non-resident individuals and between non-resident individuals.

6-1. As part of the “My Bonus” loyalty program, the Bank may set a Cash-back reward on the Customers Cards. In the event the cashless transaction made as payment for goods (works, services) within the Cash-back service is cancelled, the Bank has the right to debit the customer’s account for the award amount previously credited hereto.

The Regulations of the “My Bonus” loyalty program shall be published by the Bank on the web-site at www.belapb.by. The Bank may unilaterally introduce changes (amendments) into the Regulations of the “My Bonus” loyalty program, suspend and terminate the “My Bonus” loyalty program.

6-2. For Cards issued as part of the "Prikosnoveniya" charity project, the Customer shall instruct the Bank to debit its account by payment order for 0,3% of the amount of each cashless transaction made with a charity card and(or) its details, and shall quarterly transfer the specified amount to the local charity foundation "Prikosnoveniye k zhizni" (“Touch of Life”).

Cashless transactions are payments for goods (works, services) at merchants', transactions performed without the physical presence of the charity card, namely transactions for online payment of goods (works, services). Cashless transactions do not refer to the following: cash withdrawals from ATMs and cash advance offices (counters), transactions performed at cash advance offices (counters), ATMs, info kiosks and remote banking services systems of the Bank and other banks, transfer of funds from a charity card, crediting of funds to a charity card, debiting of the fee from the Account by the Bank.

In the event the cashless transaction is cancelled, the amount debited as donation shall be refunded in full to the Account. In the event of refund of the cashless transaction, as well as upon the Customer's request, the amount debited as donation shall not be refunded to the Account.

6-3. For "O-GO!" Cards, the Customer shall confirm his consent to be included into the list of participants of the promotion campaign "Energy of FITcoins".

GUIDELINES ON BANK PAYMENT CARD USAGE

7. The Cardholder undertakes to keep the Card details and/or the PIN secret, as well as to keep the PIN separate from the Card, since the PIN entry is an alternative to the signature. Only the Cardholder is authorized to use the card, whose first name, last name and/or signature are inscribed on the Card. The Card must never be passed for use by third parties.

8. The Card can be used to pay for goods and services, including online payments, and to perform cash transactions. Meanwhile, the logos and trademarks of the payment system inscribed on the Card must match the logos and trademarks displayed (designated) on ATMs, cash advance offices (further - CAO), infokiosks, self-service-terminals and merchants (further – Merchants).

When using the Card to pay for goods and services at Merchants', as well as when performing transactions at CAO, the Cardholder must enter the PIN on a special device and/or put the signature on the card receipt confirming the transaction, first having made sure that the Card number, the date and the amount of the transaction in this card receipt are correct.

When performing transactions using cashless Cards it is possible to perform debit transactions without authentication.

The virtual card "Unreal Card" can only be used for online transactions and transactions via remote banking servicing systems.

9. Only the PIN should be used for transactions at ATMs and other self-service terminals. Only the PIN shall be used for transactions with BELCARD cards. By signing card receipts (by entering PIN), the Cardholder acknowledges the correctness of the amount stated therein and thereby instructs the Bank to effect the account transaction. Only three wrong PIN entries are allowed when performing the transaction. If lost, the PIN is not restored. Transactions at ATMs and other self-service terminals performed with a virtual card "Unreal Card" shall not be performed.

10. The Cardholder should note that cashiers at Merchants' and CAO have the right to request a passport or any other identification document for the purpose of the Cardholder identification.

CARD VALIDITY TERM

11. The Card is issued for the validity period specified in the application form. The Card is valid up to the last day of the month and the year indicated on the Card, and shall thereafter be returned to the Bank. The virtual card "Unreal Card" shall not be returned to the Bank.

If prior to the Card expiration date the signature space on the back of the Card displays an inscription indicating the Card is not valid ("VOID" for international payment system Cards and "NOT VALID" for BELCARD cards), the Customer should contact the Bank and request the reissue of the Card. The Cardholder should note that cashiers at Merchants' and CAO have the right to refuse to accept the Card if it bears the inscription indicating the Card is not valid.

12. The Bank issues the Card no later than 10 (ten) business days from the date when the Customer submitted the completed application form, presented the identity document, and fulfilled the conditions listed in Clause 1 of these Terms and Conditions.

INFORMATION AND ADVISORY SUPPORT SERVICES

13. 24/7 Customer Support Service of JSC "Bank Processing Centre" (further-customer service (support)) provides the following services at 8-(017)-299-25-25 (26):

Adding of the Card into the exception file (blocking) in case it is lost, stolen or if unauthorized use of the Card or its details is suspected;

Removing the Card from the exception file (unblocking), including following the exceeded limit of the wrong PIN entries;

Providing information on the balance available on the Card;

Information support in unusual situations arising in connection with the use of the Card.

14. The Bank's Call Centre provides the following information at telephone number 136:

Cost of issuance and reissuance of the Cards of the Bank;

Fee for transactions performed using the Bank's Cards;

Currency exchange rates for transactions performed using the Bank's Cards;

Information on the services provided to the Bank's Cardholders;

Information on the location of ATMs and infokiosks of the Bank.

METHODS OF OBTAINING THE INFORMATION ABOUT THE TRANSACTIONS PERFORMED WITH THE CARD

15. The information on the transactions performed with the Card is provided by the Bank to the Customer on a monthly basis in the form of a statement in hard copy (account statement) upon the Customer's personal visit to the Bank where the account is held.

In addition, the Bank offers the following methods of obtaining the information on the transactions performed with the Card:

"SMS notification" – allows you to receive the information on the transactions performed with the Card by text messages;

mini-statement – a statement generated by the Customer in self-service terminals, "Internet Banking", "Mobile Internet Banking", "Mobile Banking" containing the information about the latest authorization requests on the card (maximum 13 requests), excluding balance enquiry, for a certain number of days (maximum 9);

account statement in the remote service systems – the account statement generated by the Customer in the "Internet Banking", "Mobile Banking" and "Mobile Internet Banking" systems;

monthly account statements sent by the Bank to the Customer's email address stated in the application form.

16. The method of obtaining the information about the transactions performed on the Card shall be specified by the Customer in the application form, which is an integral part of the Agreement. In case of an unauthorized transaction, the Customer is obliged to immediately block the Card.

The date of receipt by the Customer of the information about the transactions performed with the Card in case of a dispute is considered the earliest of the following dates (determined based on the data registered in the Bank's information systems or customer service (support), depending on the notification method selected by the Customer):

The date on which the Bank forwarded to the Customer a text message to the mobile phone's number within the "SMS-notification" service the Customer is subscribed to;

The date on which the Customer received a mini statement at ATM, infokiosk, via "Internet Banking", "Mobile Internet Banking" and "Mobile Banking";

The date on which the Customer received a statement generated by him in the "Internet Banking", "Mobile Banking" and "Mobile Internet Banking" systems;

The date on which the Customer received an account statement in hard copy upon the personal visit to the Bank (in the event the Customer did not request a statement– the first date of the month following the reporting month);

The date on which the Bank sent an account statement to the Customer's email address.

16-1. In case discrepancies have been found between the transactions reflected in the statement and actually performed, the Customer has the right to initiate checking of the reasonableness of the reflection of transactions on the account.

The declaration form for the disputed or unauthorized transaction shall be submitted in writing within a period of up to 30 calendar days from the date of receipt of the information on the Card transactions. Subject to documentary evidence, the time limit for submitting the declaration form for the unauthorized transaction is extended for the period during which the Customer has a good reason for not submitting a declaration form (for example, illness), but shall not exceed 90 calendar days from the date of the transaction's reflection on the Customer's account.

The Bank has the right to determine a list of documents to be provided by the Customer along with the declaration form for the disputed or unauthorized transaction depending on the nature of the disputed transaction (for example, copy of electronic correspondence with the Merchant, documents on the warranty service of goods etc.), as well as request additional documentation in the process of consideration of the Customer's declaration form. Failure by the Customer to provide the required documents is the ground for refusal to perform verification.

The time limit for considering the declaration form for the disputed or unauthorized transaction shall begin to run from the date following the date of registration of the declaration form in the customer complaint logbook. If the last day of the time limit for considering the declaration form falls on a non-business day, the time limit shall begin to run from the next business day.

The decision regarding the disputed transaction declaration form shall be made by the Bank within 45 calendar days from the date of the form's registration at the Bank. This period may be extended provided that the Customer is notified thereof no later 45 calendar days from the date of the form's registration at the Bank. Where it is necessary to dispute a transaction in the payment system, the possibility and the time limits of the disputed transaction settlement shall be determined by the payment system's regulations. The Bank has the right to set the fee for transaction reasonableness check in accordance with the Bank's Fee Guide. Failure by the Customer to pay the fee is the ground for refusal to perform verification.

Notification regarding the extension of the time limits for consideration of the disputed transaction declaration form and the results of the consideration of the

declaration form shall be carried out in a manner specified by the Customer upon submission of the disputed transaction declaration form.

The decision regarding the disputed transaction declaration form shall be made by the Bank within the time limit not exceeding:

45 calendar days from the date of registration of the form at the Bank, provided that the Card transaction was performed in the Republic of Belarus and (or) at the terminal serviced by a resident acquiring bank of the Republic of Belarus;

90 calendar days from the date of registration of the form at the Bank, provided that the Card transaction was performed outside the Republic of Belarus and (or) at the terminal serviced by a nonresident acquiring bank of the Republic of Belarus.

The Customer shall be notified on the results of the consideration of the declaration form for the unauthorized transaction within the time limit for making a decision regarding the disputed transaction declaration form. Notification on the results of the consideration of the declaration form shall be carried out in a manner specified by the Customer upon submission of the declaration form for the unauthorized transaction.

In the event that settlements with the Customer under the disputed or unauthorized transaction are made based on the results of disputing the transaction in the payment system, the amount of the disputed transaction to be reflected on the Customer's account shall be determined on the basis of the equivalent amount transferred to the bank and calculated by the payment system and the exchange rates for card transactions effective on the date of receipt of the equivalent amount of the disputed transaction.

17. The Cardholder can get information on the available balance on the card by contacting the customer service (support) at 8-(017)-299-25-25, as well as via remote services systems.

LOSS OF THE CARD OR PIN, THE CARD BLOCKING

18. If the Card is lost, stolen, the Card's details and/or PIN have become known to an unauthorized person, or if unauthorized transactions using the Card or its details are detected, the Cardholder must immediately block the Card in the Customer service (support) by calling 8(017)299-25-26(25), after which notify the Bank about this in three days in written form (or by fax with the subsequent provision of the original).

The Bank has the right to block the Card without the prior permission of the Customer or the Cardholder of the additional Card in order to prevent unauthorized access to the Customer's account. In case of cancellation of this blocking, on the initiative of the Customer or the Cardholder of the additional Card, an application for a refund on unauthorized operations performed after the blocking is canceled is not subject to satisfaction.

19. The Bank shall issue a new Card upon a written application from the Customer in accordance with the rules of the Bank. For the reissue of the Card, the Bank charges the fee established by the Fee Guide for the transactions performed by the Bank.

20. Upon the request of the Bank, the Cardholder shall provide information to investigate the circumstances of the Card loss. If the Bank has information that the illegal use of the Card occurred with the knowledge of the Cardholder, then the Customer is responsible for the transactions performed using the Card. When finding a Card previously announced by the Cardholder of the stolen or lost, the Cardholder must immediately inform the Bank of this.

21. When the Card previously declared stolen or lost is found, the use of such a Card is strictly prohibited.

PECULIARITIES OF CURRENCY EXCHANGE TRANSACTIONS

22. If the currency of the transaction does not coincide with the currency of the account, and in some cases provided for by the payment systems, a currency exchange transaction is carried out. In accordance with Clause 6 of the Agreement, currency exchange transactions are performed at rates set by the Bank at the time of the transaction, taking into account the cross rates of such international payment systems (hereinafter- IPS) as VISA and MasterCard Worldwide. For transactions using the Bank Cards, separate exchange rates are established, different from the rates for cash transactions. Currency exchange rates for transactions using the Cards can be changed during the working day on the basis of the order of the authorized structural unit of the Bank. Information on the exchange rates established by the Bank for the Card transactions is located on the main page of the Bank's website.

Information about the exchange rates set by the IPS is posted on the websites of the IPS of VISA and MasterCard Worldwide.

For the transactions performed outside the Republic of Belarus or via devices of banks not connected to the JSC Bank Processing Center (hereinafter - BPC), the moment of performing a currency exchange transaction is determined based on the settlement information received from the payment system. If the payment system does not specify the time of the transaction in the settlement information, the currency exchange rates established by the last order for this date shall be applied for the date of such a transaction.

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

23. Transactions processing using the Cards is performed in two systems. Initially - in the system of authorization processing, in which the available amount of the Card changes in real time (increases or decreases by the amount of the transaction), and then in the clearing system, in which the calculated information is formed. Only as the Bank processes the settlement information, the transaction amount is reflected on the Customer’s account.

Since the exchange rates are set by IPS on a daily basis and are updated taking into account the situation on the foreign exchange market, the transaction amount in the account currency at the authorization stage and at the transaction reflection stage may differ (upward or downward).

24. When paying at Merchants, the cashier can offer the customer to choose the payment currency in which the transaction will be performed. Among the proposed currencies, the currency of the account to which the Card is issued is indicated. It is necessary to take into account that in the course of such transactions, in addition to the rates of the issuing bank and IPS, the Merchants' rates are also used, which actually increases the purchase price. For example, if, when making a payment transaction with the Card in US dollars in Poland, the US dollar was selected as the payment currency, then the purchase amount in zloty would be converted into US dollars at the Merchant's rate, which is less profitable than the IPS's rate. In order to avoid unnecessary expenses, we recommend that you always choose the currency of the country in which payment is made when paying at Merchants.

25. When funds are returned to the account of a currency exchange transaction using the 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 or the Merchant.

PECULIARITIES OF TRANSACTIONS PERFORMED VIA THE INTERNET

25-1. Terminology:

3D-Secure is an additional authentication technology for making a payment for goods and services on the Internet using cards, on the basis of which international payment systems have developed special programs - Verified by VISA and Mastercard SecureCode; a similar technology has been developed by the national payment system BELCARD - BELCARD-InternetPassword (БЕЛКАРТ-ИнтернетПароль).

CVV2/CVC2/КПП2 is a three-digit card authentication code, which is applied to the cardholder's signature strip and is used as a security element when conducting transactions on the Internet.

25-2. The Bank provides the holder of the card issued by the Bank with the opportunity to make transactions of the payment for goods and services on the Internet using the card details, taking into account the following peculiarities:

the Bank provides the cardholder with the ability to independently connect 3D-Secure and BELCARD-InternetPassword and is obliged to activate this service within 30 minutes;

with the cards connected to the 3D-Secure technology and/or BELCARD-InternetPassword, making transactions on the Internet is available without restrictions;

at Merchants that support 3D-Secure technology and/or BELCARD-InternetPassword, transactions are possible only with the use of 3D-Secure and/or BELCARD-InternetPassword, so they can not be performed with cards that are not connected to this technology;

CVV2/CVC2/КПП2 is usually used to confirm that a transaction has been performed on the Internet; however, when making repeated (signed) payments at the same Merchant, the absence of confirmation of CVV2/CVC2/КПП2 is allowed;

The Bank may transfer the details of the issued (reissued) card (with the exception of the CVC2/CVV2/КПП2 code) to the system, which ensures the updating of the card details in online stores and services. The cardholder may refuse to transfer the details of the issued (reissued) card;

The Bank has the right to impose restrictions on making transactions for the payment for goods and services on the Internet (including with the use of 3D-Secure and BELCARD-InternetPassword technologies) using cards.

25-3. The Cardholder is responsible for the transactions made using his/her card or its details on the Internet. The Cardholder may not make claims to the Bank on transactions performed on the Internet using the card in case of violation of these Terms and Conditions. Entering the correct card details, CVV2/CVC2/КПП2 code and/or 3D-Secure verification code is a proper and sufficient authentication of the Cardholder to reflect on the Account the transaction performed using the card and its details.

RECOMMENDATIONS FOR SAFE USE OF THE CARDS

26. General recommendations.

26.1. Upon receipt of the Card, sign on its back side in a special field. Having a signature on the Card will reduce the risk of its use by others in the event of its loss, theft. If there is no signature on the Card or if the signature does not conform to the sample on the Card and identification documents, the transaction may be refused and the Card may be withdrawn.

26.2. Save the phone number of the Bank’s Cards service (support) in an easily accessible place (for example, in the memory of a mobile phone or notebook), this information may be useful for blocking the Card in case of loss or theft.

26.3. For each type of transactions (daily and/or regular transactions, payments on the Internet, foreign travel transactions) issue separate cards to different accounts. To make payments abroad, it is desirable to issue several cards of different payment systems to one account and keep the cards separately from each other.

Remember that you should not keep large sums of money on the cards that you use irregularly: for example, you should top up a card for payment on the Internet with the amount you plan to spend and just before making a payment.

26.4. Ensure the storage conditions of the Card, which exclude the possibility of its loss, damage, data copying, unauthorized and illegal use. Avoid mechanical damage to the Card, deformation, pollution, exposure to high and low temperatures, electromagnetic fields, direct sunlight, moisture, dyes, solvents, harmful chemicals and other unfavorable factors that may lead to the inoperability of the Card.

26.5. Do not give the Card to other persons. Only a 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 state that the holder's name may not be indicated. If it is necessary to provide access to your account to other persons, you can contact the Bank for issuing additional Cards to the account.

26.6. Keep confidential data of the Card in secret from other persons: the number and validity of the Card, the three-digit Card authentication code (if

available) indicated on the back, the PIN-code that you need to remember or, if this is difficult, keep it separate from the Card in an implicit form (for example, by rewriting it on a piece of paper among other groups of numbers or any other information). Never disclose a PIN code to other persons, including relatives, acquaintances, employees of banks, merchants, law enforcement representatives. Do not send the PIN code by phone or e-mail. Only the Cardholder must know his/her PIN.

26.7. We strongly recommend you to use the "SMS-informing" service, which provides prompt receipt of information about transactions performed on the Card. The "SMS-informing" service allows you to promptly get information about the account status, changes in the account balance via a text message to a mobile phone. If you receive an SMS message about the transaction that you did not perform, you must immediately block the Card and contact the Bank.

If, with the presence of the "SMS-informing" service, the messages from the Bank about the transactions performed have ceased to arrive on your mobile phone, you should contact the Bank to clarify the reasons in order to exclude the possibility of interception of SMS-messages by third parties. If the received SMS-message causes any doubts or safety concerns, promptly contact the Bank for clarification.

26.8. To interact with the Bank, use only the details of the means of communication (mobile and fixed phones, faxes, Internet sites, regular mail and e-mail), which are indicated in the documents received directly from the Bank.

26.9. In case of loss, theft of the Card, leaving it in an ATM or other self-service device, withdrawal by the cashier of the merchant, compromise of the Card (if the confidential data of the Card became known to unauthorized persons) or in case of such suspicions, it is necessary to immediately block the Card (for example, by calling the service (support), or through remote banking systems) and contact the Bank.

26.10. Keep card receipts and other documents on transactions with the Card for verification with the account statement. Try to check the account regularly, at least once a month, as well as after trips abroad in which the Card was used. If you find any discrepancies between the transactions actually performed and those reflected in the statement, please contact the Bank to clarify the validity of the transactions.

26.11. Use the possibilities offered by the Bank to set limits on transactions. It is recommended to disable or limit the possibility of payment by the Card on the Internet, as well as making transactions abroad, if you do not plan to perform these transactions in the near future.

27. Conducting transactions using the Card at ATMs and infokiosks.

27.1. When choosing an ATM or infokiosk in which you want to conduct a transaction using the Card, it is advisable to avoid poorly lit and deserted places. The safest places for transactions are the bank offices, while street ATMs in tourist areas are less secure.

27.2. To perform regular transactions, try to use the same ATM located in a well-lit place: it will be easier for you to identify the fact of installing third-party equipment on it, which can be used by fraudsters to steal information from the Cards.

27.3. Inspect the front panel of the ATM before servicing. ATMs of some banks offer to verify 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 not provided by the design of the ATM. Before using an ATM or other self-service device, touch the panels, try to move them: the fake overlays and keyboards usually hold up badly and, as a rule, even with a minor impact, wobble, move away or even fall off. Often, fraudsters leave visible traces: cracks, glue smudges and chips. It is better not to use an ATM, whose card reader looks like someone was picking it with a screwdriver or doused it with glue.

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

If the keyboard is unnaturally bulging, staggering or differs in tone, it looks new, while the ATM itself already shows obvious signs of depreciation - this is also a reason to refuse to use such a self-service device.

27.4. Do not use excessive physical force to insert the Card into the ATM (infokiosk). If the bank Card is not inserted without additional efforts, refrain from using this ATM (infokiosk).

Some ATMs (infokiosks) may use such special devices as jitters that prevent from copying Card data. In these ATMs (infokiosks), the process of accepting Cards by the device may differ from other ATMs (infokiosks) - The card vibrates at the time of its reception by the device.

27.5. When detecting extraneous equipment (for example, an overlay), do not try to remove it yourself, refrain from performing transactions, and report the detected overlay to the bank servicing the device. If doubts about the correct transaction of an ATM or other self-service device have arisen after the Card has been placed in the card reader, do not enter the PIN code. Click the button to cancel the transaction and take the Card. If you notice extraneous equipment after the end of the service, be sure to block immediately the Card in any possible way.

27.6. Make sure that the chosen ATM or other self-service device accepts your Card. The logo on your Card and on the screen of the program-technical device and (or) on its body should be the same. If you insert a Card that is not serviced in this device into an ATM or other self-service device, the Card will be returned to you, and information about the impossibility of performing the transaction will appear on the screen.

27.7. If there are suspicious people near the ATM or other self-service device, you should choose another time to use this device or use another ATM or self-service device.

27.8. Be especially careful if strangers offer you assistance in using the Card at the ATM or other self-service device. In case of difficulties arising from using the Card, do not listen to the advice of strangers, and to communicate with the Bank, use only the telephone numbers that are indicated on the Card or were received by you from trusted sources or directly at the Bank.

27.9. Pay attention to people behind you in the queue at the ATM or other self-service device, if necessary, ask them to go a distance from which they can not see the PIN code you enter. When entering a PIN code, stay as close as possible to the

ATM or self-service device, while covering the keyboard with the palm of your free hand.

27.10. When using the Card, study carefully the information displayed on the screen of the ATM or other self-service device, and check the correctness of the entered data. If you repeatedly enter the PIN-code incorrectly, the Card will be blocked and can be withdrawn by the ATM or other self-service device. In case of withdrawal of the Card (regardless of the reason) by the ATM or other self-service device, immediately block it (for example, by contacting customer service (support) or using remote banking services systems).

27.11. Do not let anyone distract you during the transaction, as you may accidentally perform an incorrect transaction. In addition, in the absence of any actions on your part during the time set for this device, it may withdraw your Card and/or money.

27.12. After receiving cash from the ATM, you should make sure that the Card was returned by the ATM, wait for the issuance of a card receipt (when requested), and only after that move away from the ATM. It should be remembered that the sequence of cash withdrawal and return of the Card at ATMs of different banks may differ. The ATM may first return the Card and then issue the requested amount of cash. It is necessary to take into account the specifics of the transaction of ATMs and not to move away from the device until the receipt of the Card, the card receipt (when requested) and money.

27.13. If an ATM or other self-service device does not work correctly (for example, it is in standby mode for a long time, it spontaneously reboots), you should stop using such a device, cancel the transaction performed by pressing the corresponding button on the keyboard, and wait for the Card return. If the device does not return the Card, immediately block the Card in any possible way and contact the Bank.

27.14. Do not leave the card receipt you requested at the ATM or other self-service device, as the receipt may indicate the amount of the transaction, the balance of funds. This may attract a burglar or fraudster.

28. Receipt of cash and carrying out non-cash payment transactions using the Card in the bank branches.

28.1. All actions of the bank employee with the Card must be carried out under your supervision. Do not allow a bank employee to go with the Card to another room.

28.2. When receiving cash or making a non-cash payment, pay special attention to the correspondence of the specified amount and the amount contained in the card receipt (slip).

28.3. A bank employee has the right to demand a passport for identification of the Cardholder and execution of the transaction.

28.4. When conducting transactions at CAO, pay special attention to the actions of the bank employee if he/she tries to hold your Card through the reader of equipment more than once. This will prevent unauthorized transactions. Be sure to ask the reason why the employee needs to repass the Card through the reader equipment.

28.5. Before entering the PIN code, carefully review the information provided on the terminal screen, and also verify that the amount and currency of the transaction are correct.

28.6. Enter the PIN code, covering the keyboard with the palm of your free hand. Never and under any circumstances do not disclose the PIN code to bank employees.

28.7. Before signing a card receipt, 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 receipt are correct.

29. Conducting non-cash payment transactions using the Card at the Merchants.

29.1. Use Cards at credible merchant.

29.2. When carrying out transactions in the restaurants, bars, shops, giving the Card to service personnel, do not let it out of sight. If necessary, follow the merchant employee to the terminal. This will prevent illegal copying of the information indicated on the Card.

29.3. When making a transaction using an imprinter or a payment terminal (POS terminal), the cashier may request to enter a PIN code or sign a card receipt in accordance with the requirements established by the rules of payment systems, within which the Cards are issued, and also provide a passport for Cardholder identification.

29.4. When conducting a payment transaction at Merchants, pay special attention to the cashier’s actions if he/she tries to pass the Card through the reader equipment more than once. This will prevent unauthorized transactions. Be sure to ask the reason why the cashier needs to repass the Card through the reader equipment. If, as a result of an unsuccessful Card transaction, you have paid for the purchase in another way (for example, in cash or with another card), save the supporting document and check whether the funds for the unsuccessful operation were written off from the account.

29.5. Enter the PIN code, covering the keyboard with the palm of your free hand. Before entering a PIN code, you should make sure that people standing near you will not be able to see it. Never, under any circumstances, do not disclose a PIN to Merchant employees.

29.6. Before signing a card receipt, make sure that the amount and currency of the transaction, the Card number (its part), the transaction date, the type of transaction, the name of the Merchant and other data indicated on the card receipt are correct.

29.7. If you decide to cancel the purchase after the successful completion of transaction, ask to cancel the transaction. Be sure to save the card receipt of the canceled transaction before checking the account statement to which the card was issued.

29.8. Contactless transactions are performed in the "self-service" mode - the holder does not give a card or other payment instrument used for payment (for example, a bracelet, keychain, mobile phone or other device) to the cashier, but independently puts the card or other payment instrument to the reader of the terminal for the transaction.

30. Performing cashless payment transactions using the Card on the Internet.

30.1 Do not use cards on which you have large sums of money for payment on the Internet. For such purposes, it is better to have a separate card (to a separate account) and transfer money to it only when needed. When using the Virtual Card “Unreal Card”, we recommend not to use it for keeping money, but to replenish the Card when needed.

30.2. To ensure the highest level of security of transactions, connect the transaction confirmation service using 3D-Secure technology and/or BELCARD-InternetPassword (БЕЛКАРТ-ИнтернетПароль). These technologies allow you to request additional confirmation of transactions performed on the Internet using a one-time password sent to the phone (via SMS), specified when you connect the service.

The website of an online store that provides payment acceptance using 3D-Secure and BELCARD-InternetPassword technologies, as a rule, should place the logos of the corresponding payment system programs:

30.3. Do not reply to the e-mails in which, on behalf of the Bank or other organizations, as well as citizens, it is asked to provide personal information, including the details of the Card, in order to update them or to register. Try to find out the validity of such offers by contacting the Bank by calling a reliable telephone number (for example, received by you directly from the Bank upon receipt of the Card).

Give the information about your card only to pay for the purchase. Never send the card data by e-mail, as the e-mail information is not completely protected from interception and use by outsiders. The websites of all well-known reliable retailers use data encryption technology that protects your personal information when making a purchase.

Never show your card number to prove that you have reached a certain age, although sometimes on some sites you may be asked to do so. Card number can not indicate that you have reached any age.

30.4. Attackers often spread virus programs through different Internet resources, from social networks to common news sites. The customer whose computer is infected, when trying to log into a personal account, can be quietly redirected to a "phishing" website, which outwardly practically does not differ from the authentic websites of Internet banks, online stores or other payment services. To avoid this, try to maximize the use of your browser and email client security features. To do this, you need to enable additional functions in the browser and mail client options. For example, "Pop-up Blocker", "Protection against phishing and malware", "Open files based on content, not extensions", etc. Moreover, do not use the preview window in the mail client you use.

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

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

When making a payment with the card on the Internet, make sure that the fragment of the web address "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.

30.6. Before making a payment for a product (service), carefully review 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. Especially read carefully the terms and conditions of transactions related to gambling (casinos, lotteries), as they may include an automatic subscription, which will entail the writing off the funds on a regular basis. Separately assess the feasibility of the transaction, if the information on the conditions of purchase is presented in an unfamiliar language. Find the phone number or e-mail address of Merchant and write them down in case you have any questions.

30.7. Keep records of transactions performed on the Internet, including the addresses of websites of online stores. Many online stores send e-mails to customers with a summary of transactions, so save or print them. Keep any electronic documents, e-mail correspondence regarding attempts to resolve the dispute with Merchants, as these documents may be very important to protect your rights. If it is impossible to resolve the disputable situation on your own, contact the Bank.

30.8. Some Merchants (for example, hotels, car rental offices) have the right to request a Card authorization before selling goods, performing works and providing services as a guarantee of the Cardholder’s solvency. As a result of authorization, the requested amount is blocked on the Customer's Card, and becomes unavailable.

30.9. If a hotel was booked via the Internet site, but for some reason it is not planned to use it, be sure to cancel the reservation through the same Internet site according to the procedures indicated on it. The receipt of the hotel cancellation code by the Customer is proof that the reservation is indeed cancelled. Otherwise, for late cancellation of the reservation, the hotel has the right to submit to the account the sum of money in the amount established by it.

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

30.10-1. Make sure that transactions performed by you are legal. If logos of payment systems are present on the website of the online casino or on other sites of gambling, this DOES NOT mean that conducting operations associated with participation in gambling is legal. If you have any questions or doubts about the legality of the transactions, contact the Bank.

30.11. Make purchases only from your devices, do not use Internet cafes and other publicly available tools where spyware can be installed to store the confidential data you enter.

30.12. Install licensed software, including anti-virus, and firewalls on your devices, and regularly update them. 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 and questionable recipients.

30.13. Connect to the Bank's services, which allow to exercise operational control over expenses on your card (Internet banking, Mobile Internet banking, SMS informing, etc.).

30.14. If you suspect illegal withdrawal of money, we recommend that you immediately block your card and contact the Bank.

31. Use of remote banking systems.

31.1. When using the Internet banking system, pay attention to the presence on the service page of the secure HTTPS protocol. Before logging in, it is recommended to verify the authenticity of the certificate and site. As a rule, to do this, click on the Internet in the address bar (the field with the lock or paper sheet icon) and check the information in the block. In the case of inconsistency of the data present with real information about the Bank, it is worthwhile to immediately leave the page.

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

31.3. Be careful when visiting websites with questionable content: they, as a rule, are the source of the newest viruses.

31.4. After completing a session with the Internet banking system, be sure to log out correctly using the appropriate option.

32. Performing transactions using the Mobile Banking and Mobile Internet Banking applications.

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

32.2. Remember that the Bank does not send its customers links or instructions for installing applications via SMS/MMS/e-mails.

32.3. Do not install the Bank’s mobile applications on the mobile phone (device) on which root rights are obtained (superuser rights). Such phones and devices are also not recommended for receiving messages from the Bank (for example, SMS with a code (one-time password) for authentication).

32.4. If you lose your mobile phone (device) on which the Bank’s mobile application is installed (SMS messages with confirming one-time passwords arrive)

or an unexpected termination of the SIM card, you should block the SIM card as soon as possible.

33. Features of performing transactions using the Card.

33.1. It is necessary to take into account that the specifics of transactions with the use of the Card imply 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 location of the transaction (in the Republic of Belarus or abroad), the technical infrastructure (Bank or other bank), the time of the transaction (night or day, working days or weekend, holidays).

33.2. Depending on the country of stay and the Bank, when conducting a transaction using the Card, an additional fee (remuneration) may be withheld, the amount of which is advisable to ask the employee who serves you before performing the transaction, or having previously studied the bank information on its official website. Moreover, such information can be displayed on the screen of an ATM or a self-service device during a transaction.

33.3. If you are still affected by fraud, you must immediately block the Card and contact the Bank. On the fact of fraud, you must file an application with law enforcement agencies.

33.4. When making transactions for the payment of goods (services), cash withdrawals abroad, it is worth paying attention to the availability of the Dynamic currency conversion (DCC) service. This service offers an additional stage of conversion, 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 set by the bank offering the DCC service. It is necessary to closely monitor the information presented on the terminal screen, as well as to check the terms of the transaction indicated in the card receipt (in particular, you should pay attention to the presence of the DCC abbreviation). In case of disagreement with the terms of the transaction, insist on g the cancellation of the transaction and its conduct without the use of dynamic conversion. In case of disagreement of employees of the organization to cancel the operation using dynamic conversion it is worth contacting the police without leaving the organization.