



GENERAL TERMS AND CONDITIONS
FOR PROVISION OF PAYMENT SERVICES AND
RELATED PAYMENT INSTRUMENTS

SECTION I. SUBJECT AND GENERAL PROVISIONS

These General Terms and Conditions (referred to as "GTC") establish the order and conditions under which "Bulgarian-American Credit Bank" AD (referred to as "the Bank"/"BACB"), registered in the Commercial Register and Register of Non-Profit Entities, maintained by the Registry Agency with UIC 121246419 and headquartered at: Sofia 1000, Capital Municipality, "Sredets" region, "Slavyanska" Str. № 2, email for contact: bacb@bacb.bg, website: www.bacb.bg, and supervised by the Bulgarian National Bank, located at Sofia 1000, "Knyaz Alexander I" Square, provides payment services and associated payment instruments as defined by the Payment Services and Payment Systems Act (PSPSA). They regulate the relationships between the Bank and: (i) individuals as users under the PSPSA (referred to as "Customer - user"), and (ii) legal entities and sole proprietors (referred to as "Customer"). Collectively, both categories are addressed as "Customers", "Account holder", or "Account holders".

(1) The GTC are mandatory for all Customers and form an integral part of the framework agreements for the opening and servicing of bank accounts, provision of payment services, remote banking, issuance of debit cards, and other services offered by the Bank. Should there be any inconsistency between the provisions of these GTC and those of the individual contracts for bank accounts, payment services, remote banking, debit cards, or other payment services agreed between the Bank and a Customer, the terms of the individual contracts will prevail.

(2) All terms and definitions used in these GTC are explained and defined in the Terms and Definitions Glossary, which is an inseparable part of these GTC.

(3) The framework agreements, GTC, and all associated documents can be signed by the Bank and the Customer electronically, using remote banking applications and/or electronic signature in accordance with the Electronic Document and Electronic Trust Services Act (EDETSA). The consequences of concluding/signing electronic documents with electronic means as described in these GTC apply.

In the relationships between the Bank and the Customer/User of remote banking applications, as regulated by these GTC, the following electronic means for signing electronic statements/documents are considered equivalent to a handwritten signature, thereby binding the parties: (a) Qualified Electronic Signature (QES), issued by a qualified authentication service provider, according to Regulation (EC) 910/2014 on electronic identification and authentication services (eIDAS); (b) Server certificate, which qualifies as an advanced electronic signature under Regulation (EU) No 910/2014; (c) "Electronic Transaction Authorization Number" (eTAN) or a PIN for mobile banking, or the Signer application or the respective application of the end-user's mobile device, owned by the Customer/User, which are recognized as either an advanced electronic signature or an electronic signature as per Regulation (EU) No 910/2014; (d) Other electronic means of signing electronic documents introduced by the Bank, such as ticking a "checkbox" and/or pressing the relevant virtual button, which are considered electronic signatures within the meaning of Regulation (EU) No 910/2014.

(4) The electronic statements/documents, signed by the Bank and/or the Customer/User of remote banking applications using the above-mentioned electronic means for signing, are deemed valid and binding documents, carrying the same weight as a handwritten signature by the respective party, as defined under the Electronic Document and Electronic Trust Services Act (EDETSA).

(5) When providing payment services and instruments, the Bank does not oversee or assume responsibility for the subject and legality of the transactions related to the use of the payment service/instrument,

unless specifically provided by a regulatory act.

(6) In initiating relationships for account opening or payment service provision, the Bank conducts identification and due-diligence in accordance with the applicable legislation on anti-money laundering and counter-terrorism financing. To this end, the Customer must submit identification documents and complete legally-required and Bank-specific declarations, information questionnaires, and forms. The Bank may request additional information and documents as per the current legislation.

(7) A power of attorney for representation at the Bank must comply with Bulgarian law, clearly express the intent for representation by the Customer for the particular service/instrument, and the authorizer's signature must be notarized. The power of attorney should be submitted in its original form along with a valid identification document of the proxy.

(8) The Bank is entitled to request explicit written confirmation of the validity of the power of attorney from the proxy, and to perform checks on the power of attorney in public registers.

(9) The Bank reserves the right to decline a power of attorney if it doesn't comply with the legal requirements or based on the Bank's own discretion. This includes, but is not limited to, situations where: the scope of the proxy's authority isn't clearly and unambiguously defined; the power of attorney includes a condition for terminating the proxy's rights or a performance condition outside the Bank's control or causing undue difficulties in providing the respective service/instrument; the power of attorney cannot be verified in the relevant registers; the Bank cannot obtain explicit written confirmation of the power of attorney's validity from the proxy; or if there are doubts regarding the regularity and validity of the power of attorney, among other similar issues.

(10) Powers of attorney for representation before the Bank shall be valid until explicitly withdrawn. The withdrawal of the power of attorney shall have effect to the Bank only and shall be binding on it as from the time the Bank has been notified in writing of the withdrawal.

(11) The powers of attorney deposited by a Customer - legal entity shall be valid and binding on the Bank until the date of their explicit written withdrawal deposited with the Bank, including after the change of the representation power of the legal entity, duly registered with the respective public register.

(12) Powers of attorney drawn up in a foreign country shall be deposited with the Bank: a/ certified in the Bulgarian Embassy or in the Bulgarian Consulate in the respective country; or (b) legalized according to the appropriate procedure; or (c) certified by Apostille. The powers of attorney shall be presented to the Bank with a certified translation into Bulgarian (with a notary certification of the translator's signature).

(13) Any amendments to the constituent documents, the good standing of the company, the representative power of the Customer, as well as to other documents presented by the Customer to the Bank, and/or to the personal and other data of the Customer and the persons authorized to dispose with the funds in a current account, shall have effect in relation to the Bank and shall be binding on the Bank as from the time it has been notified in writing of the amendment, even if the amendment has been registered with a public register.

(14) The Bank withholds tax at the source on interest income paid to an Account holder who is a foreign individual (in cases of a joint account – if one of the Account holders is such) in the cases and amounts determined under the applicable Bulgarian tax legislation. The income shall be tax-exempt in the Republic of Bulgaria provided that the foreign person submits to the Bank a certificate confirming that, for the respective calendar year, it is a tax resident of an EU or EEA Member State, issued by that state. Tax on interest income paid to an Account holder who is a local resident is withheld, if it is prescribed by the current Bulgarian tax legislation.

(15) In the event of death of a Customer - natural person or

termination and/or transformation of a Customer - legal entity, the provisions of the Bulgarian legislation shall apply to all legal consequences resulting therefrom. The Bank shall require the submission of documents certifying the rights of the legal successors of the Customer (certificate of heirs, documents for registration changes, etc.).

(a) In the event of death of a customer-natural person, the Bank shall pay each of his/her heirs (by law or by last will and testament) their respective parts of the account balances, subject to the submission of the following documents: 1/ Certificate of heirs; 2/ Certificate from the register of property relations at the Registry Agency, regarding the registration regime of the property relations (not required if the Account Holder had died prior to 1.10.2009, as well as if such person has died widowed, divorced or single). The certificate shall be required for a deceased Account Holder or the surviving spouse; 3/ A document of inheritance (if such document has been provided by the parties or if after the verification, carried out by Bank's lawyer with the IKAR – property registry, it has become evident that an last will and testament has been filed), in the form, required by the Inheritance Act; 4/ ID card or another document, evidencing heirs' identity; 5/ A certificate by the tax office, evidencing the payment of the inheritance tax or that no such tax is due (such certificate shall not be required for the surviving spouse and the direct heirs, without any limitation on the degree).

(b) The Bank shall pay amounts under inherited accounts, subject to the following terms and conditions:

(i) In case of simultaneous appearance of all heirs (personally or through an explicitly authorized representative) all the available amounts shall be paid in the manner, specified in the order, signed by all heirs; or

(ii) If only some of the heirs appear, the payment of amounts from such inherited accounts shall only take place to the heirs present, after the Bank allocates the moneys pursuant to the Inheritance Act. The shares of the non-present heirs shall remain in the account of the deceased Account Holder without interest accrual until such other heirs appear and present their instructions. When amounts from an inherited fixed-term deposit are being paid, the deposit shall be automatically terminated upon the payment of the share of the first appearing heir, and such deposit shall be transformed into a non-interest-bearing deposit. If the deceased Account holder had multiple accounts in the same currency, their funds are combined into one of the existing accounts in the following order: current account, savings account, then fixed deposit. First, the accounts accrue interest, any closure fees are deducted (if applicable), and after transferring the funds, the accounts are closed.

(iii) When other documents (complaints, objections, wills, etc.) are presented or if there are other contentious issues, the Bank may refuse to disburse funds from an estate account until the dispute is settled and can request further documentation.

(iv) In the case of a pensioner's death, the Bank disburses the balance of the account where the pension was deposited to the heirs, but only after receiving a certification from the local office of the National Social Security Institute.

(v) When a joint account holder passes away, the deceased's portion of the available funds in the joint account is allocated to their heirs. Unless specified differently in the joint account agreement, it's assumed that the shares of the account holders are equal. The funds from the joint account are then distributed into the individual current accounts of each account holder (including any accounts opened ex officio), following which the joint account is closed.

(vi) Before releasing inheritance funds, the Bank reserves the right to ask the heirs for additional documents at its discretion.

(c) Information, regarding the presence of accounts and balances of deceased individuals shall only be provided to their heirs (by law or according to the last will and testament) subject to the provision of original: death certificate of the deceased person, certificate of heirs, last will and testament (for heirs, according to last will and testament)

and document, evidencing the identity of the heir.

(d) In the event of death of the representative of a legal entity, the entry in the respective register or court decision /Commercial Register or Register of the Non-Profit Legal Entities of the Registry Agency/ for the new individual, who shall manage and represent the company shall be required.

(16) Documents issued in a foreign language and/or drawn up abroad shall be presented to the Bank in the original or as a notarized copy, duly legalized or, respectively, accompanied by an Apostille and with a certified translation into Bulgarian (with a notarized certification of the signature of the translator). At the discretion of the Bank, documents in English may also be accepted on a case-by-case basis, without translation into Bulgarian. If a document, issued by a foreign country, intended for use in the Republic of Bulgaria is submitted in English, without a certified Bulgarian translation, the Customer shall – within 30 days, submit to his/her respective office, a certified Bulgarian translation.

(17) Instructions/ orders for transactions shall be submitted by the Customer in writing at the Bank's offices or using the remote banking applications, signed by the Customer or by a person authorized by him/her. Provided that the Client has given the Bank his/ her prior written consent-declaration (according to the Bank's form) for submitting an order by e-mail, the Bank may execute orders/instructions received by e-mail based on the procedure and in the manner stipulated in the consent-declaration, while reserving its right to require additional confirmation from the Client for each of the individual orders/instructions, and in this case the costs shall be fully covered by the Client.

(18) The Bank shall verify and identify whether a Customer of the Bank falls within the scope of the categories of persons for whom the Bank should exchange financial information automatically and for such customers, in compliance with the legal provisions, the Bank shall annually provide information to the National Revenue Agency on their personal data, account balances at the end of the year, the interest income received during the previous year, and any other information required for the purpose of automatic exchange of financial information.

(19) All phone calls to the BACB Contact Centre are recorded and kept by the Bank. In case of a dispute, the Bank has the right to use these recordings as evidence.

SECTION II. PAYMENT SERVICES PROVIDED BY THE BANK

II.1. TYPES OF PAYMENT SERVICES PROVIDED BY THE BANK AND RULES FOR THEIR PROVISION

1. Opening and servicing payment accounts. (1) The Bank opens and manages payment accounts for both natural persons and legal entities, including sole traders, in local and foreign currencies. This is done following the PSPSA regulations, Bulgarian National Bank's ordinances for applying PSPSA, the Law on Credit Institutions, and other relevant provisions of Bulgarian law and these GTC.

(2) The Bank may refuse to open a payment account for any Customer without needing to explain its reasons, except when the Customer - user wishes to open a payment account for basic operations (PABO). In this case, the Bank can only refuse based on reasons listed in the PSPSA and the applicable legislation.

(3) Only the account holder or persons authorized by a notarized power of attorney have the right to manage a payment account. This excludes situations where the Bank holds an official directive from a court or another competent authority that limits the free use and disposal of the account's funds or requires a transfer of a certain amount specified in the directive, as well as in cases outlined in these GTC.

2. Opening and management of a PABO. (1) The Bank is offering to a Customer – user a PABO in the national currency, for the provision of the following services on the territory of the Republic of Bulgaria: 1/ opening, using and closing a payment account with/without issuing a debit card thereto; 2/ depositing amounts to the payment account; 3/ cash withdrawal from the account at a Bank's desk or ATM during

Bank's business hours or outside of such hours; 4/ execution of the following payment transactions: (a) direct debits /executed until 31.12.2025/; (b) payment transactions performed using a payment card, incl. online payments; (c) credit transfers in the national currency using BISERA, incl. regular transfer orders, at ATMs and POS terminals and at the bank desks as well as using the remote banking applications. To open a PABO, the customer-user deposits an Application for opening a Payment account for basic services at the Bank's desks, and certifies the circumstances stated therein by presenting the documents described in the Application.

(2) In cases where funds from the categories specified in PSPSA (such as employment compensation, pensions, social insurance and social assistance benefits, scholarships for students and doctoral candidates) are received into the PABO, the terms stipulated in Article 120a of PSPSA are applicable to that account.

3. Transfer of a payment account. A Customer - user is able to initiate the transfer of a payment account from one payment service provider to another within Bulgaria, provided that his/her accounts with both providers are maintained in the same currency. The Bank is obliged to supply the Customer with the necessary information and the account transfer procedure free of charge, either on paper or another durable medium (such as the Bank's website).

4. Cross-border opening of an account for a Customer - User. When a Customer holding a current account with the Bank notifies the Bank in writing that they want to open a current account with a payment service provider located in another EU Member State, the Bank shall: 1/ provide free of charge a list of all currently active orders for periodic credit transfers and direct debit consents /valid by 31.12.2025/, incoming periodic credit transfers and direct debits /executed by 31.12.2025/ - made to the Customer's current account for the previous 13 months. 2/ transfer the balance, if any, to the Customer's current account with the new payment service provider, provided that the request contains the full identification details of the new payment service provider and the new current account; 3/ close the Customer's current account. If the agreed time limit for the termination of the Framework Agreement is respected and the Customer has no outstanding obligations on their current account with the Bank, the Bank shall perform these actions on the date specified by the Customer, which should be at least 6 business days after the receipt of the request, unless otherwise agreed. The Bank shall immediately notify the Customer if the Customer's account cannot be closed due to the presence of outstanding liabilities, active liens and/or other blocking/reasons.

5. Payment Accounts Offered in a Package to the Customer - User. When offering services related to a payment account to a Customer - User as part of a package including various other products and services not directly linked to the payment account, the Bank provides the option to open and service the payment account independently of the package and the services included therein.

6. Bulk Transfers. Customers have the capability to perform bulk transfers in the national currency from their current account opened with the Bank to other accounts, either within the same bank or different banks in Bulgaria. These transfers are executed via an electronic submission of a Bulk Payment File (BPF), in accordance with the guidelines, methods, and procedures outlined on the Bank's website, specifically in the section "Products for Business Customers/Payments/Bulk Payments". The Customer shall be fully responsible for any and all amounts, incorrectly transferred, as a result of incorrect or inaccurately specified data in the electronic file sent and/or inaccurate/invalid/non-existent account number (IBAN) or BIC of beneficiary's bank.

7. Payment order. (1) In order to ensure appropriate execution of the payment orders, the Customer shall provide the Bank with the information, as required in the standardized payment order forms applied by the Bank. The IBAN of the bank account of the payment order beneficiary, international bank identification code of the beneficiary's bank (BIC), or other unique identifier of the beneficiary's

account (for countries outside the European Economic Community) is required for the appropriate identification of the beneficiary.

(2) Payment orders that do not comply with the Bank's forms, are accepted only if they contain all mandatory elements required for their implementation.

(3) Payment orders shall contain fields to be completed in accordance with the requirements of Regulation (EU) 2023/1113 of the European Parliament on information accompanying transfers of funds and transfers of certain crypto-assets, as well as other applicable legislation.

8. Authorization of payment transactions by the Customer. (1) The Bank shall execute payment transactions in accordance with the procedure and under the provisions of these GTC if they have been authorized by the Customer, prior to the implementation of the payment transaction through a payment order/ instruction or consent for the implementation of the payment transaction submitted on paper or electronically or by electronic means: ((a) at the Bank's service desks; (b) via remote banking applications; (c) by email, subject to the Customer's prior consent to send instructions/orders by email; (d) as stipulated in a written contract/agreement/document; (e) using payment instruments at the initiative of or via the recipient of the funds, with the Customer's prior consent for conducting such payment transactions; (f) payment order signed with a Qualified Electronic Signature (QES), in circumstances specified in these GTC or in other GTC applicable to specific products and services.

(2) The Bank executes the Customer's directed payment transactions if all of the following conditions are concurrently fulfilled: 1/ the payment transaction is ordered by the Customer or their proxy, or the Customer has agreed to its performance; 2/ there are sufficient funds in the account for the transaction and to cover any related fees and commissions; 3/ the Customer has provided all necessary documentation required by the Bank or by law for carrying out the transaction; 4/ the size and type of the payment transactions are within the Customer's or their representative's authority; 5/ the transfer order is clear, precise, and complies with the prevailing legal and regulatory standards, the terms of the Framework Agreement, the Bank's form samples, and includes all details necessary for its execution; 6/ there are no legal restrictions preventing the execution of the payment transaction.

(3) The Bank debits a Customer's account without their consent in the following cases: 1/in the event of an automatic corrective transfer within the meaning of the PSPSA and Ordinance No.3 of BNB; 2/ in the case of imposed attachment and enforcement, in accordance with the rules, set out in the applicable laws; 3/ for the payment, based on a direct debit order, received, subject to the presence of Customer's prior consent /executed until 31.12.2025/; 4/regarding ex-officio collection by the Bank, subject to Customer's preliminary consent; 5/ in any and all other cases, pursuant to the current legislation, these GTC or as expressly agreed in writing between the Bank and the Customer.

9. Limitation of payment transactions. (1) No partial transfers on individual payment orders shall be allowed. Partial payments may be executed only in the case of enforcement in accordance with the law and in the cases of ex-officio collection by the Bank.

(2) The Bank shall not execute payment orders and payment transactions related to the trading in virtual currencies (crypto currencies, bitcoins, etc.) as well as to platforms trading in such currencies. Upon receiving payment orders in favor of persons associated with the trading in virtual currencies (crypto currencies, bitcoins, etc.) or trading in virtual / crypto currencies, the Bank shall not execute the payment transaction.

10. Revocability/Irrevocability of a Payment Transaction. Withdrawal of Order/Consent. (1) The Customer, acting as a payer, cannot cancel a payment order after it has been received by the Bank, except in the cases and within the deadlines outlined herein below.

(2) In cases where a Customer and the Bank have agreed to execute a payment order on a certain day or on the day following the expiration

of a certain period, or on the day on which the payer provides the Bank with the funds necessary to execute the order, the Customer may revoke the payment order at the latest the end of the business day preceding the day agreed.

(3) After the cancellation deadlines outlined in this article, but in any case before the crediting of the recipient's account, a customer who is a consumer may cancel a payment instruction only with the Bank's consent. This rule does not apply to customers who are legal entities or sole proprietors (i.e. clients not considered consumers under the PSPSA). Clients who are legal entities or sole proprietors can cancel a payment order only with the Bank's consent and prior to its execution.

11. Execution of a direct debit in the national currency /applicable until 31.12.2025/. In the case of direct debit payments in the national currency, where the Customer is a payer, it shall give its consent in advance to the Bank, and a copy of the consent shall be sent to the beneficiary. Prior to the execution of the payment, based on a received direct debit order, the Bank shall verify that: 1/ the payer has given in advance a consent for the direct debit, related to the respective payment, incl. that all documents, required for such execution have been received, if the submission of such documents has been agreed; 2/ there is free available balance on the respective account, for making such a payment.

12. Payment order receipt. The payment order shall be considered received from the time when the Bank receives it directly from the Customer as a payer or indirectly from or through the recipient. In the event that the time of receipt is not a business day, the payment order shall be deemed to have been received on the following business day. Where the Customer and the Bank agree that the payment order is to be executed on a certain day or on the day following the expiration of a certain period, or on the day on which the payer provides the Bank with the necessary funds for its execution, the time of receipt shall be considered to be the day agreed, and if that day falls to be a non-business day for the Bank – on the following business day. Payment orders in the national currency in paper form deposited with/received by the Bank by 4.30 pm shall be processed on the same business day for the ordering party. Payment orders in the national currency for execution via the RINGS payment system (operational until 31.12.2025) within the same business day shall be accepted by 3.00 pm. Payment orders in foreign currency deposited with/received by the Bank by 4:00 pm shall be processed on the same business day for the ordering party. Payment orders deposited/received after these hours shall be processed on the following business day. The procedure for receipt and implementation of payment orders via remote banking applications shall be governed by Section III of these GTC.

13. The Bank shall be entitled to refuse to execute the payment transaction requested by the Customer under restrictions imposed by the applicable law or these GTC and/or in other cases agreed between the Bank and the Customer and where the order is unclear, inaccurate or does not contain all the details required. In case of suspicions and / or need for submission of additional documents and/or conduction of further checks to establish certain facts or circumstances relating to the implementation of the Measures Against Money Laundering Act (MAMLA), the Measures Against Terrorist Financing Act (MATFA) and any other applicable legal regulations relating to the prevention of money laundering/ terrorist financing, the Bank may suspend, delay the execution, request an additional confirmation or information for the execution of the payment transaction from the principal or refuse the execution of a payment transaction. In case of refusal, suspension or delay to execute a payment order, the reasons for it shall be communicated to the Customer, unless the effective legislation prohibits it. A payment order, the execution of which has been refused by the Bank, shall be deemed not to have been received.

14. Deadline for execution of payment transactions in the national currency, EUR and payment transactions related to a single currency exchange in Bulgaria, as well as cross-border payment transactions in EUR: (1) endorsement period: 1/ In case of a transfer – the account of the payment service provider of the beneficiary shall be credited with

the amount by the end of the next business day, following the receipt of the order, at the latest ; This term may be further extended by one more business day in case of execution of payment operations, initiated on paper; 2/ When transferring via real-time settlement payment system (TARGET or RINGS (operational until 31.12.2025)) the beneficiary's payment service provider account is credited within 1 hour of receiving the order; 3/ For incoming transfers – the value date for crediting the recipient's account is no later than the business day on which the Bank's account is credited with the transfer; 4/ When both the payer's and the recipient's accounts are with the Bank, the recipient's account is credited on the same business day; 5/ Upon receipt of an instant credit transfer in euro, the funds from the transfer shall be made available to the payee immediately, 24*7*365. (2) Period for the execution of transfers, 1/ initiated through the remote banking applications: a/ In case of a standard credit transfer in Euros (SEPA), the Bank shall debit ordering party's account with the amount of the transfer on the date of receiving the order and execute it with a value date not later than the next business day; b/ In case of express credit transfers in Euros, the Bank shall debit ordering party's account with the amount of the transfer on the date of receiving the order and execute it with value date on the same business day; c/ In the case of an instant credit transfer in euro, the Bank shall debit the payer's account with the amount of the transfer and execute it immediately, within the statutory time in seconds, subject to the availability of the payment service providers.

2/ Paper-based payment orders shall be processed according paragraph 12 above; 3/ Orders with a future execution date (up to 5 (five) business days from their deposit) are executed with the value date specified on the execution date.

15. Timeframe for executing payment transactions in a different currency. The terms stated in point 14 above apply, unless otherwise agreed between the Parties. For payment transactions within the EU, the agreed terms must not exceed 4 business days following the receipt of the order. Transfers through remote banking applications: a/ for a standard credit transfer (SWIFT), the payer's account is debited on the day of receiving the order and the transfer is executed with a value date of 1 business day at the latest; b/ for an express credit transfer (SWIFT), the originator's account is debited on the day of receiving the order and the transfer is executed with a value date of the same business day.

16. Instant payments in the national currency

(1) The Bank accepts and executes orders for instant payments in the national currency: 'BLINK' for transfers to banks participating in the BISERA payment system, and SEPA instant credit transfers in euro to banks located within the territory of the European Economic Area, participating in the SCT Inst scheme of the European Payments Council (EPC) (hereinafter jointly referred to as 'Instant Payment(s)'). The Bank processes orders for instant payments in compliance with the Rules of BORICA AD and the National Card and Payment Scheme (NCPS) for instant payments, the Rules of the SCT Inst scheme of the EPC for cross-border instant payments, as well as under the terms and conditions described below.

(2) An Instant Payment is a credit transfer in the national currency up to the maximum amount specified in the Bank's Tariff, ordered from a current or savings account in national or another currency of the Client, which is executed 24 hours a day, 365 days a year, with immediate or near-immediate processing, provided that the payee's account and PSP are available for instant payments. Instant Payments are not applicable to standing orders or bulk transfers, as well as to transfers to and from the state budget. The Bank does not execute Instant Payments with a specified future execution date.

(3) The time for execution of an instant payment order starts after the Bank has verified it (performed authentication of the payer, authorization and check for availability of funds, availability check for the beneficiary's PSP), has established that it complies with the terms and conditions for execution of instant payments and has blocked the payer's account for the transferred amount and the fees due. The

bank notes the start of the term for execution by time-stamping the order.

(4) The Bank accepts incoming instant payments and credits them to the payee's current/savings account or to an account servicing loans/credit cards, in the national or another currency, provided that such account is available for receiving an instant transfer, except for the cases under item (11) of this Article. In the event of non-compliance with the requirements set out in the previous sentence, the Bank shall refuse the execution of the transfer to the payer's institution with the relevant justification of the refusal. An incoming instant payment is processed with a value date coinciding with the calendar date of its reception.

(5) The bank accepts instant payment orders in euro for execution, made at the Bank's branch (BLINK and SEPA) or through the remote banking applications (BLINK) with a transfer amount less than or equal to the instant payment limit and the restrictions applicable to this type of payment specified in the Bank's List of Terms and Conditions.

(6) An instant payment order is processed with a value date coinciding with the calendar date of its reception. When executing an order for immediate payment, the Bank blocks the transfer amount and the fees due on the payer's account. Upon receipt of confirmation from the payee's institution that the transfer can be credited to the payee's account, the Bank shall lift the block and debit the payer's account. The Bank shall notify the payer of the successful execution of the transfer by changing its status in the remote banking application and by notification in the BACB Mobile application. Where the transfer is in euro and has been ordered at a Bank branch, the accounting entry in the payer's account shall be deemed notification to the Client of a successfully executed transfer.

(7) In the event of unsuccessful execution of an instant payment order, the Bank shall receive a refusal from the payee's institution to process the transfer, lift the block on the payer's account, and inform the payer that the order cannot be processed, stating the relevant reason for refusal, by changing the status of the transfer in the remote banking application and by notification in the BACB Mobile application. Where the transfer is in euro and has been ordered at a Bank branch, the absence of an accounting entry in the payer's account shall be deemed notification to the Client of an unsuccessfully executed transfer.

(8) The bank, in its capacity as the payer's institution, may initiate a Request for the return of an instant payment on its own behalf or on behalf of the payer, upon complying with the Rules for contesting instant payments through a NCPS account and the rules of the SCT Inst Scheme of EPC.

(9) The Bank is not responsible for unfulfilled instant payment orders due to unavailability of the payee's payment service provider in the instant payments system, unavailability of the payee's account or unsuccessful processing by other participants in the payment process.

(10) The Bank reserves the right to introduce additional limits to instant payments, which will be published in the List of Terms and Conditions and enter into force from the date of its application.

(11) In case of any suspicions regarding the security of the payment instrument or unauthorized use of the payment instrument, or in case of suspicion of fraud, money laundering, terrorist financing or obligation of the Bank to apply sanctions regimes, targeted financial and other sanctions and/ or restrictive regimes, as well as in case of other suspicions, including any established significant deviation from the Client's typical behavior and in the case of an established high risk of money laundering/ terrorist financing, the Bank reserves the right to designate a Client's current or savings account as unavailable for sending/receiving instant payment orders.

II.2. FEES, COMMISSIONS, INTEREST RATES AND EXCHANGE RATES

17. Fees and commissions. The Bank shall collect from the Customer fees and commissions for the payment services provided and the payment transactions executed in compliance with the Bank's Tariff. The Bank and the Customer may negotiate other fees and commissions. The Bank shall reserve the right to change its Tariff at

any time, and the changes shall become effective for the Customers - Users in accordance with the provisions of Section VII below.

In the case of payment transactions in euro or in the currency of a member state, when the payment service provider of both the payer and the recipient, or the sole payment service provider, is located within the EU, each party bears the fees charged by their respective payment service provider.

18. Interest rates. On the payment accounts opened, the Bank shall apply the interest rates set out in the Bank's Interest Bulletin. The parties may also negotiate other interest rates. The Bank shall reserve the right to change the Interest Bulletin and the changes shall become effective for the Customers - Users in accordance with the provisions of Section VII below. When the changes in the interest rates are more favorable to the Customer - User, they shall apply without prior notice. The deposit accounts offered by the Bank shall solely serve for the purpose of saving money and accordingly the changes in the interest rates on them shall be applied without prior notice.

19. Exchange rate. When exchanging currency, the Bank shall apply the valid buying exchange rate and selling exchange rate at the time of the exchange accounting, announced on the Bank's counters and on the Bank's website, as well as in the remote banking applications. Within the day, these exchange rates may change, and the change shall be made public in a prominent place. The Bank and the Customer may negotiate other exchange rates. Upon the receipt of a transfer in a currency other than the currency of the account, the Bank shall ex-officio convert the amount received to the currency of the account at the exchange rate at the time of the conversion.

II.3. CORRESPONDENCE WITH THE CUSTOMER IN RELATION TO PAYMENT SERVICES AND PAYMENT INSTRUMENTS PROVIDED. ACCOUNT STATEMENT. NOTIFICATION OF EVENTS ON THE PAYMENT ACCOUNTS.

20. Account Statement and Customer Correspondence. (1) To reflect a payment transaction on a Customer's account, the Bank prepares an Account Statement and provides it to the Customer in a manner and frequency chosen by them, as follows: (1) through remote banking applications; or (2) by sending it to the Customer's specified email address (for legal entities and individuals with an active debit card); or (3) on paper at a counter in a Bank branch at chosen intervals or upon request. (2) When opening an account, the Customer declares and indicates in writing to the Bank their preferred method and frequency for receiving the Account Statement, as well as notifications, information, and any other correspondence (collectively referred to as "Customer Correspondence"). At any time, the Customer may change the chosen method and frequency of receiving it. The official language of the Customer Correspondence is Bulgarian.

21. For Customers who have remote banking applications registration, the Account Statement and Customer Correspondence shall be provided through the remote banking applications, with the Customer being able to request an additional method/frequency for receiving the Account Statement/Customer Correspondence.

22. Notification of Completed Payment Transaction. The Customer is considered notified by the Bank of a completed payment transaction, and of having received the Customer Correspondence, as follows: (a) if the chosen method of receipt is at a counter in a Bank branch at a specific interval - on the date the Customer Correspondence is filed in the Customer's dossier, with the Bank providing the Account Statement no later than the next business day following the date of its preparation, depending on the frequency chosen by the Customer; (b) if the chosen method of receipt is by email to a specified address - on the date the Bank sends the email message to the Customer's specified email address; (c) for Customers registered in remote banking applications - through the remote banking application, immediately after the accounting of the relevant transaction; (d) if the chosen method of receipt is "upon request" - from the moment the relevant transaction is accounted for; (e) in case of receiving notifications - from the moment an electronic notification for the latter has been received.

23. The Customer has the right to submit claims and objections related to payment transactions reflected in the Account Statement/ Customer Correspondence in writing within the deadlines specified in Section II.5. of these GTC.

24. The Customer is responsible for maintaining the validity of the email address they have provided for correspondence. In cases when there's a change in their email address which is not communicated to the Bank in advance, or if an invalid (false, non-existent, or incorrect) email address is provided, any electronic statements and documents will be deemed received upon their dispatch from the Bank's information system to the email address specified by the Customer.

25. The Bank issues a Statement of Fees, in accordance with Article 106 of the PSPSA, to Customer-users upon their request, available once per year.

26. **Notifications Regarding Payment Account Events.** (1) At the Customer's request, the Bank provides a service to notify and inform about events relating to payment accounts. This is done through text messages to a mobile phone and/or email messages. Events concerning the Customer's accounts include transactions, balances, due dates, expiration of subscriptions, or other events specified by the Customer linked to their payment accounts. (2) The conditions of this service are detailed in Section VI of these GTC.

27. **Updating Correspondence Address.** If a Customer alters their correspondence address, including email or mobile phone number, it is imperative that they promptly inform the Bank. Failure to do so means that any notifications and documents sent to the previously indicated addresses and mobile phone number are considered to have been validly received by the Customer. The Bank is absolved from any liability for damages resulting from the Customer's non-notification or delayed notification of such changes.

II.4. OBLIGATIONS ON USING PAYMENT INSTRUMENTS AND ACCESS TO CUSTOMERS' ACCOUNTS. BLOCKING.

28. Every Customer, Authorized Debit Card User, and Remote Banking Applications User (subsequently referred to as "Customer/ User/ Consumer") is bound by the obligations set out in this Section when performing payment operations at a Bank branch counter, via a payment instrument including debit card, or through remote banking applications. Blocking or termination of access in these instances is to be carried out within 2 hours following the receipt of the request.

29. **Obligations to ensure the security of payment instruments/ personalized security tools and access to the current accounts.** When using a payment instrument / personalized security tools provided by the Bank, as well as when accessing current accounts opened with the Bank, the Customer – User/ User shall be required to take all actions to ensure their safety, including:

(a) to use the payment instruments in compliance with the terms governing their issue and use;

(b) upon receiving the payment instrument, to take immediately all reasonable steps to ensure the inaccessibility of the personalized security devices (username, password, eTAN, mobile banking PIN, debit card PIN, additional debit card security code, dynamic and static password for additional authentication for Internet payments or B-Trust Mobile application, a mobile device on which a mobile wallet is installed, and or other similar measures), including not to record any information about these security tools on the payment instrument and not to store such information with it;

(c) to use only in person and not to disclose or make available to third parties the data of their personalized security tool and the devices on which they are stored or from which such data is generated;

(d) to inform the Bank immediately in the following cases: upon finding out of any loss, theft, misappropriation or unauthorized use of the payment instrument / personalized security tools / a mobile device on which a mobile wallet is installed terminal device for mobile banking;; execution of unauthorized payment transactions through a current account digitalized card and/or a payment instrument; disclosure / compromise of the secrecy of any personalized security tool (stated in item (b) above) of the Customer/ User/ Consumer and

the devices, where these are stored or from which these are generated; of any inaccurately executed payment operation.

30. The Customer / User / Consumer shall perform their information obligation for notification of the Bank in the following ways:

(a) for payment services made at a counter and through a remote banking applications (i) by a written notice submitted personally at a counter in an office within the working hours of the Bank, or (ii) electronically via remote banking applications with a notification signed with the appropriate personalized security means, which the Bank accepts and processes within its business hours.

(b) for debit cards, at the telephones of Borica AD: +359 2 8705149 or +359 2 9702600 - 24 hours a day.

31. In order to obtain information on the use of payment services and payment instruments for remote banking applications and the procedure for their blocking, the Customer / User shall contact the Bank on the contact telephones of the Bank announced on the Bank's website.

32. **Blocking of payment instruments and the access to current accounts.** The Bank shall be entitled to block the use of a payment instrument and the access to current accounts of the Customer / User/ for objective reasons related to: (a) the security of the payment instrument; (b) suspicion of unauthorized use of a payment instrument and/or a current account; (c) suspicion of the use of a payment instrument and/or a current account with the purpose of fraud; (d) for security reasons; in case of information about illegitimate transfers received; (e) in case of suspicion of performing an action with the use of a payment instrument and/ or current account related to money laundering or terrorist financing; (f) significant increase in the risk that the Customer may not be able to implement their obligations to make duly payments - for loan-related payment instruments; (g) notification by the Customer for events under Art. 29, point (d) herein above; (h) upon receipt of an explicit written request for blocking by the Customer / pursuant to art. 30 above at any time, and blocking/ access suspension in such case shall be carried out within 2 hours from receiving the request.

33. **In case of blocking of a payment instrument and the access to payment accounts at Bank's initiative,** if possible before blocking the payment instrument for remote banking applications and/ or the current account, or at the latest thereafter, the Bank shall inform the Customer / Consumer / User of the reasons for the blocking of the payment instrument, unless such disclosure is not permitted for security reasons or to comply with regulatory requirements.

34. The Bank shall unblock the payment instrument or replaces it with a new payment instrument after the reasons for blocking have been eliminated.

35. The Bank shall not be held liable for its failure to duly execute transactions ordered by the Customer / User if the Bank has blocked a payment instrument; and/ or access to a current account under the provisions of this section, including if the grounds for blocking stated in the request for blocking, later on prove to be false.

II.5. NOTIFICATION OF UNAUTHORIZED OR INACCURATELY EXECUTED PAYMENT TRANSACTIONS

36. (1) When a customer, user, or account holder learns of an unauthorized or inaccurately processed payment transaction that could give rise to a claim, they must inform the Bank without undue delay and within specific deadlines: (a) if they are an individual consumer as defined by the PSPSA, notification must be immediate and in any case no later than 13 months after the date their account was charged; (b) if they are not an individual consumer as per the PSPSA: (i) for transactions made at a service desk or with a debit card - by the end of the first business day after becoming aware of it, but no later than 14 days after their account was charged; (ii) for transactions conducted via a remote banking application - no later than the next business day after their account was charged.

(2) The customer is considered to be aware of the unauthorized or inaccurately executed payment transaction from the moment the Bank provides them with the relevant correspondence about the

transaction, according to the methods and procedures set out in Section II.3 above.

II.6. LIABILITY IN CASE OF UNAUTHORIZED PAYMENT TRANSACTIONS

37. In the event of an unauthorized payment transaction, the Bank shall reverse its amount to the Customer and, where applicable, reverse the current account in the state in which it was before the execution of the unauthorized payment transaction within the statutory time limits after being notified in writing by the Customer of an unauthorized payment transactions/ inaccurately performed payment transaction within the terms set out in art. 36 above, except where the Bank has reasonable suspicions of fraud and notifies the competent authorities thereof.

38. (1) For unauthorized payment transactions incurred by a Client who is a natural person (a consumer under the Payment Services and Payment Systems Act), stemming from the use of a lost, stolen, or unlawfully appropriated payment instrument, the Client as a natural person is liable for the losses from these unauthorized transactions, up to a maximum limit of 100 Bulgarian Leva.

(2) For Customers – legal entities and sole traders who are not Users within the meaning of the PSPSA, the provision of the preceding Article (1) shall not apply and the Bank shall not be liable for unauthorized payment transactions and the Customers shall bear fully the losses related to all unauthorized payment transactions resulting from the use of lost, stolen or misappropriated payment instrument, regardless of the size.

39. The Customer (including a customer – legal entity, consumer within the meaning of the PSPSA) shall bear all losses regardless of their amount when such losses are related to unauthorized payment transactions caused by fraud, intentionally or due to gross negligence or as a result of the failure to implement one or more of the Customer's obligations under these GTC, including but not limited to the obligations under Art. 29 above for the protection of the security of the payment instruments/ customized security means and means for access to the payment accounts.

40. When a Customer/ User notifies the Bank of the loss, theft, misappropriation or unauthorized use of a payment instrument/ personalized security tool immediately upon becoming aware thereof, the Customer/ User shall not suffer any property damage/ loss as a result of the unauthorized use of this payment instrument/ personalized security tool, except where he acts or has acted fraudulently.

41. In the event the Customer claims that they have not authorized the execution of a payment transaction or that the transaction has been inaccurately executed, the burden of proof and the obligation to prove that the payment transaction has not been authorized and/or executed accurately, as well as that the transaction has been affected by a technical fault or other defect in the service, shall lie completely with (a) the Customer who is not a natural person (User within the meaning of the PSPSA), and (b) by the Bank, where the Customer is a natural person (User within the meaning of the PSPSA).

42. The Bank shall not be held liable for any damages caused by the use of a payment instrument in case it has executed the instructions of the Customer/ User before being notified by the Customer of the destruction, loss, unlawful seizure, tampering or unlawful use of a payment instrument / personalized security tools, which has led to unlawful use of the respective payment instrument or access to a current account.

43. The Bank shall not be held liable for any instructions executed by it ordered by the Customer/ User whose rights and/or powers have been changed and the Bank has not been duly informed thereof, as well as in the cases where the Customer/ User has not complied with its obligations under these GTC.

II.7. RESPONSIBILITY OF THE BANK FOR THE EXECUTION OF PAYMENT TRANSACTIONS

44. The Bank shall transfer in full the amount of the payment transaction. No partial transfers on individual payment orders or direct debit requests /executed until 31.12.2025/ shall be allowed.

The Bank in its capacity of the beneficiary's bank is entitled, before crediting the account of the Customer, to deduct from the amount transferred the fees due, in which case the information provided to the Customer shall indicate the amount of the payment transaction separately from the amount of the fees withheld.

45. Unique Identifier (IBAN). Where a payment order has been executed in accordance with the unique identifier of the beneficiary specified therein, the order shall be deemed to have been accurately executed in respect of the beneficiary. The Bank shall not be liable for any failure or inaccurate execution of a payment transaction in the event of incorrectly specified / invalid unique identifier by the Customer. In this case, the Bank shall, within the scope of the due cares, take efforts to recover the amount of the payment transaction, including by providing the information required for the reversal of the funds under the general procedure. In the event of failure to execute a payment transaction due to an invalid unique identifier specified, the Customer's Bank in its capacity as an ordering party shall refund the amount to the Customer's current account at the latest on the following business day.

46. Non-execution, inaccurate execution or delayed execution of payment transactions for payments ordered by the Customer as the payer. When the Customer – payer has submitted a payment order, the Bank shall be held liable to the Customer for the correct execution of the payment transaction unless it proves to the Customer / the bank of the beneficiary that the latter has received the payment amount within the statutory time limit. In this case, the beneficiary's bank shall be liable to him for the exact execution of the payment transaction and immediately makes available to him the amount of the payment transaction and, where applicable, shall credit the beneficiary's current account with the corresponding amount. In the event of a failed or inaccurate payment transaction ordered by the Customer - payer, the Bank shall, upon request, take actions within the scope of the due cares to track the payment transaction and notify the Customer of the outcome.

47. In the event that, upon receipt of a transfer to a Client's account, the Bank establishes a discrepancy between the name of the account holder and the payee, the Bank may make an enquiry to the payer's bank or return the transfer.

48. Discharge from liability. The Bank shall not be held liable under this Section in cases of force majeure, exceptional and unforeseen circumstances beyond the control of the Bank, the consequences of which would inevitably occur in spite of the efforts made to prevent them, as well as in cases where the Bank acted in compliance with a statutory obligation under the European Community law or the Bulgarian law.

II.8. CORRECTING ERRORS

49. Where the Bank of the Customer - payer is liable to the Customer for an inaccurate payment transaction where the funds have been wrongly transferred to another account with a different unique identification number / IBAN/ from that specified by the Customer in the payment order), or the account of the beneficiary has been credited but with an amount other than that specified by the Customer in the payment order, or when the Bank has debited the Customer's account with an amount other than that specified by the payer in the payment order, or in case of a duplicate execution of an authorized payment transaction, the Bank shall be entitled to request from the beneficiary's bank to perform a corrective transfer ex officio from the account of the wrong recipient of the funds within 5 business days from the date on which the Bank has refunded the amount of the incorrectly executed payment transaction in the Customer's account but no later than one month after being notified by the Customer or in any other way of the incorrectly executed payment transaction.

50. The Bank of the Customer - beneficiary of the incorrectly executed or unauthorized payment transaction shall, within 5 business days of receipt of the request under the preceding Article, carry out a corrective transfer from the beneficiary's account to the account of the payer's bank.

51. In cases where, in accordance with the procedure and within the terms of this Section no corrective transfer has been executed ex officio, the relationship between the Bank and the Customer shall be settled according to the general procedure.

SECTION III. REMOTE BANKING

52. The Bank shall also provide payment services and the related payment instruments within the meaning of the PSPSA through remote banking applications.

53. These GTC shall regulate the relations in connection with the use of remote banking applications between the Bank, on one hand, and on the other – the Customers, and/or the persons authorized by the Customers to represent them before the Bank (referred to in these GTC as "Remote Banking Applications User").

III.1. REMOTE BANKING SERVICES.

54. (1) Through remote banking applications, The Bank shall provide the Customer with access to his funds in accounts with the Bank for the use of payment and other services, including: opening of payment accounts, making payments in the national currency and foreign currency in Bulgaria and abroad, buying and selling foreign currency, operations with deposit and other accounts, payment of utility bills, standing orders and orders with future value dates, submission of requests for the issuance of payment cards and other payment instruments, creating payment templates, sending instructions to the Bank with free-form text, electronic orders for the execution of payment operations with limits set out in the Tariff of BACB, etc., obtaining reference information on the status and movement of bank accounts with the Bank, obligations to the Bank, exchange rates, interest rates, etc., sending a request for closing bank accounts, creation of a personal calendar for forthcoming payments, reporting of problems with the use of remote banking applications and filing complaints related to services provided by the Bank, keeping track of the current status of orders, requests, complaints, etc. filed with the Bank; maintaining and providing access to the documents signed electronically by the Customer.

(2) To authorize or sign off on payment operations through remote banking applications, the Client/User must use the personalized security tools and authorization methods implemented by the Bank. The Bank may, at any time and at its own discretion: (a) modify and/or introduce new or additional personalized security means for verification of Customer's/ User's identification and/or for signing/ confirming by the Customer/ User and by the Bank of electronic documents and (b) to change the scope of the services offered through the remote banking applications, as well as to exclude the possibility of using them in respect of separate accounts of the Customer in the cases of service changes, regulatory changes, security considerations or other considerations at the discretion of the Bank.

III.2. ACTIVATING AND USING REMOTE BANKING APPLICATIONS. OPENING A CURRENT ACCOUNT ELECTRONICALLY. LIMITS. OBLIGATIONS OF THE CUSTOMER.

55. (1). Access to remote banking applications is provided: (a) following an explicit written request by the Customer ("Request"), submitted as per Article 56, para. 1 below, or in electronic form, signed with a Qualified Electronic Signature (QES) or another electronic method accepted by the Bank, for certain products and services. This is contingent upon a Framework Agreement for Remote Banking being established between the Bank and the Customer, or (b) via the self-registration service on the remote banking applications. This applies in cases where an individual Customer enters into a Framework Agreement for Remote Banking with the Bank and consents to these GTC. Here, the Customer may gain access to the Bank's remote banking applications by completing self-registration on the website for accessing the applications. The Bank is responsible for verifying and confirming the Customer's identity, creating, and providing a Framework Agreement for Remote Banking for signature in the web-based application. By doing so, the Bank is deemed to have consented to and electronically signed the Agreement in accordance with the Electronic Document and Electronic Trust Services Act. The

Customer signs the provided Framework Agreement for Remote Banking with an eTAN, received via SMS on the mobile number they are currently registered in the Bank. Successful self-registration allows the Customer to use the remote banking applications within the standard limits, set in the current Tariff of BACB, depending on the personalized security tool used by the customer.

For customers who have signed documents with a one-time Qualified Electronic Signature (QES) issued by a qualified provider of authentication services, according to Regulation (EC) 910/2014 on electronic identification and authentication services (eIDAS), the Bank provides the possibility of self-registration in remote banking applications, where the Client receives durable medium access to electronically signed documents.

The self-registration service in the remote banking applications is not available for authorized representatives, legal representatives of Customers who are legal entities or principals whose products at the Bank have been opened through a proxy.

(2) In the Request, the Customer/User must provide a valid and unique email address for receiving electronic communications and documents from the Bank, as well as a valid and unique mobile phone number. The Customer must affirm that these contact details are used solely and exclusively by themselves. An email address or mobile phone number already registered in the system for another user cannot be reused for the registration of a new Customer/User. Regardless of whether they are an authorized representative on multiple accounts, a Customer/User is limited to a single registration.

(3) Should there be any changes to the information provided in the Request, the Customer is obliged to inform the Bank. This notification has to be made in person by the Customer/User at a Bank branch, filling in a Request for the amendment of registration details in the remote banking applications. If there are changes to the email address or mobile phone number provided in the Request, without a written notification to the Bank, or if the information provided is incorrect or non-existent, any communication sent to this email and/or phone number is considered as duly received. A change of client data for a User in the remote banking applications shall apply to all Clients with whom that User is registered.

(4) If a Customer/User needs to re-register due to forgetting their username or other personalized details, this must be done in person by the Customer/User, following the process outlined in Section (1) above.

56. (1) The application for initial registration and access to remote banking applications must be submitted in person at a bank branch by the Customer/User or an authorized representative with an express notarized power of attorney.

(2) When submitting the application, the Customer may designate one or more Users to operate on his behalf and at his expense via the remote banking applications with his accounts at the Bank. In this case, the request must include their identification data and rights. The Users can be: (a) Users authorized to manage the Customer's accounts, with "active access" either unrestricted or limited to specific accounts and/or amounts per payment transaction, who are explicitly authorized by the Customer with a notarized power of attorney, deposited at the Bank's counters. (b) Users with "passive access" rights (observing account movements and transactions made by the Account holder) or "limited access" (observing account movements, transactions conducted by the Account holder, and able to create payment orders on behalf and at the expense of the Account holder, without the right to send them to the Bank for processing), which the Customer explicitly specifies and authorizes for representation before the Bank in the Request.

(3) The Bank registers the Customer/Users within 3 business days after: 1/ Receiving the Request and 2/ Concluding a Framework Agreement for remote banking between the Bank and the Customer in the manner provided in these GTC.

57. When using the self-registration service for access to remote banking applications, the Customer receives instructions by the Bank

to create a username, password and PIN for mobile banking or identification applications, applicable to the respective remote banking applications. For this purpose, the Bank sends to the mobile number, specified in the request, SMS notifications containing codes for access activation and to the email address specified in the request – profile activation code. The Bank shall not guarantee the delivery of the SMS with a unique code or eTAN to foreign mobile phone number (mobile phone numbers issued by foreign mobile operators). The User must submit in person a new mobile phone number issued by a Bulgarian operator by visiting an office of the Bank.

58. In order to get access to Mobile Banking Applications in addition to the registration under the preceding Article by the Customer, it shall be necessary for the Customer to have a device with the necessary technical capabilities and operating system to allow the installation and proper functioning of the specialized software application for Mobile Banking stipulated by the Bank on its website; to have installed this software application on that device and to have secured the connectivity of the device with the mobile network in a way that allows the Customer to use mobile phone services and mobile network data transmission services.

59. Upon gaining access to remote banking applications, the Customer/ User shall have access to all or some of their accounts and products opened with the Bank through the applications in accordance with the Customer's assigned access rights. Any newly opened account or product thereafter shall automatically become available to the users through all the remote banking applications in accordance with the Customer's access rights.

60. Limits in remote banking applications:

(1) In Remote Banking Applications Users may order payment transactions and sign other instructions up to the Customer's specified limits for transactions from the Customer's accounts within a calendar day, as specified in the Tariff.

(2) The Customer limits may be changed at any time at the discretion of the Bank for security reasons, and the change shall take effect 5 business days from the date of notification sent to the Customer through the Remote Banking applications.

(3) The account holder (natural person, legal representative of a legal entity, proxy of a natural person/ legal entity, holding a notarized power of attorney may request a change in the standard daily limits set by the Bank or a change to the limit of an individual User by submitting the necessary request form in a bank office. Changes to the standard daily limits for a single day may be requested once every month, and in such cases the Customer/ User shall send a signed instruction via the remote banking application, no changes to the limits shall be permitted at the security tool level.

(4) The Bank may refuse to change limits, in accordance with its internal security policies, in case of suspicions regarding the use of a payment instrument and/or payment account for the purpose of fraud, in case of suspicions for money laundering and/or for security reasons. In case of a refusal to change (increase) such limits, the Bank shall notify the Customer, without having to explain such refusal.

61. Obligations of the Customer.

(1) The Customer/User is obligated to: a/ Follow the Remote Banking Instructions (User Manual for the use of BACB AD's remote banking applications, Guide for installation, registration, and use of the BACB Signer application, Guide for self-registration of individuals in the BACB Online remote banking application, Guide for re-registration of individuals from BACB Plus to the new BACB Online remote banking application, Security tips for using online banking, etc.), available at all times on paper at the Bank's offices or on the Bank's website. b/ Not to use operating systems and browsers other than those published on the Bank's website for accessing the remote banking applications. Failure to meet this obligation is considered gross negligence on the part of the Customer/User and incurs their liability in accordance with the PSPSA. c/ The customer is obliged to change the official password received at the first access to the respective remote banking application.

(2) The following non-exhaustive cases shall represent a default, under the conditions of gross negligence, of the obligations of the customer/ user under Art. 75 PSPSA: 1/ when, due to Customer's/ User's failure to adhere the Remote banking applications Instructions, a third party acquired personalized security tools/credentials of the Customer/ User, used to sign electronic documents and order payment transactions; 2/ when the unauthorized payment transaction was performed from a computer/ device, where malicious software/virus is installed or the Customer has provided his authentication credentials for the activation of a phishing attack; 3/ when the unauthorized payment transaction was signed by eTAN, PIN, application on a device with built-in biometrical identification and conformation of electronic statements or another safety feature provided by the Bank for mobile banking; 4/ when the Customer/ User has failed to use the protected remote banking channels, detailed in the Remote Banking Instructions, and has used a "phishing address"; 5/ if the Customer/User has failed to notify the Bank in writing and in due time, of the change in the persons, authorized to dispose of Customer's accounts and this has caused the occurrence of preconditions for unauthorized transactions, involving Customer's accounts; 6/ other cases, different from those, detailed above, which may be classified as gross negligence in the implementation of legal obligations.

(3) The Customer/ User shall abide all obligations under these GTC, specifically those in this Section III, and shall be fully responsible for all actions performed by them or by third parties through the use of any devices and/or personalized security tools. In the cases where the Customer/User has granted access to any of the devices and/or personalized security tools specified herein to a third party, in the relationships with the Bank, any actions performed by these persons through the use of those devices and/or personalized security tools shall be deemed actions, authorized and performed by the Customer/ User and the latter shall be fully responsible for all the consequences of doing so.

62. In case of a forgotten password and/or username or loss/theft of mobile devices, as well as in case of unauthorized access to a username, password or mobile device for remote banking, the Customer may request in writing from the Bank to change the username and generate a new password. The change in the username shall be made based on a new written Request submitted at a Bank's office.

III.3. IDENTIFICATION. ACCESS RIGHTS. CONFIRMATION OF ELECTRONIC PAYMENTS STATEMENTS.

63. The identification of the Customer/ User when using remote banking applications and the confirmation of the electronic payment orders shall be made in one of the following ways:

(1) For web-based remote banking application: a/ for logging in - by entering a username and a password, selected by the User (second factor of user identification) or by using the Signer application; b/ for confirming electronic orders: using eTAN, received as an SMS on the mobile number, provided by the User or using the Signer application.

(2) for mobile remote banking applications: a/ for logging-in by entering the username and PIN created by the User, or by using the respective mobile device, property of the Customer/ User (second factor of user identification); b) for confirming electronic payment orders: using eTAN, an SMS received on the mobile phone number, provided by the User or by using the respective application on the mobile device, property of the Customer/ User.

64. Electronic entering of the eTAN, received as an SMS or using the "Signer" application on the mobile device, property of the Customer/ User when confirming electronic payment operations, shall have the value of a legally valid statement signed by a handwritten signature of the Customer/ User.

III.4. EXECUTION OF PAYMENT ORDERS.

65. (1) The Customer / User shall have access to the respective remote banking applications on a 24*7 basis. The Bank shall accept payment orders from the remote banking applications until the officially

announced closing hours for payment orders and after these hours the payment orders shall be considered as deposited with the Bank on the next business day and shall be processed in accordance with the working hours of the payment systems, to which the Bank has access and through which it provides payment services. For the status of any payment order deposited through remote banking applications, the Bank shall notify the customer through the appropriate remote banking applications.

(2) For the execution of transfers between Customer's own accounts within the Bank, transfers for repayment of obligations under credit cards issued by the Bank, as well as payment of utility bills ordered via the remote applications, no signing is required by the Customer/User with a security token. By ordering such a payment transaction via the remote banking applications, the Customer/User agrees that the payment transactions are signed with an electronic signature which is equivalent to a handwritten signature.

(3) For blocking/ unblocking of a debit / credit card, using the remote banking applications, no signing the order by the Customer/ User with security tools shall be required. By ordering the operation, using the remote banking applications, the Customer/ User agrees that it shall be signed by electronic signature, equivalent to a handwritten signature.

66. The data received by the Bank electronically shall have the force of valid and binding written statements signed by the Customer / User. The Customer/ User shall be deemed to be informed and agrees that the Bank may store in log files traffic data and the IP address of the Customer / User as well as any other information necessary to identify them and for reproduction of electronic statements/ documents sent by them to the Bank in connection with ordering payment and other transactions. The information and documents thus collected may be used by the Bank in the event of litigation and other statutory obligations of the Bank, as well as to be provided by the Bank to relevant authorities in case of suspicion of unauthorized use of the payment instrument and suspicions of money laundering, terrorist financing and/or transactions with funds of criminal origin.

67. A payment order or other instruction received by the Bank in the form of an electronic statement through one of the remote banking applications shall be deemed received upon its entry into the accounting system of the Bank servicing the remote banking applications. The content and timing of receipt of the electronic statement in the accounting system of the Bank shall be established through an operating journal kept by the Bank.

68. In cases where, according to the current legislation, the Customer/ User has to submit a written statement, additional information and/or documents for execution of a transaction ordered by an electronic payment order, the latter shall be required to provide to the Bank by e-mail or in other manner indicated by it, all necessary documents justifying the transaction.

69. In the event that an ordered payment or transaction cannot be executed or has been refused by the Bank, the Bank shall immediately notify the Customer/ User by telephone or in writing, by e-mail to the e-mail address or via one of the remote banking applications.

70. The Customer may cancel an electronically transmitted electronic order only in case that the transaction is not executed by the Bank (in the case of a payment order - the Customer's account is not debited). Cancellation occurs when the Customer/ User deposits at an office / branch of the Bank or sends an order to the Bank via the Remote banking applications with an explicit request for cancellation of the transaction signed by an authorized person.

71. Upon request, the Customer may receive from the Bank a certified copy of a payment document received and processed through a remote banking application.

III.5. NOTIFICATION OF UNAUTHORISED OR IMPROPERLY EXECUTED PAYMENT TRANSACTIONS. BLOCKING. LIABILITY. OBJECTIONS

72. (1) The procedures and deadlines for notifying of improper actions when using remote banking applications, for unauthorized or inaccurately executed payment transactions ordered via the remote

banking applications, blocking of remote banking as a payment instrument and/or a payment account operated through remote banking applications, and the liability of the Bank and the Customer/User, are set out in Section II of these GTC.

(2) The Bank blocks the Customer/User's access to the remote banking applications in the cases and in the manner described in Section II.4 above.

SECTION IV. CASH-FREE PAYMENTS FOR UTILITIES AND OTHER SERVICES

73. (1) The Bank provides a service for making cash-free payments for utilities and other service obligations to "Merchants" with whom EPAY AD and EASYPAY AD have a contractual agreement, as well as a subscription for their automatic payment.

(2) For the purposes of this Section (a) "Merchant" means a person providing utility services and other services, who is a party to a contract with ePay AD and EasyPay AD and accepts online payments through their systems in an online regime (b). "ePay.bg" is a payment system with online exchange of data related to payments for utility and other services. (c) ePay AD is the operator of the ePay.bg system. (d) EasyPay AD is a payment institution within the meaning of the PSPSA, licensed by BNB and providing payment services.

(3) The Bank receives information about the amounts due by the Customer for utilities and other services through the ePay.bg system. The Bank is not responsible for its authenticity and accuracy, including in case of inaccurate information submitted by the Merchant to ePay AD for the Customer's obligations. EPAY AD provides real-time information to the Bank about the amount of the Customer's obligation submitted by the respective Merchant.

(4) The payments for utility services ordered by the Customer shall be executed through the mediation of EasyPay AD, the amounts being credited to a special (protected) account of EasyPay AD opened with the Bank under a specific contract entered into by and between the Bank and EasyPay AD, subject to the provisions of Art. 23 (2) PSPSA. The Bank undertakes to credit the account of EasyPay AD with the amounts paid by the Customer, with a value date of the payment order of the Customer.

(5) From the moment when the account of EasyPay AD with the Bank is credited with funds of a Customer, the Bank shall not be responsible for the crediting of the accounts of the respective Merchant by EasyPay AD. The Bank is not a party in the contracts between ePay AD, EasyPay AD and the Merchants and is not liable to the Merchants for non-received payments.

(6) In case the Customer informs the Bank in writing that the Customer has duly made payment to the Merchant, but the Merchant does not verify it as paid, the Bank shall take immediate measures to clarify the case and notifies the Customer of the result of the investigation.

74. (1) The Bank shall provide the Customer with an option, through remote banking applications, to register Customer / other numbers for which the Customer wants to receive up-to-date information about the amounts due to Merchants, with whom ePay AD and EasyPay have concluded a contract, and subsequently the Customer may, at their own discretion, order payment of all or part of these obligations.

(2) The Bank shall keep a list of Merchants providing utility services and other services that can be monitored and paid.

75. Subscription for automatic payment of utility bill and other services.

(1) Under a Contract for Automatic Payment of Utility Bills and for Other Services concluded with the Bank, the Customer may order the Bank to automatically pay on his behalf and from the Customer's account the obligations for utility bills or other services payable to service providers designated by the Customer for specified Customer numbers.

(2) The Customer shall specify: (a) His current account/s from which the obligations for utility bills and other services shall be paid. (b) The Customer shall also specify the priority of debiting the respective accounts; (c) Service Providers, the obligations to which the Bank should pay automatically upon the receipt of the bills on behalf and

for the account of the Customer. The Customer shall also specify the priority of making payments by the respective Customer numbers and the Bank shall act accordingly when making payments within one business day; (d) Customer numbers the obligations of which are ordered by the Customer to be paid automatically by the Bank to the respective suppliers upon the receipt of the relevant bill; (e) The period of validity of the consent for automatic payment of the obligations of the respective Customer number to the respective service provider; (f) Instructions on whether to pay the entire amount due to the respective provider or to pay the obligation only if below the maximum amount of single payment is defined by the Customer; (g) Whether the Customer wants to receive notification by SMS or e-mail to a designated telephone / e-mail address and in what cases: Receipt of a bill for obligations to a specific supplier; unsuccessful attempt to pay the bill and/or successful payment of the bill.

(3) In case of automatic payment of a debt from an account in a currency other than the national one, the currency exchange shall be made at the buying exchange rate of the Bank for the day of the exchange.

Automatic payment of utility bills and other obligations shall be made as follows: Every business day the Bank receives information from ePay AD about the obligations of the Customers according to the Customer numbers designated by the Customers to the respective suppliers and the Bank proceeds as follows: 1/ If in the Customer has designated in the Contract that the entire amount due to the respective provider for the respective Customer number should be paid and the Customer has sufficient available cash in the account designated for automatic payment, the Bank shall debit the respective account of the Customer with the amount of the obligation and transfer the amount due in the account of EasyPay AD with the Bank. If the customer does not have sufficient available cash on any of the accounts designated for automatic payment, no payment shall be made. 2/ If the Customer has designated in the Contract that the Bank shall pay the obligation only if it is below a certain maximum amount and the obligation is below or equal to that maximum amount and the Customer has sufficient available cash to make the transfer, the Bank shall debit the respective Customer's account with the amount of the obligation and transfer the amount due to the account of EasyPay AD with the Bank. If the customer does not have sufficient available cash on any of the accounts designated for automatic payment, no payment shall be made; 3/ If the Customer has designated in the Contract that the Bank shall pay the obligation only if it is below a certain amount, but the obligation is greater than this amount, the Bank shall not make the payment.

(4) The Customer may request notifications from the Bank by SMS or e-mail at the phone or email address specified by the Customer in the following cases: a/ receipt of a bill for the obligation to a specific provider; b/ unsuccessful attempt to pay the bill; and/or c/ successful payment of the bill. The Bank shall charge each notification in accordance with the Tariff of the Bank and collect the total amount of the notification fees due from the Customer ex-officio at the end of the month. If within two months the Customer fails to provide sufficient available cash on one of the accounts designated for payment of the notification fees due, the Bank shall automatically terminate the notification of the Customer.

(5) When service providers enter an additional fee for the payment through EasyPay AD and information on its basis and amount is not provided by EasyPay to the Bank, the Bank shall refuse and shall not execute payment orders to these service providers if it cannot provide the Customer with the preliminary information on the type and amount of fees and commissions due by the Customer to the relevant service provider. In this case, the Bank shall terminate the subscription for automatic payment to this service provider and notify the Customer by e-mail to the address designated by the Customer upon the registration with the Bank within 14 business days of the change and the deactivation.

SECTION V. ISSUANCE AND USE OF INTERNATIONAL DEBIT CARDS

V.1. GENERAL PROVISIONS, DEFINITIONS AND INTERPRETATION.

76. (1) The provisions of this Section shall regulate the terms and conditions for issuance, use and service of international debit cards VISA CLASSIC DEBIT, VISA GOLD DEBIT, and VISA BUSINESS by the Bank (hereinafter referred to as "the Card" or "the Cards") as well as the relationship between the Bank and the Customer / Authorized User regarding their issuance, use and service.

(2) For the payment services provided by the Bank under the provisions of this Section, the Bank and the Customer shall sign a Contract-Request for the issuance of a bank card (Request – Agreement). In the event that the respective Contract-Request contains terms other than those in these GTC, then the conditions agreed in the Contract - Request shall prevail.

(3) The international cards are designed for transactions in Bulgaria and abroad, on VISA standards. The cards shall be used for carrying out transactions via terminal devices marked with the trademark of the relevant card VISA, and the Bank undertakes to execute the following transactions when instructed by the Authorized User: payment for goods and services and receiving cash at POS terminals; payment for goods and services, as well as transfer between accounts through virtual online POS terminals and online payment for goods and services through the online payment systems; cash withdrawal at ATMs; payment for services at terminal ATM devices; transfer between payment accounts, payment for services at ATMs in Bulgaria, if the respective card operators and the respective banks, operating the ATMs, have provided the necessary technical capabilities for that; card payment transactions initiated by or executed through the beneficiary; reference and other payment and non-payment transactions.

(4) The Bank may extend or limit the scope of the services that may be used through the Card; to change the conditions, incl. fees, interest rates, and commissions based on changes to the legislation in force, security considerations, or improvements in the particular service. The Bank shall notify the Customers of the new services and the special terms and conditions of their use by publishing them on the Bank's website and shall not be liable for any damages and lost profits as a result of limiting the scope of the services. In the event that, as a result of a change in the terms and conditions, the fees, interest rates, and commissions are higher, the Bank shall notify the Customer at least two months prior to the date of entry into force of the changes pursuant to these GTC.

(5) The Bank accepts to make payments to the account under which the card transactions are reported under the terms of overdraft only if this is expressly agreed between the parties in a separate Contract.

V.2. ISSUANCE OF PRIMARY AND ADDITIONAL CARDS.

77. At the request of a Customer-natural person, the Bank shall issue to the Customer's current account (including to the Payment account for general purposes) a Primary Card. At the request of the Customer-legal entity or sole proprietor, the Bank shall issue to the Customer's current account a business debit card VISA Business ("business debit card") in the name of the Authorized User: the natural person - legal representative of the Customer.

78. (1) Upon Customer's request, the Bank shall issue additional debit cards / business debit cards to the account in the name of Authorized Users of additional cards specified by the Customer in the Contract-Request. At the request of a Customer - natural person, the Bank shall issue up to 5 additional debit cards, regardless of the number of accounts opened in the name of the Customer and regardless of the debit card brand. By using additional cards / additional business debit cards, the Authorized Users of additional debit cards/ business debit cards may dispose of the funds available on the Customer's account and/or to the overdraft amount, if any, within the transaction limits for which the Customer shall expressly give his consent.

(2) The issuance and use of additional cards shall be at the sole risk and responsibility of the Customer. The Customer assumes responsibility for all actions performed with the additional card. All transactions made with it and the fees, principal amounts /in case of

authorized overdraft/ and interest rates charged, as well as other liabilities associated with transactions ordered by the Authorized User of an additional card, shall be valid and shall be for the account of the Customer.

79. (1) Each card issued by the Bank is personal and is issued to a natural person - Authorized User. (2) The Bank shall issue bank cards based on a power of attorney in the following cases: when depositing to the Bank a Contract-Request by a person duly authorized by the Customer by virtue of a notary certified power of attorney, in which case a bank payment card shall be issued to the Customer or to the authorized person, as specified in the power of attorney. The right to receive a payment card issued by an authorized person shall occur only if there is an explicit text for the above in the notarized power of attorney issued in favor of the proxy, in which case the Authorizing Customer shall bear the full responsibility and risk of misuse of the bank payment card by a third party, insofar as the Customer has explicitly authorized them to receive from the Bank a debit card and the PIN code to it.

(3). The Bank reserves the right to refuse the issuance of a card without giving any reasons.

80. (1) Each card shall be issued with a unique Personal Identification Number (PIN) - a type of personalized security tool that represents a combination of at least four digits and serves to identify the Authorized User in making payment and non-payment transactions in accordance with these GTC.

(2) The Bank shall transmit the card and the PIN thereto in person to the Authorized User within 10 days as from the conclusion of the Request – Contract as follows: (a) The card shall be transmitted to the Authorized User in one of the following manners: (i) via courier to the address specified by the Authorized User in the Contract-Request, or (ii) at an office of the Bank, as specified in the Contract-Request, (b). The PIN shall be passed to the Authorized User in one of the following manners: (i) in a sealed envelope sent by courier to the address specified by the Authorized User in the Contract-Request (for security reasons, the PIN is sent separately from the Card); (ii) in a sealed envelope at the Bank's office specified in advance in the Contract-Request; (iii) via SMS message to the telephone of the Authorized User set out in the Request-Agreement; (iv) via a web-based remote banking application, where possible.

(3) The Bank may transmit the card and the PIN to the Authorized User also in a manner other than the above-described meeting the requirements of security of the international VISA organization.

(4) The card is inactive at the time of its receipt by the Authorized User. The activation of the card takes place after the Customer makes a phone call to the telephones specified by the Bank - +359 2 8705149 or +359 2 9702600 – available 24 hours a day and after the identification of the Authorized User and the verification of the data stated by him in the Request – Contract (name, PIN, mother's maiden name (keyword) and other information), the card shall be activated. The Bank recommends to the Authorized User to change the PIN code at an ATM as soon as the Authorized User receives and activates the card. The PIN may be changed at any time by the Authorized User with a new one known only to him by an ATM (of the bank or of other bank) installed on the territory of the country.

(5) If the Authorized User has forgotten the PIN, at their request the Bank shall issue a new card with a new PIN and shall transmit to the Authorized User the new card and the new PIN.

(6) The Authorized User shall be required to affix his/her signature on the signature strip on the back of the card upon its receipt

(7) The card shall be the property of the Bank and the Authorized User is required to return it to the Bank upon the expiration of its validity or upon the termination of the Contract.

(8) The name of the Authorized User according to an identity document (and the name of the legal entity nor the sole proprietor for business debit cards) - in Latin characters, the card number and the expiry date are written on the face of the card. Upon change of name, the Customer / Authorized User is required to file a request for re-

issuance of the card.

(9) Change of the office servicing the account, to which a debit card of an authorized user has been issued, shall be made based on an express written request/ statement of the user;

81. (1) For conducting payment transactions with payment cards remotely, the Bank provides the Authorized User with access to a two-factor authentication model for internet bank card payments under the Terms and Conditions of BACB for using the "Additional Authentication for Internet Payments" service, available on the BACB website. This ensures compliance with the PSPSA's requirements for enhanced verification of the payer's identity.

(2) The Bank provides Authorized Users the opportunity for: 1/ registering for the "Additional Authentication for Internet Payments" service (Visa Secure); 2/ registering their bank card in the B-Trust Mobile application, through which a B-Token is activated for authorizing payment operations using mobile devices with biometric data. By activating the B-Token in the B-Trust Mobile application, all bank cards of the Authorized User are automatically registered for this method of confirming online card payment transactions. A dynamic password for Internet payments is generated for each payment at a merchant registered under the Visa Secure program and is sent free of charge via SMS to the phone number provided by the Authorized User; 3/ registering a debit card in the Mobile Wallet application, thereby digitizing it.

(3) The Bank shall be entitled to change the tools used for ensuring the security of the online payments in case of changes in the requirements and standards of International Card Organizations. The Bank shall notify all customers of the changes made by posting a notice on its website, through personalized messages to the cardholders or by other electronic means of providing information.

(4) In case of payment operations, using bank cards at a low value of up to BGN 5.00 (five) until 31.12.2025 / 2.50 EUR after 01.01.2026 or the equivalent amount in another currency, additional authentication may not be requested by the Customer/Authorized user. The bank may at any time change this amount, in order to ensure compliance with the security requirements of the payment instrument or any legal amendments and regulations of the International Card Organizations. Upon reaching five successive low-value payment operations with a bank card with no additional authentication, the Bank shall request from the Customer/Authorized user to use his/her chosen method of additional authentication.

V.3. PROVISION OF REMOTE CONSENT FOR CARD PAYMENT TRANSACTIONS INITIATED BY OR EXECUTED THROUGH THE BENEFICIARY.

82 (1) The Bank shall apply strong customer authentication at the time the Customer provides his/her consent to the following: the beneficiary of a payment transaction to perform on behalf of and for the account of the Customer (acting as the payer) payment transactions using a payment card in cases where the beneficiary is a merchant registered for the Visa Secure program in compliance with the standards of the international card organizations.

(2) The consent shall be given through an initial transaction, verified by strong customer authentication of the Customer through the additional authentication model and initiated by the Customer. Through this transaction, the Customer agrees to the beneficiary of the payment transaction on the basis of the requirements / policies of the merchant or its servicing bank, respectively, for subsequent transactions to be initiated by the merchant acting as the beneficiary.

(3) The subsequent transactions effected with a payment card at the initiative of or through the beneficiary shall be carried out without applying strong customer authentication of the Customer as the beneficiary. Such transactions may have the nature of future or periodic subscription payments, payment of insurance premiums, payment of utility bills, payment for media services, etc., for which the Customer has given prior consent to be executed using a payment card at the initiative of or through the beneficiary.

(4) In cases where the beneficiary of a payment transaction executed

using a payment card at the initiative of or through the beneficiary is not registered for the Visa Secure program for an additional level of security, the strong customer authentication of the Customer shall be carried out by the respective merchant, acting as the beneficiary, rather than the Bank - issuer of the payment instrument.

(5) The Bank shall not be liable for unauthorized payment card transactions executed at the initiative of or through the beneficiary, where the Customer has given his/her consent, without applying the Bank's procedures for strong customer authentication. In this case, the responsibility for the authorized transactions shall be borne by the respective merchant as the beneficiary and the merchant's payment service provider, who shall prove whether the payment transaction made with a payment card at the initiative of or through the beneficiary is authorized by the Customer or not.

(6) The Customer, as a payer, shall be entitled to request the Bank to reverse the entire amount of a card payment transaction already executed and authorized, provided that it has been ordered at the initiative of or through the beneficiary and the following conditions have been simultaneously met:

(a) At the time of the authorization for execution of the payment transaction, its exact value was not indicated, and

(b) The value of the payment transaction exceeds the value expected for the Customer as a payer, in view of his previous costs for similar transactions.

(7) The request for reversal shall be made by the Customer to the Bank within 56 days from the date on which the account was debited. Upon request of the Bank, the Customer shall provide evidence of the existence of the conditions under para. (6) above.

(8) Within 10 business days of the receipt of the request, the Bank shall reverse to the Customer the full amount of the payment transaction or refuse to recover it, stating the reasons for the refusal and the authorities to which the payer may make an appeal if it does not accept the reasons for the refusal set out. This period may be extended in the event of an international dispute regarding payment card transactions in compliance with the rules and policies of the international card organization VISA

(9) For the purposes of para (6) above, the Customer may not refer to reasons for currency exchange operations where the reference exchange rate agreed with the Bank has been applied.

(10) The Customer shall not be entitled to reversal under para 6 above, when he/she has given his/her consent to the execution of the payment transaction directly to the Bank or where the beneficiary has provided or made available to the Customer, in his/her capacity as a payer, information about the forthcoming payment transaction, as agreed, at least 28 days before the date of the execution of the payment transaction with a payment card initiated by or executed through the beneficiary.

V.4. REQUEST FOR A MINIMUM NON-REDUCIBLE BALANCE. EX OFFICIO CLOSURE AND DEACTIVATION.

83. The Customer shall maintain on the account to which the debit payment card has been issued (hereinafter "account") a minimum non-reducible balance specified in the Tariff of the Bank.

84. The Bank shall be entitled ex officio to close the Account, to which a debit payment card has been issued, if the card has not been received by the Authorized User and no transactions have been made on the account for a period of three months and there are no funds in the account. Where an issued card has not been activated within three months of its production, the Bank shall be entitled to deactivate it ex officio without further re-issue or re-activation.

V.5. TERMS OF USE. OBLIGATIONS OF THE AUTHORIZED USER

85. (1) The card shall be used only in person by the Authorized User in accordance with the terms and conditions for its issuance and use in compliance with the security measures under these GTC.

(2) The customer is not allowed to lend, transfer or make the card available to third parties in any other way. The card number shown on its front side as well as the additional security code (CVC2/CVV2), depicted on the back of the card shall not be communicated to third

parties.

86. By using the card by the Authorized User at a terminal device (ATM and POS) by inserting / sliding / approaching in/through the device (contact and/or contactless transactions) and in cases where the terminal requires it - by entering the PIN and/or by affixing a signature on the transaction document and by presenting an identity document upon request by the merchant when using the card at a POS at the merchant, the Authorized User shall be identified and authenticate the respective transaction, agrees and instructs the Bank to execute it, which unconditionally binds the Authorized User with the consequences, and the Bank shall not be liable for any damages or lost profits resulting from its execution.

87. The Customer / Authorized User undertakes:

(1) to take all reasonable steps to preserve the personalized security tools of the card/ mobile wallet such as: (a) to keep the card responsibly with the due care by taking all necessary measures against its damage, destruction, loss, tampering, stealing, misappropriation or use in any other illegal manner other than the conditions for its issuance; (b) to keep in secret the PIN, the additional security code (CVC2/CVV2) and the Dynamic and Static Password for two-factor authentication for payments by bank card online or the B-Trust Mobile application and take all necessary measures against third parties' knowledge of it. The Authorized User shall be required not to keep the PIN in a way that makes it possible to be known by third parties, including not to write it on the card or on any item carried together with the card. The PIN selected by the Authorized User should not consist of an easily identifiable combination (such as telephone number, date of birth, vehicle registration number, etc.). The Authorized User shall be required to use the PIN (Dynamic and Static Password for Payments online or the B-Trust Mobile application) only after making sure that they cannot be seen/acquired by third parties in order to prevent possible malicious actions (frauds) by third parties;

(2) to protect the card from bending, breaking, demagnetizing and other mechanical damage;

(3) to provide funds for repayment of the liabilities under the account, including through the overdraft provided, if any;

(4) to promptly notify the Bank to one of the following telephone numbers in Borica AD: +359 2 8705149 or +359 2 9702600 - 24 hours per day in case of: (a) destruction, damage, retention, loss, theft, other misrepresentation, tampering or use in any other unauthorized manner of the card, as well as any suspicion that a third party has or could have known the PIN; (b) carrying out a transaction with the card not authorized by the Authorized User; (c) in all other cases provided for in these GTC;

(5) The Customer/ Authorized User shall also have all other obligations under these GTC, including those under Section II.4 and Section II.5 of the GTC herein.

V.6. PAYMENTS AND CASH WITHDRAWALS

88. The card entitles the Authorized User to make non-cash payments of goods and services at home and abroad, by contact or contactless, as well as with a mobile device via a digitalized card on-line or in off-line mode, at traders via terminal devices marked with the sign of the respective card.

89. When using the card or via a mobile device with a digitized card for payment of goods and services on a terminal device, the Authorized User shall be required, prior to confirming the transaction, to make sure that the payment amount is correct and then enter the PIN/ mobile device password when required and/or to sign the document of the performed transaction (receipt, voucher, other) presented to the User by the person receiving the payment. The signature on the document for the performed transaction should correspond to the signature placed on the back of the card. By using the card at a terminal device, by entering the PIN of the card, respectively by signing the document for the performed transaction, the Authorized User certifies the amount of the payment and orders the Bank to debit the account with the amount of the payment and transfer it to the account of the beneficiary, including in case of

contactless transactions. The person accepting the payment order shall be entitled to verify the identity of the Authorized User by requiring the presentation of an identity document.

90. When paying for goods or services ordered by telephone, fax, Internet, etc. the Authorized User typically executes the transaction by communicating / entering the holder's name, card number and expiration date, including CVC2 / CVV2 - the last three digits of the code printed on the paper strip on the back of the card in Italics, as well as other information in accordance with the rules of the card organizations, where necessary. By entering the required data, the Authorized User is identified, confirms the amount of the payment and orders the Bank to debit the account with the amount of the payment and transfer it to the account of the beneficiary.

91. In the process of Internet payment by card on websites marked as safe (according to the standards of VISA - Visa Secure), in addition to the card details, the Authorized Holder shall also enter the components of the two-factor authentication for Internet payments - dynamic and static password, or the B-Trust Mobile application or use another security tool provided by the Bank, with the aim to perform secure payments on the Internet and minimize the risk of abuse in this type of payments.

92. The person accepting payment by cards at a POS (Merchant) through which the payment is made may refuse to use the card in the case of: (a) invalidity of the card; (b) non-compliance of the signature on the card with the signature on the transaction document or identity document or absence of signature on the card; (c) refusal of the card holder representing himself for Authorized User, to produce a document confirming his identity, or where the Trader finds that an unauthorized person is using the card; (d) inability to obtain confirmation of the transaction; (e) suspicion of a false or forged card.

93. The persons accepting card payments shall be entitled to request the authorization of the card payment by blocking funds from the availability on the Customer's account.

94. The card may be used to withdraw cash in one of the following methods: (a) at an ATM (ATM terminal); (b) at POS terminals (cash advance) of the authorized banks at home and abroad, for cards bearing the VISA trademarks; or (c) (cash back) at retail establishments in the country providing this service, after authorization of terminal devices on the territory of the country marked with the VISA trademarks.

95. (1) The Bank provides an automatically activated Visa Click to Pay service when making a card payment online at websites marked as offering Click to Pay as a payment option. When making an online payment with Click to Pay, the Authorised User does not enter the card details – card number, expiry date or CVC – but instead the e-mail address or telephone number with which they are registered with the Bank. The Click to Pay service does not alter the requirement for mandatory entry of the components of two-factor authentication for online payments – dynamic and static password, or the B-Trust Mobile application, or another security tool provided by the Bank – for the purpose of carrying out secure online payments and minimising the risk of misuse with this type of payments. The procedure, method and process for amending the e-mail address and telephone number used, as well as management of the service, are set out on the Bank's website in the 'Cards' section and in the BACB Terms and Conditions for the use of the Visa Click to Pay service.

(2) The Bank provides all cardholders with the opportunity to use the Visa+ service for receiving money transfers to a card by means of the Authorised User's mobile phone number. In order to use the service, the Authorised Holder must designate one bank card to which money transfers may be received via their phone number. The procedure, method and process for registration and management of the service are set out on the Bank's website in the 'Cards' section and in the BACB Terms and Conditions for the use of the Visa+ service.

96. For any cash withdrawal from an ATM on the territory of the country the Authorized User may order issuance of a receipt by activating the respective service.

97. The Bank shall execute the transactions ordered through the Card by debiting the Customer's account with the amounts in accordance with the order of their receipt at the Bank.

The debit of the account takes place up to 3 business days after a transaction in the Republic of Bulgaria and up to 10 calendar days after a transaction abroad. Exceptions, where the account may also be debited for another, longer period, may arise depending on the time of receipt of the payment request by the bank servicing the person receiving the payment. The transaction shall be registered for the account with a Value Date being the date on which the payment has been ordered by the Authorized User.

98. When making a payment in a currency other than the currency of the Account, the Bank shall carry out conversion of the amount using the exchange rate of the Bank as at the time of debiting / crediting the account. For transactions abroad, the amount shall be converted into a settlement amount in the currency and at a VISA exchange rate, according to the Card type, after which the Bank shall convert the amount so received into the currency of the Account by applying the exchange rate of the Bank as at the time of debiting / crediting the account.

99. For each card transaction other than payment of goods and services at e Merchant, the Customer shall pay a fee in accordance with the Tariff, debited ex officio from the account by the Bank.

100. Limits. (1) The Authorized User may make cashless payments and withdraw cash using the card up to the limits set by the Bank for: one transaction, for 24 hours, for seven consecutive days, and for a maximum number of transactions for the relevant period (withdrawal/payment limits) as well as according to the amount of account balance and the authorized overdraft, if any.

(2) The Bank may unilaterally modify the limits set for the card, for which it shall promptly notify the Customer by announcing it at its bank offices or on its website or in any other appropriate manner.

(3) The limits set for the card may be changed at the request of the Customer and after approval by the Bank.

(4) The Bank executes the Customer's instructions for changing the parameters of the card is up to 5 business days.

101. Payment by a contactless international debit card. (1) The maximum amount that does not require a PIN shall be determined for each country by the International Card Organizations. For security reasons, it is possible to require a PIN for contactless payments below the amount set for the relevant country.

(2) Any ordered contactless payment using the Card shall be considered authorized by the Customer and shall be executed by the Bank by debiting the Customer's Account with the ordered amount and transferring it to the account of the beneficiary, even in case of insufficient cash on the Account. In case of insufficient cash in the accounting processing of contactless payment, an unauthorized overdraft is formed on the Account.

(3) The amount of the Customer's liabilities on the account shall be established on the basis of the entries in the Bank's books of account. The entries of all transactions performed with the card are accounting documents within the meaning of the Accountancy Act and shall be considered to be true until proven otherwise. The records of orders for execution of transactions kept by the Bank and other information shall be accepted as final evidence of their content as well as of the time when they are filed or executed.

V.7. OVERDUE PAYMENTS WHEN THE ACCOUNT BALANCE IS EXCEEDED

102. The Customer and the Authorized User shall be entitled to make payments using the Card up to the amount available on the Account (available balance or the authorized overdraft, respectively, if any). Upon exceeding the availability of the account due to offline transactions or for any other reason, the Bank shall open ex officio a loan account of the Customer that shall be treated as an unauthorized overdraft and shall accrue interest at an interest rate for the respective currency according to the Tariff. The Customer must immediately repay the amount that exceeded the account balance.

103. In the event that the customer fails to implement any of its

obligations under the issued debit card within the specified period of time, the Bank shall be entitled: 1/ to collect the outstanding amounts due as an unauthorized overdraft ex officio, without court intervention; 2/ to block all cards issued to the account. The cards shall be unblocked after the repayment of the overdue obligations. 3/ to deactivate the cards and to take immediate actions on enforced collection of the amounts due, including by court proceedings.

V.8. RESPONSIBILITIES, OBJECTIONS AND NOTIFICATION FOR UNAUTHORIZED PAYMENT OPERATIONS WITH THE CARD

104. The client shall be liable for all obligations arising from the issuance and use of all cards issued to his account.

105. The responsibility of the Bank and the Customer for any unauthorized or inaccurate transaction in connection with the use of a payment instrument-debit card is regulated by the provisions of Section II of these GTC.

106. The Bank shall not be responsible in any way for the transactions on which the Authorized User makes payments using the card. In case the Customer / Authorized User fails to implement its obligations to the Bank in connection with the use of the card, they may not make objections based on their relations with third parties.

107. The Bank shall not be liable for any unreasoned refusal of third parties to accept payments using the card or if a payment initiated by the Authorized User cannot be made with the card for technical, communication or other reasons beyond the control of the Bank. The bank cannot be held liable for refused transactions due to reasons beyond its control.

108. The use of an expired card subject to return to the Bank, of a blocked or forged card is forbidden and may serve as a basis for seeking civil and/or criminal liability in the court.

109. The Customer/ Authorized User shall be entitled to file written objections regarding the use of the Card issued by the Bank, and for duly established unauthorized or inaccurately executed payment transactions using a card in accordance with the procedure, under the terms for notification of the Bank set out in Section II of these GTC.

V.9. CARD VALIDITY

110. (1) The validity of a card is three years, detailed on the card itself and expires at the end of the specified month and year.

(2) When a card's validity period ends, the Bank automatically issues a new one. The Bank retains the right to decide not to renew any of the cards associated with the account without stating reasons thereof. The Authorized User can receive their new card, no sooner than 20 (twenty) days before the card's expiry, at an address they have provided or through another mutually agreed method.

(3) If a Client opts against having a new card issued, they must inform the Bank in writing at least 40 (forty) days before the existing card's validity period is due to expire.

V.10. BLOCKING, DEACTIVATION OF THE CARD

111. The Bank shall be entitled to block the Card in the following cases:

(1) at the request of the Customer and at the request of the Authorized User of an additional card only in respect of the additional card issued in his/her name. The Customer shall be entitled without the consent of the Authorized User of an additional card to block or deactivate that card. The additional card shall be automatically deactivated upon the termination of the contract with the Customer;

(2) in case of seizure of the Customer's account, in accordance with the procedure provided by the law;

(3) for objective reasons related to: (a) the security of the Card; (b) suspicion of unauthorized use of the Card; (c) suspicion of the use of the Card with the purpose of fraud; (d) for security reasons and upon information about received illegal payment transactions with the card; (e) in case of suspicions of carrying out actions involving the card, related to money laundering or terrorist financing;

(4) upon notification by the Client of events under Art. 29, letter (d) above;

(5) in the event of death or placement under guardianship of the Customer / Authorized User - as from the day on which the Bank became aware of this circumstance. In the event of death, the heirs

shall be required to submit to the Bank a death certificate, a certificate of heirs and other documents required by law, and shall be required to return to the Bank the Card in order to be destroyed;

(6) automatically, in three consecutive entries of wrong PIN or in repeated entries of wrong components of the two-factor authentication model for Internet payments by bank card;

(7) at a significantly increased risk that the Customer is unable to fulfil its obligation to the Bank under an overdraft on a current (card) account (if any) and / or in the event of exceeding the amount allowed (unauthorized overdraft);

(8) in the cases specified in the law or these GTC.

112. The Bank shall notify the Customer of the blocking of the Card and the reasons requiring such blocking, unless the disclosure of such information is not permitted for security reasons or regulatory compliance or compliance with obligations for implementation of regulations aimed at preventing money laundering/ terrorist financing.

113. The Card blocked under Art. 111, para.2, para 3 and para 7 above shall be deblocked ex officio by the Bank after the elimination of the reasons for its blocking, and for all other cases it shall be unblocked with the explicit written request of the Customer, deposited at a Bank's office or through the remote banking applications of the Bank and after the payment of a fee according to the Tariff.

114. (1) The Bank shall automatically deactivate the cards issued to the account upon termination of the Contractual relations with the Customer for issuance of a debit card, and in the case of a card blocked under Art. 111 (5) - after the Bank has received a written notification of the heirs, respectively the appointed guardians.

(2) The Bank may also deactivate an issued Card in other cases expressly specified in the law and these GTC.

(3) The Bank shall not be liable for damages caused as a result of deactivation of the Card under the terms and in the cases specified in these GTC.

(4) The Bank shall not be liable for damages if it has received a false notification that lead to blocking/ deactivation of the card, from a person who, on unambiguous circumstances, has been empowered to do so and the Bank in good faith has taken the necessary measures for protecting the Customer and has blocked the card.

115. Upon receiving a notification from the Customer regarding events under art. 29, letter (d) of these GTC, the Bank shall take all necessary measures to stop the use of the Card by blocking the Card for any transaction within the time required to process the notification.

116. In the event of a card being held by an ATM due to technical failure at the ATM or mechanical damage to the Card, the Customer / Authorized User shall be required to notify the Bank and the latter shall issue a new Card upon the receipt of a request for reissuance of the card.

117. (1) The terms and conditions for termination of the Request – Contract are set out in Section VII of these GTC.

(2) In any case of termination of the contract (a) the Bank shall be entitled to block all cards issued to the Account on the day of receiving, respectively sending of the notice of termination and to deactivate them at the expiration of the notification period; (b) The Customer shall be required to ensure that the Authorized Users return all the cards issued to the account; (c) The Customer shall be required to fully settle all of the Customer's obligations under the Account to the Bank and to implement all other obligations to the Bank, incl. all fees and charges due relating to the use of the Cards and the servicing of the Account prior to the expiration of the notice of termination; (d) All outstanding liabilities, incl. payments received after the date of termination of the Contract, payment transactions made with the Card(s) before that date shall be due by the Customer until their final repayment, and the Customer shall remain liable to the Bank after the termination of the Contract, regardless of the grounds for termination, whereby (e) the Bank shall be entitled to ex officio collection of the amounts due to it.

SECTION VI. MOBILE PHONE TEXT MESSAGES AND E-MAIL NOTIFICATION SERVICES

118. Notification via text message/SMS and/or email for specific events related to a payment account.

(1) Based on a Notification Agreement - Request, the Bank offers 24*7 notification services for certain events (account movements and balances, maturity dates, subscription expirations, and others) as stipulated in the request.

(2) The Client agrees that in delivering this service, the Bank may convey information possibly constituting banking secrecy to third-party operators or service providers under contractual agreement.

(3) Notifications are sent to the mobile number or email address designated by the Client.

(4) The Client pre-pays fees for the notifications according to the Bank's prevailing Tariff. If the Client has bought an SMS notification package and usage reaches 10% of its limit, the Bank informs the Client of the remaining SMS notifications in the package and the number of sent ones.

(5) This service can be terminated any time by the Client via a written application or unilaterally by the Bank if: (a) the Client's accounts are closed; (b) the Client fails to fulfill their obligations; or (c) the prepaid SMS notification package is exhausted.

(6) The Bank bears no responsibility if: (1) the service provider for sending text message/SMS or email does not ensure or delays the transmission of the notification; (2) the notification is not sent or received by the Client due to factors beyond the Bank's control (power failures, earthquakes, other disasters, and force majeure situations); (3) the tariff plan with the respective mobile operator doesn't allow for receiving SMS notifications abroad; (4) for third-party actions in using the notification, and for inaccuracies in the Client-provided email address, mobile phone number, and/or bank account number.

(7) The Client must inform the Bank of any changes in the provided email address, mobile phone number, and/or other details in the Request-Contract within seven days of such change. Otherwise, all notifications sent by the Bank to the last provided email address and/or phone number of the Client are considered as duly executed, and the Bank is absolved of responsibility for information disclosed.

119. Notification via text messages/SMS on a mobile phone for transactions conducted with a debit card (1) Upon request, the Bank provides 24*7 notification services via text message/SMS to a mobile phone for details regarding the card, transactions conducted, dynamic passwords for online payments, and changes to the GTC.

(2) The provisions in paragraphs (2), (6), and (7) of Article 118 are applicable in providing this service.

SECTION VII. AMENDMENTS TO THE GENERAL TERMS AND CONDITIONS. TERMINATION OF FRAMEWORK AGREEMENTS

120 (1) The Bank shall be entitled to amend and supplement these GTC. All such changes shall become effective as of the date stipulated in the decision of the Bank's competent body.

(2) In respect of Customers - natural persons (Users within the meaning of the PSPSA) who already have a Framework Agreements with the Bank for payment services and/ or other products/ services, for which these GTC apply, the Bank shall notify about the envisaged changes at least two months before the date of entry into force of the changes. The notification and the information about the envisaged changes shall be send via an email message or via text message/SMS send to the specified by the Customer for communication e-mail or mobile telephone number or via post to the specified by the Customer post address (in absence of provided e-mail and mobile telephone number). Information about the envisaged changes shall be provided on paper at the Bank's counters and in electronic form on the Bank's corporate website, in Bulgarian and English.

(3) The Customer-User shall be deemed to have accepted the changes in the GTC and shall be bound by them, unless he notifies the Bank in writing that they do not accept the changes in the GTC before the date on which they enter into force.

(4) In case the Customer-User notifies the Bank in writing about their disapproval of the changes of the GTC before their commencement

date, the Customer-User shall have the right to promptly terminate the Frame Agreement, without bearing any responsibility whatsoever for any expenses and compensations.

(5) The amendments to the GTC, which are connected with the expansion of the scope of services and/or a change of the payment instruments provided by the Bank and/or a change of the personalized security means used, as well as changes of the fees and/or conditions of the rendered payment services, which are more favorable for the Customers, shall be applicable without the need for a preliminary notice to the Customer.

(6) The amendments to the interest rates and currency exchange rates resulting from changes of the applicable reference exchange rates and interest rates for their determination, shall be immediately applicable and without the preliminary notification of the user. The Bank shall place at the user's disposal all respective changes through announcement of the applicable interest rates and currency exchange rates at its bank branches and on its website, or on any other permanent carrier, unless agreed otherwise by the Bank and the Customer as regards the term and way of making the information available.

121. Termination of the Framework Agreement for opening and servicing bank accounts and for the provision of payment services.

(1) The Framework Agreement for opening and servicing bank accounts and for the provision of payment services shall be terminated and the accounts opened under it shall be closed in the following cases:

(a) by mutual agreement of the Customer and the Bank;

(b) unilaterally by the Customer by one-month written notice, in the event that the Customer has no outstanding liabilities to the Bank at the expiry of the notice period;

(c) unilaterally by the bank with a written notice, as follows: (i) by means of a two-month written notice to the Customer-natural person, user within the meaning of the PSPSA, in printed form or in another durable form, submitted pursuant to the order of receiving the Customer Communications, specified by the Customer when opening the account or at Bank's desks or by registered mail, (ii) with a one-month written notification to a Customer, who is not a user within the PSPSA on paper on another long-term carrier, submitted pursuant to the order of receiving the Customer Communications, specified by the Customer when opening the account or at Bank's desks or by registered mail;

(d) unilaterally, ex-officio by the bank, in case of simultaneous occurrence of the following conditions: (i) for a period of more than 6 (six) consecutive months there is no payment transaction in the Customer's account, and (ii) the Customer has not paid the fees due for the monthly account maintenance and there is no balance under the account. Based on this procedure the Bank is also entitled to close current accounts with imposed distraint. For Customers - Holders of payment accounts with basic features, the term under item (i) shall be 24 /twenty-four/ months; In case of accumulated liabilities of the Customer on such account, the Bank may collect such liabilities ex-officio from another account of the Customer, with sufficient balance, as in case of different currencies, Bank's exchange rate on the date of deduction shall be applied;

(e) unilaterally by the Bank and the Customer, without an advance notice, in case of default by the other Party under these GTC and/ or the relevant Framework Agreement for payment services;

(f) unilaterally by the bank, in case of (i) suspicious transactions by a Customer relating to money laundering/ terrorist financing or establishing the execution of suspicious operations to the customer's account within the meaning of the Measures against Money Laundering Act, the Measures Against Terrorist Financing Act and the current legislation on the prevention of money laundering and terrorist financing; (ii) in case of suspicion of unauthorized use by a Customer of a payment instrument / current account or in case of doubt about the use of a payment instrument or a current account have been for the purposes of fraud; (iii) for security reasons; in the

case of information received by the Bank for the execution of illegal payment transactions. In such cases, the Bank may terminate the relations with the Customer without prior notice, and notify them in writing, unless the disclosure of such information is inconsistent with the applicable law. The Bank may terminate its relationship with clients, PABO holders, by giving them written notice within the time limits and for the reasons specified in the Payment Services and Payment Systems Act.

(2) If following the termination of a framework agreement there is a credit balance available in the Customer's account, then the Bank shall transfer it to its temporary, interest-free account until the disposal of the relevant amount.

122. Termination of a Request-Contract for Issuing a Debit Card. (1) A Request-Contract for the issuance of a debit card may be terminated at any time during its validity as follows: (a) in the cases described above in Article 121, para. 1, items (a), (b), and (c); (b) unilaterally by the Bank without notice in the event of non-fulfillment of an obligation and/or responsibility by the Client/Authorized Holder under the Request-Contract for issuing a debit card or the current GTC.

(2) Upon termination of the contract, regardless of the grounds thereof, all cards linked to the account, including additional ones, are deactivated.

123. The conditions for terminating framework contracts for other types of services are governed in the respective contract.

SECTION VIII. APPLICABLE LAW AND DISPUTE SETTLEMENT

124. As regards all issues not covered by these GTC or the Framework Agreement, or in other agreements between the customer and the Bank, the provisions of the following documents shall be applicable: the Payment Services and Payment Systems Act (PSPSA), Ordinance No.3 of the Bulgarian National Bank (BNB) on the terms and conditions and the procedure for opening of current accounts, for execution of payment transactions and for the use of payment instruments, the Credit Institutions Act (CIA), the Law on Electronic Document and Electronic Certification Services (EDECSA), the Remote Providing of Financial Services Act (RPFSA), the Measures Against Money Laundering Act (MAMLA), the Measures Against Terrorism Financing Act (MATFA), other applicable national and European legislation, the directions of the European Banking Authority, the rules of Visa with respect to the international debit cards issued by the Bank.

125. The Bank and the Customer shall take efforts and shall strive for the settlement of all disputes occurred between them by way of negotiation and by mutual agreement, out-of-court. In case of unauthorized payment transaction, inaccurate or incorrect execution of a payment transaction on behalf of the Bank, the Customer shall have the right to submit a written objection (complaint) to the Bank. Complaints/objections, regarding payment operations, made using payment cards, issued by the Bank, shall be submitted by the Account Holder/Authorized User in writing, in a form, required by the Bank, in one of Bank's offices or sent by the Account Holder / Authorized User electronically in the form of an electronic document, signed by means of a qualified electronic signature to Bank's email address: cards@bacb.bg, or using a remote banking channel, as electronic documents, signed using eTAN. A request for challenging payment orders and other payment operations, performed by a Customer in one of Bank's offices or through the remote banking applications shall be deposited by a customer – account holder/ proxy, in one of Bank's offices or sent by the customer as an electronic document, signed by a QES to the following email address of the Bank: Payments@bacb.bg or sent by the Customer, using remote banking applications, as an electronic document, signed by an eTAN. The Bank shall take a decision on and notify the Customer in writing about every complaint received, within a term of 14 days as of its submission, following the procedure stipulated in the BACB's Customers Complaint Management Policy available online on the Bank's website. As an exception, whenever the Bank cannot take a decision within the above term of 14 days as of submission of the written complaint due to reasons beyond the Bank's control, the Bank shall send to the

Customer a reply specifying the reasons for the respective delay, as well as the term, within which the Customer would receive a decision on the complaint logged by him/her. The time limit for making a decision may not exceed 35 business days from the receipt of the complaint.

If the Bank does not rule on the objection, as well as when no agreement is reached between the Bank and the Customer or when the decision of the Bank does not satisfy the Customer, the dispute shall be referred to the Payment Dispute Conciliation Commission set up at the Consumer Protection Commission at address: 1 Vrabcha Street, floor 3, 4 and 5, Sofia 1000, telephone: +359 2 9330577; E-mail: adr.payment@kzp.bg; internet page: www.kzp.bg и <http://abanksb.bg/pkps> or to the competent Bulgarian court.

126. The objections of the Customer/ Authorized User on payments made abroad (chargeback) with a debit card issued by the Bank shall also be considered according to the procedure determined by the respective card organization VISA Europe.

SECTION IX. PERSONAL DATA PROTECTION

127. (1). Personal data provided by the Customer to the Bank in connection with and upon conclusion of an agreement under these GTC shall be processed and kept by the Bank in compliance with Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(2) Detailed information about the data identifying BACB as a data controller and the contact information for contact with the DPO, the objectives and legal grounds for the processing of the personal data, including whenever such processing is necessary for the purpose of protection of the legitimate interest of BACB AD; the categories of recipients of personal data; the term of storage of the personal data; the rights of data subjects in connection with the processing of personal data by BACB AD, as well as information about the way of exercising the same; including any other information required to be provided to the Customer by the General Data Protection Regulation, contained in the Personal Data Protection Policy of BACB AD and in a Notice to Customers of "BACB" AD regarding the protection of personal data (Privacy Notice) available and announced on www.bacb.bg and at the offices of BACB.

SECTION X. BANK DEPOSIT GUARANTEE

128. (1) The payment of funds under deposits (accounts) at the Bank shall be under the guarantee of the Bulgarian Deposit Insurance Fund (BDIF) in compliance with the Bank Deposit Guarantee Act (BDGA). The BDIF shall guarantee the deposits in the Bank of Bulgarian and foreign natural persons and legal entities, in the national and in a foreign currency up to the amount and under the conditions specified in the BDGA and in the Bank's Information Bulletin available at the Bank's counters and on its website, Section "Documents/Other Documents", and shall be provided to the Customer before the opening of an account.

(2) The BDIF shall guarantee the payment in full of the amounts under a person's accounts with the Bank regardless of their number and size up to BGN 196 000 (one hundred and ninety-six thousand) until 31.12.2025 / up to EUR 100 000 (one hundred thousand) after 01.01.2026, as such amount shall also include the interests accrued as at the date of the BNB's decision for withdrawal of the issued license for bank activity of the Bank or another act specified in the following article hereunder. The following deposits shall be guaranteed up to an amount of BGN 250 000 (two hundred and fifty thousand) until 31.12.2025 / up to EUR 125 000 (one hundred and twenty-five thousand) after 01.01.2026 for a term of three months as of the moment, at which the respective amount is credited to the depositor's account or as of the moment, at which the depositor acquires the right to dispose of the deposit amount, as within the above term of 3 months the same are not part of the calculation of the total amount of the Bank's liability towards a depositor: (a)

deposits of natural persons resulting from deals with real estates for residential needs; (b) deposits of natural persons occurred as a result of amounts paid in connection with the conclusion or termination of a marriage, termination of employment/official relations, disability, death; (c) deposits occurred as a result of insurance/social security payments or of the payment of a compensation for damages due to crimes or due to a cancelled sentence.

(3) The BDIF shall pay the Bank's liabilities to the depositors up to the guaranteed amounts in the following cases: (a) when BNB has taken a decision for the withdrawal of a bank activity of the Bank; or (b) when BNB has taken a decision for the establishment of unavailable deposits and that at the Bank's discretion it seems incapable of paying the deposits and incapable of doing this for a short period of time; or (c) in case of an act ruled by a judicial body, which impedes the demands for depositors' receivables against the Bank.

SECTION XI. MISCELLANEOUS

§1. These GTC have been drawn up in Bulgarian language and adopted by the Management Board of the Bank. For convenience of the Customers, the Bank shall provide them, at their request, in English. In case of discrepancy or contradiction between the Bulgarian and the English versions, the Bulgarian text shall prevail and shall be deemed binding on the parties.

§ 2. The Bank shall publish on its website the updated version of the effective GTC. Throughout the term of validity of the Framework Agreement, the Customer may request, and the Bank shall provide the GTC on paper or another permanent carrier.

§3. These GTC have been originally adopted by a decision of the Management Board (MB) of BACB of 28 June 2018, effective as from 6 September 2018, amended by a decision of the MB of 4 July 2019, effective as from 29 July 2019 for legal entities and customers who are not users within the meaning of the PSPSA and as from 15 September 2019 for customer - users within the meaning of the PSPSA, as amended by Decision of the MB of 9 April 2020, and shall become effective as from 24 April 2020, amended by decision of the MB of 14 May 2020, effective as from 16 June 2020, amended by Decision of the MB of 21.10.2021, effective as form 15.11.2021, amended by Decision of the Management Board of BACB AD of May 26, 2022, effective from June 13, 2022, amended by Decision of the Management Board of BACB AD of 18.08.2022, effective from 01

September 2022, amended by Decision of the Management Board of BACB AD of 23.03.2023, effective from 01 April 2023, amended by Decision of the Management Board of BACB AD of 31.08.2023, effective from 01 September 2023 and amended by Decision of the Management Board of BACB AD of 19.10.2023, effective from 01.11.2023 for legal entities, sole traders and Customers who are not consumers within the meaning of the PSPSA and new Customers-consumers, from 01.01.2024 for current Customers – consumers within the meaning of PSPSA, amended by Decision of the Management Board of BACB AD of 16.05.2024 and 23.05.2024, effective from 28 May 2024; amended by Decision of the Management Board of BACB AD of 25.07.2024, effective from 01.08.2024; amended by Decision of the Management Board of BACB AD of 07.11.2024, effective from 11.11.2024 amended by Decision of the Management Board of BACB AD of 19.12.2024, effective from 01.01.2025, amended by Decision of the Management Board of BACB AD of 02.10.2025 and effective from 06.10.2025.

§4. These GTC shall also apply to and govern the relations with Customers who, prior to the effective date of these GTC, have executed Framework Agreements with the Bank for the provision of payment services and/or for using payment instruments, including framework agreements for the opening and maintaining bank accounts and the provision of payment services, for remote banking, automatic payment of utility bills and other services, for the issuance of debit cards and/or business debit cards.

§5. For the services and products governed by these GTC, the following provisions and conditions are also applicable and binding for the Client, and these documents are available on the Bank's website: 1/ Instructions for Remote Banking - A Guide to using BACB AD's remote banking applications, Guide for installing, registering, and using the BACB Signer application, Guide for self-registration of individuals in the BACB Online remote banking application, Guide for re-registration of individuals from BACB Plus to the new BACB Online remote banking application, Tips for secure online banking, technical requirements and others; 2/ BACB's Terms for using the "Additional Authentication for Internet Payments" service with a bank card; 3/ BACB Terms and Conditions for the use of the 'Visa Click to Pay' service with a bank card; 4 / BACB Terms and Conditions for the use of the 'Visa+' service with a bank card.

For the Bank:

For the Customer:

/signature and full name/