ANNEX 3

SPECIAL TERMS AND CONDITIONS FOR THE USE OF DEBIT CARDS FOR ENTREPRENEURS APPLICABLE TO LEGAL ENTITIES

1. GENERAL PROVISIONS

1.1. Scope of the Bank's General Terms and Conditions Annex

These Special Terms and Conditions for the Use of Debit Cards for Entrepreneurs and Legal Entities of AikBank A.D. (hereinafter: the Bank) govern the mutual rights and obligations of the Bank and payment service users – legal entities and entrepreneurs – in connection with the terms under which the Bank provides debit card issuance and usage services for entrepreneurs and legal entities. These Terms also contain information on fees, foreign exchange rates, means and methods of communication, as well as the terms for amendment, supplementation, and termination of the Framework Agreement, in accordance with the Law on Payment Services (hereinafter: the Law) and the Bank's internal acts applicable to entrepreneurs and legal entities.

These Special Terms and Conditions for the Use of Debit Cards for Entrepreneurs and Legal Entities, together with:

- the General Terms and Conditions of AikBank a.d. Beograd (hereinafter: GTC),
- the Special Terms and Conditions for Payment Accounts and Payment Services for Legal Entities and Entrepreneurs of AikBank a.d. Beograd (hereinafter: Special Terms),
- the Price List of the Bank's Services for Legal Entities and Entrepreneurs (hereinafter: Extract from the Price List);
- the Transactions Schedule for the Receipt and Execution of Payment Transactions for Legal Entities and Entrepreneurs, which forms an annex to these Special Terms (hereinafter: Transactions Schedule),
- and the Limits for the Use of Payment Instruments,

form the **Framework Agreement** (hereinafter: the Framework Agreement or the Agreement).

Terms used in this Annex to the General Terms and Conditions shall have the following meaning:

1. **Payment Service User (User)** – An entrepreneur or legal entity that uses or has used a payment service as a payer and/or payee or has approached the Bank for the purpose of using such services.
2. **Primary Debit Payment Card** – A payment card issued by the Bank to the User, linked to the User's payment account held with the Bank and used for initiating payment transactions.
3. **Additional Debit Card** – A payment card issued by the Bank at the request of the User to a person designated by the User and linked to the payment account of the primary cardholder.
4. **PIN** – Personal Identification Number known only to the User, used for transaction authorization, especially when using the debit card at ATMs and POS terminals.
5. **Current Account** – A payment account maintained by the Bank, used for executing payment transactions in local and foreign currencies (RSD/FX), as well as for other purposes in relation to services provided by the Bank under specific agreements.
6. **Payment Transaction** – A deposit, transfer, or withdrawal of funds initiated by the User as payer or payee, or on behalf of the payer, carried out regardless of the legal relationship between the payer and the payee.
7. **Remote Payment Transaction** – A payment transaction initiated via the internet or a device that can be used for remote communication.
8. **Payment Order** – An instruction given by the User, as payer or payee, to the Bank requesting the execution of a payment transaction.
9. **Instant Credit Transfer** – A domestic payment transaction of up to RSD 300,000, marked as urgent, initiated via a paper-based payment order or other payment instrument, at any time

of day, every day of the year, where funds are transferred in real or near-real time.

10. **Initiation of a Payment Transaction** – Actions that are a prerequisite for starting the execution of a payment transaction, including the issuance of a payment order and conducting authentication.

11. **Payment Instrument** – Any personalized device and/or set of procedures agreed between the User and the Bank, used by the User to issue payment orders or initiate payment transactions.

12. **Payment Instrument Based on a Payment Card –** Any payment instrument, including a card, computer, mobile phone, or any other technical device containing a payment application, enabling the payer to initiate a payment transaction using the card.

13. **Issuance of Payment Instruments** – A payment service in which the payment service provider issues a payment instrument to the payer under an agreement, for initiating and processing the payer's payment transactions with that provider.

14. **Payment Brand** – Any physical or digital name, label, mark, symbol, or combination thereof that identifies a card payment system under which a card-based payment transaction is executed.

15. **Co-branding of a Payment Instrument** – The inclusion of at least one payment brand and at least one non-payment brand on the same card-based payment instrument.

16. **Acceptance of Payment Transactions** – A payment service provided under an agreement between a payment service provider and a payee for accepting and processing payment transactions, involving the transfer of funds to the payee.

17. **Payment Initiation** – A service that involves issuing a payment order on behalf of the payer from an account held at another payment service provider, at the request of the payment service user.

18. **Account Information Service** – A service provided via the internet that enables consolidated information about one or more payment accounts held by a payment service user at another or multiple payment service providers.

19. **Account Servicing Payment Service Provider (ASPSP)** – A payment service provider that opens and maintains a payment account for the payer (i.e., the Bank).

20. **Payment Initiation Service Provider (PISP)** – A payment service provider that issues a payment order at the request of a payment service user on an account held at another provider.

21. **Account Information Service Provider (AISP)** – A payment service provider that provides online consolidated information on one or more payment accounts held by a user at another or multiple providers.

22. **Authentication** – The procedure allowing the payment service provider to verify the identity of a payment service user or the validity of use of a specific payment instrument, including the use of the user's personalized security credentials.

23. **Strong Customer Authentication** – Authentication using two or more elements categorized as knowledge (something the user knows), possession (something the user possesses), and inherence (something the user is), which are independent so that compromising one does not compromise the others, and which is designed to protect the confidentiality of the authentication data.

24. **Personalized Security Credentials** – Personalized data and features assigned by the payment service provider to the user for the purpose of authentication.

25. **Sensitive Payment Data** – Any data, including personalized security credentials, that may be used to execute fraudulent transactions. In the context of payment initiation and account information services, the account holder's name and account number are not considered sensitive.

26. **Payer** – A legal entity or entrepreneur who, from their payment account, issues a payment order or gives consent to execute a transaction initiated by a payee, or a private individual issuing the payment order if no account is held.

27. **Payee** – A private individual or legal entity designated as the recipient of the funds that are the subject of the payment transaction.

28. **Credit Transfer** – A payment service where the User, as the payer, initiates one or more payment transactions from their payment account with the Bank, including standing orders, resulting in the payee's account being credited with the transaction amount.

29. **POS Terminal** – A device installed at the merchant's point of sale or at the Bank's counter that enables card use and records payment transactions electronically (EFTPOS).

30. **ATM** – An electromechanical device allowing cardholders to deposit and/or withdraw cash and/or access other services (e.g., fund transfers, account balance inquiries).

31. **Funds** – Cash, account balances, and electronic money.

32. **Cash** – Banknotes and coins

33. **Business Day** means a day, or part of a day, on which the Bank operates in a manner that enables the execution of payment transactions for its User as a payment service user;

34. **Value Date** means the reference date or reference time used by the Bank for the calculation of interest on funds debited from or credited to the payment account;

35. **Reference Exchange Rate** means the rate used as the basis for calculating a currency conversion, which is made available by the Bank or originates from a publicly available source (e.g. the NBS middle exchange rate);

36. **Reference Interest Rate** means the rate used as a basis for calculating interest, which is publicly available and determined independently of the unilateral will of the User and the Bank (e.g. NBS reference rate, Euribor, Libor, etc.);

37. **Unique Identifier** means a combination of letters, numbers and/or symbols assigned by the Bank to the User, which is used in a payment transaction for the unequivocal identification of the User and/or the User's payment account (e.g. the current account number, credit card number, etc.);

38. **Durable Medium** means any instrument that enables the User to store information addressed personally to them, to access it and reproduce it in an unchanged form during a period that is adequate for the purposes of the information;

39. **Domestic Payment Transaction** means a payment transaction where both the payer's and payee's payment service providers provide their services within the territory of the Republic of Serbia;

40. **International Payment Transaction** means a payment transaction where one payment service provider operates in the Republic of Serbia and the other in a third country, or where the same payment service provider services one user in the Republic of Serbia and another in a third country. Transactions in dinars between residents and non-residents, as well as transactions between non-residents, are considered international payment transactions. For the purposes of these General Terms and Conditions, a domestic payment transaction executed in a foreign currency shall also be deemed an international payment transaction. The Bank does not execute international payment transactions in virtual currencies.

41. **Virtual Currency** means a type of digital asset that is not issued or guaranteed by a central bank or public authority, is not necessarily pegged to a legally established means of payment and does not have the legal status of money or currency, but is accepted by natural or legal persons as a means of exchange and can be bought, sold, exchanged, transferred, and stored electronically;

42. **Home Country** means the country in which the legal entity has its registered seat;

43. **Registered Seat** means the place registered as the seat of a legal entity, or if the legal entity has no registered seat according to the regulations of its country, the place from which its business is managed;

44. **Host Country** means any country other than the home country in which a legal entity provides services through a branch or another entity, or directly provides services;

45. **Lawful Residence in the Republic of Serbia** means residence of a natural person in the Republic of Serbia in accordance with the laws governing the residence and domicile of citizens or the residence of foreigners, including refugees and asylum seekers under applicable laws or international agreements;

46. **3D Secure Service** means a service provided by the Bank during online payments with a payment card at merchants participating in the Mastercard SecureCode and/or Verified by Visa programs, offering the cardholder additional protection from unauthorized use during online transactions;

47. **One-Time Password (OTP)** means a one-time numeric code created by the User during a purchase at a 3D Secure internet point of sale;

48. **Transaction Date** means the date on which the cardholder initiated or gave consent for the execution of the payment transaction;

49. **Value Date** means the date on which the Bank debits the User's debit card in connection with the execution of the payment transaction;

50. **Authorization** means the process by which a transaction made with a debit card is approved;

51. **Slip** means a receipt for a transaction executed with a payment card;

52. **Point of Sale (POS)** means a merchant location where payment cards are mandatorily accepted as a non-cash means of payment for the sale of goods and provision of services;

53. **Online Point of Sale** means a sales point where the presentation and sale of products and services, as well as all other actions related to the sales process, are carried out via electronic communication channels (internet, phone, email) without physical contact between the merchant and the User;

54. **Cash Disbursement Point** means a location where a business entity is authorized to accept payment cards for the service of disbursing cash via a POS terminal;

55. ; **Digital Wallet** means a mobile payment application solution offered by a digital wallet service provider, allowing the User to register within the app data related to one or more payment cards and thus tokenize the card(s) for the purpose of initiating payment transactions. In addition to the contractual relationship with the Bank, the terms and manner of using the digital wallet are agreed between the User and the service provider, particularly with regard to the type and characteristics of the mobile device on which the digital wallet application can

56. be contracted and installed. The User may refer to the Bank's website for information on which digital wallets support the addition of one or more debit cards issued by the Bank;

57. **Digitized Card** means the digital representation of a debit card in a Digital Wallet and/or in the Bank's electronic and mobile banking applications, allowing the User to perform contactless payment transactions at sales and cash withdrawal locations and ATMs that support wireless data transmission over short distances between two devices, and/or at online points of sale that support such payment methods. The Bank, as the card issuer, determines which card types can be digitized;

58. **Mobile Device** means the device on which the Digital Wallet is installed, as contracted by the User with the Digital Wallet service provider;

59. **Digital Wallet Service Provider (Service Provider)** means a legal entity that provides the Digital Wallet service in which the Bank, based on a cooperation agreement with the service provider, enables the User to register one or more debit cards issued by the Bank.

1.2. Debit Cards

1.2.1. Terms of Issuance and Card Types

The Bank issues a debit payment card to the User, which is linked to the User's payment account held with the Bank. The Bank issues the following types of debit cards: DinaCard, Visa, and Mastercard, under the conditions defined by the Agreement, General Terms and Conditions, and these Special Terms and Conditions.

The issued debit card may be used by the User to pay for goods and services and/or withdraw cash from ATMs and at bank counters displaying the corresponding card brand signs – Dina, Visa, or Mastercard – up to the available account balance, which may include an approved overdraft.

The Bank issues a card free of charge if processing, netting, and settlement of domestic payment transaction orders are carried out within the payment system of the Republic of Serbia. Additionally, at the User's specific request, the Bank may issue another debit card from its offering, where such processing is performed outside the Republic of Serbia.

The User's rights related to the use of co-badged payment instruments are governed in accordance with the provisions of the law regulating interbank fees and special business rules for payment transactions based on payment cards.

The validity of the debit card ranges from one (1) to ten (10) years. Issued debit cards remain the property of the Bank, are registered in the User's name, and are non-transferable. The Bank issues debit cards solely to Users who maintain a current account with the Bank.

Upon expiration, the Bank reserves the right to renew/reissue the debit card in accordance with its applicable procedures and internal acts.

A debit card may be issued to any adult natural person employed by the User as an End User, as specified in the Debit Card Issuance Request for Legal Entities and Entrepreneurs, submitted by the User's authorized representative. The User shall inform the end user of the rights and obligations stipulated in the Agreement, General Terms and Conditions, and these Special Terms and Conditions.

The debit card is issued in the name of the end user.

By signing the Debit Card Issuance Request, the User explicitly consents to the defined functionalities and authorizations related to the use of the debit card by selecting one of the options offered in accordance with the Bank's current offer.

The User has the right, throughout the validity of the Agreement, to amend the elements of the Debit Card Issuance Request by submitting a new request that revokes the previous one, thereby defining a different method of operation and authorization.

The debit card may be used at all points of sale and ATMs displaying the symbols of the card organizations – Dina, Visa, Mastercard – as well as for remote retail commerce enabled through card use.

The Bank charges the User for services rendered in accordance with the Bank's Price List for services (hereinafter referred to as the "Price List"). The Bank reserves the right to grant the User more favourable fees than those listed in the Price List.

The Bank may deliver the debit card and Personal Identification Number (PIN) to the User at a Bank branch or via mail to the User's address, provided technical conditions allow.

In case of delivery to the User's address, the Bank bears the delivery risk, except when the User has failed to provide the correct address or to timely notify the Bank of any changes.

The debit card remains the property of the Bank and may only be used by the User. Use by any third party is prohibited. The Bank is not liable for damages resulting from third-party use of the debit card.

The User is obliged to use the card in accordance with the law, solely for the purchase and payment of goods and services that are not prohibited by applicable regulations.

The debit card is valid until the last day of the month printed on the card.

The User shall be liable for all purchases and cash withdrawals made using the debit card, including any fees incurred from the use of additional card(s), as well as for any violation of the Agreement, General Terms and Conditions, and these Special Terms and Conditions.

The validity period of the debit card is automatically extended upon reissuance. Each reissued debit card constitutes an extension of the original validity period and shall be governed by the same Agreement, General Terms and Conditions, these Special Terms and Conditions, and the initially selected accompanying services, unless amended accordingly and communicated to the User.

If the User does not wish to extend the validity period of the debit card or accompanying services, they shall notify the Bank in writing (or in a manner that clearly identifies the User) no later than 60 (sixty) days before the card's expiration date. In such case, the card will not be renewed.

Failure to notify the Bank within the specified period obligates the User to cover the applicable costs in accordance with the Bank's Price List.

The User agrees that the Bank may, upon reissuance or earlier during use, replace the debit card with one bearing a different card brand. The Bank is obligated to inform the User in writing of its intention to change the card brand, the delivery method of the new card, and the period in which the previous card may still be used. If the User does not accept the new brand debit card, they may cancel the use of the card in writing, settle any obligations on the current account, and request account closure.

The card may be used at all POS terminals and ATMs domestically or internationally, unless otherwise stipulated by the Special Terms and Conditions or the Agreement between the Bank and the User.

For security reasons, the User must safeguard the debit card and handle it responsibly.

The User shall bear full legal liability for any unauthorized use of a debit card issued in their name. The Bank is not responsible for the quality of goods or services paid using the debit card and shall not be liable in the event of disputes related to quantity or quality. Any claims are to be addressed directly by the User at the point of sale, while obligations toward the Bank arising from the card use must be fulfilled regardless of disputes with merchants.

Domestic debit card transactions are calculated in dinars and charged to the User's dinar current account, while foreign transactions are also debited from the dinar account based on the dinar equivalent. Foreign currency transactions are converted into dinars at the Bank's selling exchange rate on the date of the transaction.

The debit card must not be used unlawfully, including for purchasing prohibited goods or services or contrary to this Agreement. Any use of the card for illegal purposes, such as for prostitution, drug trafficking, or purchasing pornography, is punishable. The debit card may not be used as collateral for debt settlement. Any unlawful use or use contrary to the Agreement results in the termination of card rights, confiscation of the card, and the User being held liable for all potential losses.

1.2.3. Obligations of the User

1.2.2. Obligations and Rights of the Bank

The Bank stores and uses data related to debit card operations in accordance with the law. By signing the request for the issuance of a debit card, the User consents to the Bank processing and storing the personal data provided in the request, either by automated means or manually.

The debit card is non-transferable and may be used only by the User or the designated End User. All debit cards can be used at all points of sale and ATMs within the country or abroad, unless otherwise stipulated by the Special Terms and Conditions or the Agreement between the Bank and the User.

For security purposes, the User is obliged to safeguard the debit card and handle it responsibly.

The User bears full legal responsibility for any unauthorized use of the debit card issued in their name. The Bank is not liable for the quality of goods and services paid for using the debit card and shall not be held responsible for any disputes regarding quantity or quality of goods. The User shall address any disputes directly with the merchant and is required to settle all obligations to the Bank arising from the use of the debit card, regardless of any ongoing dispute with the seller.

Domestic debit card transactions are calculated in RSD and charged to the User's RSD current account up to the available balance. For transactions made abroad, the User's RSD current account will be debited in the dinar equivalent. Foreign currency transactions resulting from the use of the debit card abroad are converted into RSD at the Bank's selling exchange rate on the date of the foreign currency debit.

The debit card must not be used for unlawful purposes, including the purchase of goods or services prohibited by law or contrary to the provisions of this Agreement. Any use of the debit card contrary to the law, including for the purchase of prohibited goods and/or services (e.g. using the debit card for prostitution, drug trafficking, narcotics, or other illegal activities), is punishable by law. Additionally, using the debit card as collateral for debt settlement or for the purchase of pornographic content is not permitted.

Unlawful use of the debit card or use contrary to the law or this Agreement will result in the termination of the right to use the card, its confiscation, and shall entail the User's liability for all resulting losses.

The User is obliged to use the payment card in accordance with the prescribed and contractually agreed terms and conditions governing the issuance and use of the payment card, which must be objective, non-discriminatory, and proportionate.

The User is particularly required to, immediately upon receiving the payment card, take all reasonable and appropriate measures to protect the personalized security elements of the payment card (e.g., Personal Identification Number – PIN). The User is also obligated to monitor the spending made via debit cards, which is limited to the available balance in the current account.

The User must ensure that the following types of transactions do not exceed the available funds in the current account:

1. Transactions below the authorization threshold – These transactions are approved at the point of sale without checking the available balance by the Bank.
2. Transactions authorized by the card scheme or a third party involved in the authorization process on behalf of the Bank under an agreement with the Bank.
3. Transactions involving payment for goods and services via the internet or through MO/TO transactions (Mail Order, Telephone Order) – The User cannot revoke their consent for execution of a payment transaction made with a card once the consent has been given, unless the merchant provides the Bank with a written confirmation of the revocation, in a form and content satisfactory to the Bank.

The User is required to ensure that sufficient funds are available in the account to cover the amount of executed payment transactions and the corresponding fees.

An authorized payment transaction will be recorded in the Bank's system as a reservation until the transaction is posted, for a maximum of 30 days.

The User is obliged to notify the Bank in writing, no later than within three (3) days, of any changes in the User's legal status relevant to legal transactions (e.g., change of company name, registered seat, business activity, current account number, change of authorized representative, change of company seal if used, initiation of bankruptcy or liquidation proceedings, and any other changes relevant to the implementation of the Agreement).

The User expressly agrees that the Bank may, in accordance with the law governing payment services, update data concerning the User's status and other changes related to the User's accounts based on information obtained from the organization responsible for maintaining the Register of Business Entities, within three business days of retrieving such information.

Should the User fail to comply with the obligations specified in the preceding paragraphs, the Bank may terminate the Agreement and block any further use of all debit cards issued under the Agreement.

The person authorized by the User to communicate with the Bank shall be responsible for providing all required documentation related to debit card operations upon the Bank's request.

The Contracting Parties agree that the Statutory Representative of the User shall be the responsible person for signing all documents relating to debit card operations.

1.2.4. User Conduct for the Secure Use of the Debit Card

Upon receiving the card, the User is obligated to immediately sign it in the designated area on the back of the card. The signature must match the one provided in the Application

Form. Certain transactions are carried out based on the User's signature, and if the User has not signed the debit card in the appropriate space, the User shall be deemed responsible for any transactions executed with that debit card.

The User must keep the debit card in a secure place and must not leave it in locations accessible to other persons, such as a workplace, car, etc.

The User must use the debit card solely for its intended purposes.

The User is obliged to keep the PIN code confidential. It is strictly prohibited to disclose the PIN code to anyone, including family members, friends, or any third parties. No person, including the issuing Bank, is entitled to know the User's PIN code.

The PIN code, which is considered the User's electronic signature, is generated under conditions of strict data confidentiality. The User must memorize the PIN code upon receipt and keep the envelope containing the PIN code secure and private.

The User must not record the PIN code anywhere, not even in disguised form, such as hiding it in a phone number.

The User must enter the PIN code discreetly at ATMs and POS terminals where PIN entry is required. The User is advised to ensure no one is watching and to cover the keypad with their hand. It is recommended that the User does not allow anyone to interrupt them during PIN entry. If the User notices anything unusual, they are advised to immediately inform the Bank and, where possible, the merchant.

When paying at POS terminals, the User is advised to keep the debit card in sight at all times. The User should request the return of the debit card immediately after payment or after it is swiped through the POS terminal.

If the User has valid reason to believe their PIN code is no longer confidential, they are advised to immediately change the PIN at an ATM. If the User cannot change the PIN, they are advised to immediately contact the Bank.

If an unknown person requests the User's PIN code, the User is obliged not to disclose it and to inform the Bank immediately after the incident. The User is advised to always keep the Bank's Customer Service contact number with them in order to be able to reach the Bank at any time.

When changing the PIN code, the User is advised not to select numbers that are too obvious (e.g., part of a date of birth, postal code, the first four digits of a phone number, etc.).

Failure to comply with these obligations shall be considered gross negligence and lack of due care.

In the case of card-not-present transactions, the User is obliged to take basic precautionary measures, which include the following:

- Never send sensitive debit card information or other personalized security credentials via email, SMS, phone, fax, or any other communication channel.
- For these types of transactions, only three pieces of information are sufficient: card number, expiration date, and security code (CVV/CVC).
- It is recommended to use only trusted and secure websites.

The User has the right to cancel the debit card free of charge.

When making payments for goods and/or services at a point of sale equipped with a POS terminal, the User must personally enter their PIN (if required) or sign a payment receipt (hereinafter: slip).

For security reasons, the User must safeguard the debit card and handle it responsibly, and ensure that end users of the debit card do the same and exercise special care. All actions involving the debit card at the point of sale must be conducted in the end user's presence.

The User must memorize the PIN or store it in such a way that it is not accessible to unauthorized persons who could misuse the information. The debit card is non-transferable, meaning it can only be used by the User.

The debit card can be used at all points of sale and ATMs in the country and abroad that display the logo of the card scheme to which the specific debit card belongs, as well as for all types of remote retail transactions enabled by the use of the debit card.

The User shall be held liable for any misconduct by end users contrary to the provisions outlined in the previous paragraph.

For every completed payment at the point of sale, a receipt is issued. A copy of the payment confirmation is retained by the User for their own records.

1.3. Conditions for the Use of Payment Services

1.3.1. Personalized Security Element

The Bank issues the User a personalized security element (Personal Identification Number, hereinafter: PIN), which is a numerical combination used for the authentication of the User when using the debit card. The Bank assigns the PIN to the User, and the User is required to provide it to clearly identify the end user and/or the payment account of the end user used in the payment transaction.

The Bank shall ensure that only the User has access to the PIN until the debit card is delivered.

The Bank assumes the risk related to the delivery of the debit card and PIN to the User.

1.3.2. Form and Manner of Giving and Revoking Consent for the Issuance of a Payment Order or Execution of Payment Transactions

Consent for the execution of a payment transaction must be given by the User prior to the execution of the transaction, by performing one or more actions simultaneously, unless otherwise specified by the Agreement, whereby the User may also give consent after the execution.

The User gives consent (authorization) for the execution of a payment transaction in the following ways:

- by reading the chip or contactless reading of the chip and entering the PIN on a POS terminal, or at some POS terminals with or without a signed slip;
- by contactless chip reading at a merchant's POS or ATM without entering the PIN;
- by signing the slip when the magnetic stripe is read;
- in the case of card-not-present transactions (e.g., internet transactions), by entering the security elements required by the payee (card number, expiry date, CVV/CVC code, One-Time Password (OTP));
- by using the Digital Wallet in the manner described in these Special Terms and Conditions.

The PIN entered during the execution of the transaction and confirmed as valid shall be considered an electronic signature of the transaction by the User. A payment transaction for which the User has given consent in one of the aforementioned manners shall be considered an authorized payment transaction.

The User must give consent for the execution of the payment transaction before it is carried out.

An authorized payment transaction in the Bank's system is recorded as a reservation until the moment of settlement, for a maximum of 30 days.

The User may give consent for the execution of a payment transaction also through the payee or through a payment initiation service provider.

If the User does not give consent for the execution of a payment transaction in the form and manner specified by the Agreement and these Special Terms and Conditions, such payment transaction shall be deemed unauthorized.

The Bank may reject the execution of a payment order if the conditions from this article are not met, if prescribed by regulation, or if the Bank has reasonable doubt regarding the authenticity of the payment order or any of its elements, or if the Bank suspects misuse of the card. In such case, the Bank shall notify the User of the rejection of the payment order or initiation of the payment transaction (verbally, via slip, email, or SMS, depending on the communication channel chosen in the Application for Issuance of the Debit Card), including the reason for the rejection, if possible, and the procedure for correcting the deficiency that caused the rejection, within the time period established for the execution of the payment transaction, unless notification is prohibited by law.

1.3.3. Time of Receipt of the Payment Order and Deadline for Execution of Payment Services or Individual Payment Transactions

The time of receipt of the payment order refers to the moment when the User has given consent for the execution of the payment transaction or when the Bank has performed the authentication process. The time of receipt of payment orders and deadlines for the execution of payment transactions are defined in the Transactions Schedule.

The User's payment account may not be debited before the payment order is received.

The Bank, as the payer's payment service provider, is obliged to ensure that the value date of the debit on the User's payment account related to the execution of the payment transaction is the same or later than the date on which the account was debited for the amount of the payment transaction.

The payee's payment service provider is obliged to ensure that the value date of the credit on the payee's account is no later than the business day on which the payment transaction amount was credited to its account.

In the case of a domestic payment transaction, if the User deposits cash in the currency of the payment account to the payment account held with the Bank – the Bank must ensure that the value date of the credit to the payment account is the date on which the cash was received.

In the case of international payment transactions or payment transactions in the currency of third countries, the Bank is not obliged to provide or make available to the User the information on the execution time or the fees of the payee's bank in the third country if such information is not available at the time of initiating the payment transaction. However, the Bank must provide information on the expected execution time of the payment transaction.

1.3.4. Transaction Limits for the Use of Debit Cards

Users may dispose of funds up to the available balance on the User's account to which the debit card is linked.

The Bank determines daily spending and cash withdrawal limits, the maximum number of daily transactions, as well as the daily limit for deposit of daily takings (merchant cash deposits), all of which are published on the Bank's website and

in its business premises, within the document Limits for the Use of Payment Instruments, which forms an integral part of the Framework Agreement.

The Bank, in accordance with the technical capabilities of ATMs, enables the User to deposit daily takings in RSD to the current account linked to the debit card.

Upon written request from the User, the Bank may approve a change to these limits, either an increase or a decrease.

The Bank reserves the right to change the amount of the limits. The User shall be informed in advance of any new limit.

1.4. Information and Data on Fees and Exchange Rates

1.4.1. Type and Amount of Fees Charged by the Bank to the User

At the time of signing the Application, the User was informed of the Price List, i.e., notified of the types and amounts of fees charged by the Bank, by being presented with the Price List.

The User is obliged to pay the Bank the applicable fees in accordance with the Price List.
Fees are charged by directly debiting the debit card account.

The User hereby expressly and irrevocably authorizes the Bank to, without any further consent or instruction, debit any of the User's accounts held with the Bank to collect all due and outstanding fees relating to the use of any or all contracted services, in accordance with the Price List, unless there are legal restrictions to such execution.

If the User does not have sufficient funds in the required currency on their accounts, the User agrees that the Bank may convert funds from other currencies held on the User's accounts and use them to settle the Bank's claims.

The Bank reserves the right to amend the amounts of fees and other charges, or to introduce new ones, of which the User shall be notified.

The type and amount of fees for services provided by the Bank to the User, including those related to the method and frequency of delivery or availability of information in accordance with the Law, are defined in the Framework Agreement with the User and aligned with the applicable Price List.

Fees charged by third parties are determined and amended based on the applicable decisions of competent authorities and organizations whose services are used by the Bank's Users in connection with financial services.

The Bank shall inform the User of changes in fees before their application, indicating the effective date of the amended fee, to the extent and in the manner regulated by Article 3.1 of this Annex.

1.4.2. Exchange Rate – Transaction Currency

A payment transaction shall be executed in the currency agreed upon between the User of payment services and their payment service provider, in accordance with applicable foreign exchange regulations.

The Bank shall execute the payment order in the currency and with the currency code indicated in the order.

Execution of the payment order may require the purchase and/or sale of domestic or foreign means of payment (currency conversion); for such conversions, the Bank shall apply the buying/selling exchange rate from the Bank's daily **Exchange Rate List** for foreign currency.

When converting domestic currency into foreign currency (purchase of foreign currency), the Bank will use its selling rate, and when converting foreign currency into domestic currency (sale of foreign currency), it will use its buying rate, applicable on the day of currency conversion.

The Bank reserves the right to apply a more favourable exchange rate than the official daily rate, to be determined by mutual agreement between the Bank and the User.

The Bank's Exchange Rate List is available at the Bank's business premises and on its official website.

Liabilities incurred in foreign currency through the use of the debit card abroad are converted by the Bank into RSD using the Bank's selling exchange rate. The User acknowledges and accepts the possibility of a rate change occurring between the moment of the transaction and the moment of its financial settlement.

Exchange rate changes may be applied immediately and without prior notice to the User if they are based on changes in the reference exchange rate.

Currency conversion cannot be executed without the User's consent.

1.5. Information on the Means and Methods of Communication Between the User and the Bank

1.5.1. Notifications

The User shall provide the Bank with contact details at the time of establishing a business relationship, as well as subsequently during the term of the business relationship with the Bank.

The means of communication between the User and the Bank may include the following, depending on the type of communication:

- Orally – by visiting a branch or calling the Bank's Contact Center;

- In writing – including notifications, letters, and other written documents;
- Electronically – including the Bank's website, chat, email, digital and mobile banking applications and features (such as in-app or push notifications), use of applications and social media such as Viber, WhatsApp, Facebook, etc., SMS messages, and other applications enabling individual communication with the User, as well as any other application solutions made available by the Bank depending on technical capabilities.

Where the User has provided the Bank with an email address, the Bank may use it to send, among other things, the following:

- Account statements including all information on payment transactions, in accordance with the Law on Payment Services;
- Reports on fees charged, in accordance with the Law on Payment Services;
- All other notifications regarding existing products and newly offered products, in accordance with applicable legal regulations and the terms of the agreement concluded;
- Any other notifications required by law.

Delivery of such communications as described above shall be deemed to fulfil the Bank's legal and contractual obligation to inform the User.

The User is required to immediately notify the Bank of any changes to their address, email address, or phone number. If the User fails to comply with this obligation, any communication sent by the Bank to the last known address, email, or phone number provided shall be deemed properly delivered.

By signing the application in the designated place, the User is considered to have accepted and agreed to all provisions of these General Terms and Conditions, which form an integral part of the Framework Agreement.

All communication between the Bank and the User, relating to the rights and obligations under the Agreement, shall be conducted in the Serbian language. This does not exclude the use of other languages, in accordance with best practices in banking operations.

The Bank is authorized to use any contact information provided by the User at the time of establishing or during the course of the business relationship with the Bank (e.g., mobile number, email address, telephone number, postal address, etc.). In addition to the chosen method of communication, the Bank may send notifications and information related to the fulfilment of contractual obligations via telephone, SMS, online and mobile banking, voice messages, email, or any other means of remote communication that allows individual communication with the User (such as applications and social media like push/in-app notifications, Viber, WhatsApp, Facebook, etc.), chat, or via internet portals made available by the Bank. The Bank may use one or a combination of these communication methods.

The User may state their preferred method of communication with the Bank and/or request a change to the selected method of communication in a manner that reliably confirms the User's identity (e.g., sending an email from the registered email address, an SMS from the registered mobile number, a call to the Contact Center from the registered phone number, visiting a branch, or using electronic or mobile banking applications or communication applications that allow individual communication, such as push notifications, Viber, WhatsApp, etc.).

The Bank guarantees the confidentiality of data in accordance with the Law on Banks and ensures that the data will be used only for the purposes stated. In the event that a notification cannot be delivered due to the User's fault (e.g., unpaid bills to their service provider, provider system error, incorrect/incomplete address, changed phone number), the Bank shall not be held liable for any resulting direct or indirect damage.

All relevant information (fees, exchange rates, etc.) related to the execution of payment transactions, as well as contact addresses for communication with the Bank, can be found on the Bank's website. The User has the right to receive one copy of the Agreement in writing or on another durable medium, and throughout the duration of the contractual relationship, may request copies of the Agreement or of the pre-contractual information constituting mandatory elements of the Agreement, in a format that enables the User to review the conditions applicable to the provision of payment services and compare offers from different payment service providers to assess whether the terms and services meet their needs.

Any notice, request, or reminder regarding outstanding obligations issued by the Bank—even if related to an additional card—shall be sent to the primary cardholder at the address stated in the Application for Card Issuance or to a new address if the User has informed the Bank in writing of an address change.

It is explicitly agreed that the last address provided by the User shall be unconditionally and irrevocably deemed their legal address for all purposes, to which all notifications and documents shall be sent.

1.5.2. Receipt of Information by the User

Any information or document delivered by the Bank to the User, in accordance with the agreed method of communication, shall be deemed to have been received by the User as follows:

- if posted within the Bank's electronic or mobile banking application – on the date of posting;
- if sent via email – on the date the email was sent;
- if sent by post – on the date it was submitted to the postal service or a company registered for delivery;
- if sent via SMS – on the date the SMS was sent;
- if sent via another electronic communication channel, i.e., via a medium that enables individual communication with the User (e.g., through Viber, WhatsApp, push notification, etc.) – on the date the message was sent.

The Bank shall not be liable for delivery or functioning of electronic communication channels that are not part of its own information systems and that the User has opted to use (e.g., where the User's antivirus program blocks emails from the Bank's address, etc.).

The User is obligated to ensure all technical and other preconditions for the proper functioning of the chosen electronic communication channels (e.g., that the provided email address is active, that the User has not blocked the Bank as a sender for SMS or Viber delivery, that the User has enabled push notifications for the Bank's mobile banking app, etc.).

1.5.3. Additional Services and Special Use of Provided Contact Information

The Bank may provide the User with access to and use of additional services in which the provided contact details are used for identification or authorisation, independently or in combination with other methods of identification or authorisation, based on the user guidelines for these services, including:

- Contact Centre
- Interactive Voice Response (IVR)
- SMS/Push notifications
- ChatBot service
- Online requests

The Bank shall regularly inform the User about the account balance through account statements, e.g., by mail, SMS, or email.

Upon the User's request, the Bank is obligated, prior to executing a specific payment transaction initiated by the User under the Agreement, to provide accurate information on the execution time for that transaction and the fees to be charged. If the Bank charges fees in aggregate, it must also provide information on the type and amount of each individual fee included in the total.

The Bank is obliged, upon the User's request, to provide a paper account statement once a month free of charge, showing executed payment transactions, which must include the following information:

1. a reference number or other data enabling the User to identify the individual payment transaction and information relating to the payee;
2. the amount of the payment transaction in the currency in which the User's payment account is debited or in the currency specified by the payer in the payment order;
3. the amount of any fee charged to the User for executing the individual payment transaction, and, where such fees are charged in aggregate, the type and amount of each individual fee included in the total;
4. where currency conversion is applied – the reference exchange rate used and the amount of the payment transaction after currency conversion;
5. the value date of the debit to the User's payment account or the date of receipt of the payment order.

The User has the right, at any time during the validity of the Framework Agreement, to request a copy of the Agreement, as well as to change the communication channel with the Bank, unless such change would be contrary to the provisions of the concluded Framework Agreement or incompatible with the nature of the product or service.

1.6. Information on Protective and Other Measures in Connection with the Execution of Payment Transactions

1.6.1. Procedure in Case of Loss, Theft or Misuse of the Payment Card

The User is obligated to immediately notify the Bank or an entity designated by the Bank upon becoming aware of the loss, theft or misuse of the debit card. In the event that the debit card is lost, stolen, or if any third party has knowledge of the PIN code, the User must, without delay, notify the Bank by calling the Contact Centre or in writing and request the blocking of the debit card.

If the notification is made via telephone, it will be recorded electronically, and the Bank is obligated to block any further use of the debit card. Any material damage incurred due to loss, theft, or misuse of the debit card prior to notification shall be borne by the User. If the User finds the debit card after

reporting it as lost, stolen, or misused, they must not use it and must return it to the Bank without delay.

In the event of damage to the debit card or if the card has been lost or stolen, the User must submit a request at a Bank branch for the issuance of a new debit card to replace the damaged, stolen, or lost card. When signing the request for a new debit card, the User shall return the damaged card to the Bank.

The User shall not bear losses arising from this clause if the Bank has not provided an appropriate method for reporting the lost, stolen, or misused payment instrument—except where the losses occurred due to fraudulent actions by the User.

1.6.2. Right of the Bank to Block the Debit Card

The Bank may block the use of a debit card if there are justified reasons related to the security of the card, if there is suspicion of unauthorized use or use for fraudulent purposes, or if there is an increased risk that the User will not be able to fulfil their payment obligations, especially when the debit card is linked to an approved credit or authorized overdraft.

The Bank is required to inform the User of the intention to block the debit card and the reasons for doing so, either in advance or, at the latest, immediately after the card has been blocked, through the agreed communication channels (by phone or in writing).

The Bank will re-enable the use of the debit card or replace it with a new one once the reasons for the blockage cease to exist.

1.6.3. Payment Transactions Where the Transaction Amount is Not Known in Advance

If a payment transaction initiated by the payee or via the payee is executed using a payment card, and the exact amount is not known at the time the User provides consent for the execution of the transaction, the User's payment service provider may not reserve funds on the User's account unless the User has consented to the specific amount of funds to be reserved.

The User's Bank must release the reserved funds on the User's payment account without delay after receiving the information on the exact amount of the payment transaction, and at the latest immediately upon receipt of the payment order.

1.6.4. Liability of the Bank and the User for Initiated, Unexecuted, Incorrectly Executed, or Unauthorized Payment Transactions

In the case of an unauthorized, unexecuted, or incorrectly executed payment transaction, and without prejudice to the obligations set out in Article 6 of these Special Conditions, the Bank is obligated—regardless of liability for the proper execution of the payment transaction—to take appropriate steps, upon the User's request, to trace the flow of funds related to the payment transaction and to promptly provide the User with information on the outcome of such steps.

The Bank shall not charge the payer any fee for acting in accordance with paragraph 1 of this clause.

The User has the right to request compensation from their Bank or, if the payment transaction was initiated through a payment initiation service provider, from that provider, in accordance with the applicable law, for any damages arising from the execution of an unauthorized payment transaction, or due to failure to execute, incorrect execution, or delayed execution of a payment transaction for which the provider is responsible.

If the User claims not to have authorized the payment transaction, or that it was not executed or was incorrectly executed, the Bank—if it claims otherwise—is obligated to prove, for the part of the service it provided, that the transaction was authenticated, properly recorded, and posted, and that the execution was not affected by any technical failure or other deficiency.

If the payment transaction was initiated via a payment initiation service provider, that provider is obligated to prove that the transaction, for the part of the service it provided, was authenticated and properly recorded, and that no technical failure or other deficiency affected its execution.

A payment transaction is considered authenticated, within the meaning of paragraphs 4 and 5 of this clause, if the payment service provider applied the appropriate procedures to verify and confirm the use of the specific payment instrument, including its personalized security elements.

If the payer claims that they did not authorize the payment transaction carried out using a payment instrument or initiated through a payment initiation service provider, the payment service provider's record of the use of that instrument or the initiation of the payment transaction is not, by itself, sufficient proof that the payer authorized the transaction, acted fraudulently, or acted with intent or gross negligence.

The Bank, and accordingly the payment initiation service provider, must provide evidence sufficient to support the likelihood that the User acted fraudulently or with intent or gross negligence.

1.6.5. Liability of the User for Unauthorized Payment Transactions

The User shall bear losses resulting from the execution of unauthorized payment transactions up to the amount of RSD 3,000 if such transactions were executed as a result of:

1. the use of a lost or stolen payment instrument, or

2. the use of a payment instrument that has been misused.

Notwithstanding paragraph 1 of this Article, the User shall bear all losses resulting from the execution of unauthorized payment transactions if such transactions were carried out due to the User's fraudulent actions or failure to fulfill their obligations under Articles 1.2.4 and 1.6.1 of these Special Terms and Conditions, due to intent or gross negligence.

The User shall not be liable for losses under this Article in the following cases:

1. if the User could not have detected the loss, theft, or misuse of the payment instrument prior to the execution of the unauthorized transaction, except in cases referred to in paragraph 2 of this Article;
2. if the unauthorized transaction is the result of an act or omission of an employee, agent, or branch of the payment service provider or another entity to whom the payment service provider's activities were outsourced, except in cases referred to in paragraph 2 of this Article;
3. if the Bank did not provide the User, at all times, with an appropriate means to report the loss, theft, or misuse of the payment instrument without delay and free of charge, unless the losses were the result of the User's fraudulent actions;
4. if the Bank did not require strong customer authentication, unless the losses resulted from fraudulent actions by the User.

If the Bank requires strong customer authentication and the payee or the payee's payment service provider fails to apply it as required, they shall compensate the Bank for any resulting losses.

The User shall not be liable for losses arising from unauthorized payment transactions executed after the User has properly notified the Bank in accordance with these Special Terms and Conditions that the payment instrument has been lost, stolen, or misused—except where such losses resulted from fraudulent actions by the User.

By exception to paragraph 1 of this Article, the National Bank of Serbia may prescribe that the User shall bear losses from unauthorized transactions up to an amount lower than RSD 3,000, particularly taking into account the nature of the personalized security features of the payment instrument and the circumstances under which it was lost, stolen, or misused.

1.6.6. Liability of the Bank for Unauthorized Payment Transactions

The Bank is liable for the execution of a payment transaction for which the User has not given consent (hereinafter: unauthorized payment transaction).

In the case of an unauthorized payment transaction, the Bank is obligated, immediately upon becoming aware and no later than the next business day after discovering or being informed about such a transaction, to refund the amount of that transaction to the User—unless the Bank suspects fraud or misuse on the part of the User. In such a case, the Bank must, within ten days of becoming aware of the unauthorized transaction, take one of the following actions:

1. explain to the User the reason for refusing the refund and report the fraud or misuse to the competent authority; or
2. refund the transaction amount to the User if, after further investigation, it concludes that the User did not act fraudulently or commit misuse.

The Bank must return the User's payment account to the state it would have been in had the unauthorized transaction not occurred, ensuring that the value date of the credit to the User's account is no later than the date on which the account was debited.

The Bank must also refund any fees charged to the User and pay any interest the User would have earned had the unauthorized transaction not been executed.

If the payment transaction was initiated via a payment initiation service provider, the provisions of this Article apply to the Bank as the account servicing payment service provider.

1.6.7. Liability for Non-Executed or Improperly Executed Payment Transactions or Delays in Execution of Transactions Initiated by the User (Payer)

If the payment transaction was initiated directly by the User, the Bank is liable to the User for its proper execution up to the payment service provider of the payee.

If the Bank is responsible for the non-execution or incorrect execution of a payment transaction, it must, immediately upon becoming aware, refund the amount of the unexecuted or improperly executed transaction to the User or return the User's account to the state it would have been in had the improper execution not occurred—unless the User has requested proper execution of the transaction.

In such cases, the Bank must ensure that the value date for the credit to the User's account corresponds to the date the account was debited for the improperly executed transaction.

If the Bank provides proof to the User (and, if necessary, to the payee's payment service provider) that the account of the payee's provider has been credited with the transaction

amount, the payee's payment service provider shall be liable to the payee for the non-execution or improper execution of the payment transaction.

The payee's payment service provider must ensure that the value date for the credit to the payee's account is no later than the business day on which the funds would have been credited had the transaction been correctly executed.

If the payment transaction was executed later than the time prescribed by law, the payee's payment service provider must, at the request of the Bank acting on behalf of the User, ensure that the value date of the credit is no later than the business day on which the funds would have been credited had the transaction been executed correctly in accordance with the Law and these Special Terms and Conditions.

If the Bank is responsible for the non-execution or incorrect execution of the payment transaction, or a delay in execution, it must refund the User all fees it charged in connection with the transaction and reimburse any interest the User would have earned in relation to the unexecuted or incorrectly executed transaction.

If the payment transaction was initiated by the User via a payment initiation service provider, the Bank is considered the User's payment service provider for the purposes of paragraphs 1–4 and 6 of this Article.

In the case of such a transaction, the payment initiation service provider must prove that the Bank received the payment order in accordance with Article 1.3.3 of these Special Terms and Conditions and that, for the part of the service it provided, the transaction was authenticated, properly recorded, and unaffected by any technical failure or deficiency related to the non-execution or improper execution of the transaction or delay in execution. The provider must promptly deliver such evidence upon the Bank's request.

1.6.8. Liability for Non-Executed or Improperly Executed Payment Transactions or Delay in Execution of a Payment Transaction Initiated by the Payee or by the User (Payer) via the Payee

If a payment transaction is initiated by the payee or by the User via the payee, the payment service provider of the payee shall be liable to the payee for the correct transmission of the payment order to the Bank, acting as the payment service provider of the User.

If the payment order is not transmitted, or not transmitted correctly, as per paragraph 1 of this Article, the payee's payment service provider shall, immediately upon becoming aware, transmit or retransmit the payment order to the Bank.

If the payment order was transmitted to the Bank after the deadline agreed upon between the payee and their payment service provider, the payee's provider shall ensure that the value date for the credit to the payee's account is no later than the date the payee's account would have been credited if the payment transaction had been executed on time.

If the amount of the payment transaction initiated by the payee or by the payer via the payee has been credited to the account of the payee's payment service provider, that provider shall be liable to the payee for the proper execution of the payment transaction.

If the payee's payment service provider is liable under paragraph 4 of this Article, they shall ensure that the value date for the credit to the payee's account is no later than the date the account would have been credited if the transaction had been properly executed.

If the payee's payment service provider provides evidence to the payee—and, if necessary, to the Bank—that it is not liable under paragraphs 1 to 4 of this Article, the Bank shall be liable to the User for the non-executed or improperly executed payment transaction.

The provisions of Article 1.6.7, paragraphs 2 and 3, of these Special Terms and Conditions shall apply mutatis mutandis to the Bank in cases where it is liable under paragraph 6 of this Article.

The Bank shall not be liable under the preceding paragraph if it proves that the payee's payment service provider received the transaction amount and that the delay in execution was minimal. In such case, the payee's provider must ensure that the amount is credited to the payee's account with a value date no later than the date it would have been credited had the transaction been executed properly.

A payment service provider that is liable under this Article shall reimburse its payment service user the full amount of any fees charged, and shall also refund or pay the full amount of any interest to which the user is entitled in relation to the non-executed or improperly executed transaction.

1.6.9. Notification or Request as a Condition for Refund or Correct Execution of the Payment Transaction

The Bank shall be obligated to provide a refund or ensure the proper execution of a payment transaction if the User notifies the Bank of an unauthorized, non-executed, or improperly executed payment transaction—or requests the correct execution of such a transaction—immediately upon becoming aware of it, provided that the notification or request is submitted no later than 13 months from the date of debiting the account.

If the Bank has not provided the User with the information regarding the payment transaction, it shall be liable for the unauthorized, non-executed, or improperly executed transaction and must provide the refund even after the

expiration of the 13-month period, provided the User reported the issue immediately after becoming aware of it.

If a payment initiation service provider was involved in the execution of the transaction referred to in paragraph 1 of this Article, the refund shall be requested by the payment service user from the Bank that maintains the user's account.

1.7. Rights and Obligations of Payment Service Providers in Case of Payment Transactions Resulting from Fraud or Misuse and in Certain Cases of Incorrectly Executed Payment Transactions

If the Bank receives a request for a refund of funds along with data, information, and documentation based on which it is likely that the payment transaction in question resulted from fraud or misuse, the payment service provider of the payee shall be obliged not to credit these funds to the payee's account and to disable the payee from disposing of such funds for a period of three business days from the date of receipt of said data, information, and documentation.

If, in the case referred to in paragraph 1 of this Article, the payment service provider of the payee subsequently, but before the expiry of the deadline referred to therein, receives from the Bank data, information, and documentation—including the relevant report submitted to the competent state authority—which, collectively and beyond reasonable doubt, indicate that the transaction was fraudulent or abusive, the payment service provider of the payee shall:

1. Immediately refund the funds to the User if the payee, within 15 business days from the date they were notified by their payment service provider of the data, information, documentation, and report referred to in this paragraph, fails to prove or make it likely that the funds are of lawful origin, or if the payee refuses to provide the requested evidence;
2. Allow the payee to dispose of the funds upon the expiry of 30 business days from the deadline set in paragraph 1 of this Article, provided that the payee has, within the period referred to in item 1 above, proven or made it likely that the funds are of lawful origin and that the competent state authority has not issued or submitted a ruling prohibiting the disposal of said funds.

The payment service provider of the payee shall be liable to the payer for any loss incurred as a result of a payment transaction referred to in paragraph 1 of this Article if the provider allowed the payee to dispose of the funds contrary to the provisions of paragraphs 1 and 2, and it is established in the relevant procedure that the payee committed or participated in the fraudulent or abusive activity.

The Bank has the following rights and obligations in specific cases of incorrectly executed domestic payment transactions:

1. If the payer's payment service provider transfers to the payee's payment service provider an amount that exceeds the amount stated in the payment order or erroneously executes the same payment order multiple times, the payee's payment service provider shall be obliged to immediately return such funds to the payer's provider based on evidence provided by the payer's provider who made the error;
2. If an amount less than that specified in the payment order is transferred to the payee's provider, the payer's payment service provider may, on the same business day, transfer the difference to the payee's provider without a request from the payment service user for correct execution of the transaction;
3. If the funds are transferred to a payee other than the one indicated in the payment order, the payer's provider may, on the same business day when the payment order was received, correctly execute the payment transaction even without a request from the payment service user for proper execution, while the payee's provider who erroneously received the funds shall, in any case, be obliged to return (re-transfer) the funds without delay to the payer's provider based on evidence of the error.

Refunds of funds under paragraph 2, item 1 and paragraph 4, items 1 and 3 of this Article shall take precedence over the execution of any other payment transactions from the payment account to which the funds were transferred.

1.7.1. Refund of an Authorized and Properly Executed Payment Transaction to the User

At the User's request, the Bank shall refund the full amount of an authorized and properly executed payment transaction (hereinafter: Refund Request) initiated by the payee or by the User via the payee, if the following conditions are met:

1. The User gave consent for the execution of the payment transaction without specifying the exact amount;
2. The amount of the payment transaction exceeds the amount that the User could reasonably have expected, considering their previous payment transactions, the terms set forth in the Framework Agreement, and the specific circumstances of the case.

The Bank may require the User to provide evidence of facts related to the fulfilment of the above conditions. The User may not claim that the amount was unexpectedly high if the higher amount is a result of currency conversion at a reference exchange rate.

The User shall not be entitled to a refund of the amount of the payment transaction if the following conditions are met:

1. The User directly gave consent to the Bank for the execution of the payment transaction;

2. The Bank or the payee provided information about the forthcoming payment transaction to the User in the agreed manner at least 28 days prior to the due date.

The User may submit the Refund Request within 56 days from the date of the account being debited. The Bank is obliged to refund the full amount of the payment transaction or notify the User of the reasons for rejecting the Refund Request within 10 business days of receiving the Request. The value date of the credit to the User's account shall be no later than the date the account was debited for the said transaction.

If the Bank refunds the claimed amount to the User and later determines in the dispute resolution procedure (in accordance with card network rules) that the claim was unfounded, it shall debit the User's payment account for the amount that was unjustifiably refunded, without requiring further consent from the User.

If the Bank rejects the User's Refund Request, it must inform the User of:

1. The procedure for exercising the User's rights and interests, including extrajudicial dispute resolution;
2. Legal remedies available for breaches of statutory provisions;
3. The competent authority responsible for conducting such proceedings.

The User shall not be entitled to a refund of the transaction amount from paragraph 1 of this section if:

1. The User directly gave the Bank consent to execute the payment transaction;
2. The Bank or the payee provided the User with information about the upcoming transaction at least 28 days before the due date in the agreed manner.

1.7.2. 3D Secure Protection

For additional protection when making payments online, the Bank's Visa and Mastercard payment cards support *3D Secure* secure authentication protocols.

If the website used for payment supports 3D Secure, the Bank may require additional user authentication via a One-Time Password (OTP).

2. Digital Wallet

The rules and conditions for executing cashless payment transactions using Digital Wallet functionality are defined by these Special Terms and the AikBank Rules and Conditions for the use of this functionality, which form an integral part of the Framework Agreement for the issuance and use of a debit card.

2.1. Activation of the Digital Wallet, Use, and Execution of Transactions with a Digitized Card

The User contracts the Digital Wallet service with the Wallet Provider. The Bank is not a party to that agreement, nor does it assume or can it assume any rights or obligations arising therefrom. The Bank is not liable for the availability or the operational functionality of the service.

The User may register their debit card in the Digital Wallet either via the Wallet Provider's app or via the Bank's mobile banking application, provided that the Bank has enabled such functionality. By registering a debit card in the Digital Wallet, a digital (electronic) version of the card is created, and all terms and conditions applicable to the original physical debit card also apply to its digital version, in accordance with the Framework Agreement concluded between the User and the Bank.

If the User has more than one card registered in the Digital Wallet, they may independently choose which card to use for initiating a payment transaction.

Consent for executing transactions initiated through the Digital Wallet is given by the User by holding their mobile device near a POS terminal or ATM, or by selecting the Digital Wallet payment option on an online merchant site and entering the personalized security elements they set or agreed upon with the Wallet Provider.

The Bank shall debit the User's payment account linked to the debit card for the amount of such transaction. The User may obtain information about transactions executed through the Digital Wallet not only from the Bank but also from the Wallet Provider.

It is not possible to make instalment payments using the electronic card at partner merchant locations.

2.2. Conditions for Using Digital Wallet Services

The digital wallet service is free of charge. Fees and charges incurred by the User in connection with transactions are governed by the Framework Agreement or the agreement on the issuance of the relevant Card.

To add their Card to the digital wallet on a mobile device, the mobile phone number used on that device during the activation of the service must be previously registered with the Bank. If the User's mobile number is not registered with the Bank, the Bank reserves the right to perform additional identification or to reject the registration. The User may add a single Card to a maximum of nine (9) devices.

The Wallet Provider will enable payments via the digital wallet on a mobile device. The digital wallet service allows Card Users to register the Card in the application and manage a token. A token is a surrogate of the card within the digital wallet service, created when the Card is registered in the digital wallet application on a mobile device. Adding the Card to the

digital wallet as part of the service functionality requires the User to enter the card number, card expiration date, CVC code (three-digit number printed on the back of the card), and basic User information. After registration and acceptance of these Terms and Conditions for using the digital wallet service, the User receives a one-time verification code sent to the phone number registered with the Bank, which must be entered in the designated input field.

After saving the Card in the digital wallet application, the service allows the User to make secure payments in physical stores, apps, and on websites that support the Wallet Provider's application and accept the Bank's payment cards.

The User gives consent for executing a payment transaction by bringing the device on which the digital wallet is installed close to a POS terminal, and if necessary, by confirming the transaction using authentication methods agreed with or set by the Wallet Provider.

The service enables Users to register a payment Card in the digital wallet application and manage the token. The token is created when the Card is registered and stored in the digital wallet application, and it enables secure payments at merchant locations equipped with NFC technology that accept digital Cards (from the digital wallet application).

The User may add more than one card to the digital wallet application. The first card added becomes the default (primary) payment card. The User may subsequently change or adjust the primary card settings at any time.

By using the digital wallet service, the User may perform transactions up to the limits authorized by the Bank, as agreed with the Bank.

The User is entitled to request the registration of a Card in the digital wallet only on devices of which they are the lawful owner/holder. The registration of the Card may be initiated directly within the digital wallet application. Card registration in the application must be performed only on iOS/Android devices with original software, compatible with the application of the respective Wallet Provider, equipped with NFC technology, and running an operating system supported by the Provider. The Wallet Provider may impose its own limitations or restrictions regarding the use of the digital wallet. For a Card to be registered in the digital wallet application, the User must cumulatively meet all requirements set by the Wallet Provider under a separate agreement concluded between the User and the Provider.

Aik Banka is not responsible for the establishment or modification of the conditions imposed by the Wallet Provider under said agreement.

The Bank reserves the right to unilaterally disable the ability to perform transactions via the digital wallet or to prevent token creation (card digitalization) in the event of suspected card data misuse, suspected fraudulent behaviour by the User or third parties, or suspected unauthorized transactions within the card scheme. If the User does not have a phone number registered in the Bank's system, card registration in the digital wallet will not be possible.

In the event of suspected compromise of the device's security settings (e.g. password, PIN, default pattern, etc.) used to access a mobile device on which a digitized Card has been added or is planned to be added, the Bank shall, upon learning of this, block the Card, which will result in the blocking of all associated tokens across all devices, and shall promptly inform the User thereof.

2.3. User Obligations

The User of the digitized card service is obliged to:

1. Register the Card in the digital wallet application only on devices that legally belong to the User and are used exclusively by the User;
2. Set a password with a high level of complexity to secure the device and keep that password in a safe place;
3. Not use security settings (password, PIN, default pattern, etc.) on the mobile device on which the Bank's Digitized Card is added or intended to be added in a way that could be easily guessed or associated with the User;
4. After registering the Card in the digital wallet application, ensure the same level of care in protecting the device as required for the physical Card, and protect the device from unauthorized use, loss, or theft, and prevent misuse of the token in the event of loss or theft;
5. Not allow other individuals to access the mobile device by storing their biometric data (fingerprint, facial recognition, etc.);
6. Immediately notify the Bank in the event of loss or theft of the Card or theft of the Card data required to use the service;
7. Immediately notify the Bank of the loss, destruction, theft, unauthorized access to, or unauthorized use of the device that contains the token;
8. Continuously monitor the account linked to the Card and review transactions made using the digitized card service and immediately report any irregularities or deficiencies to the Bank;
9. Not allow transactions to be executed by any third party, except the User, and ensure that only their own biometric data are stored on the device in cases

10. where biometric verification is used for user authentication and transaction confirmation;
11. Protect security options on the device (PIN and other security elements) from exposure and misuse.

Removing a token from the digital wallet application removes it only from that specific device. If the User reports the loss of a device containing the token, the Bank will block the digitized payment card only on that device (the card will not be blocked on other devices). To reactivate the digital payment card on the same device, the registration process must be initiated again in accordance with these Terms and Conditions.

If the User notifies the Bank of the loss, destruction, theft, unauthorized access by another person, or unauthorized use of the device containing the token (digitized payment card), the Bank will remove the token only from that device (which results in the deactivation of the digitized payment card on that specific device). The User will still be able to use the payment card and the digital wallet on another device (provided that device is owned by the User). If the User wishes to block the digitized payment card on all devices where the Bank's digital wallet application and the digitized card are installed, the User must explicitly request this from the Bank.

In the event that the card is permanently blocked, the Bank will deactivate all tokens related to that card on all devices used by the User, which will result in the inability to make payments via the digital wallet using the permanently blocked card on all devices where that card was installed. If the User, based on a blocked card, requests that the Bank issue a new replacement card, the Bank is obliged to activate a new token without requiring a new registration process, i.e. the Bank is required to enable the use of the replacement card through the digital wallet.

If the User encounters any issue related to the use of the service, they may contact the Bank's Contact Center.

The Bank processes and protects personal data in accordance with the Privacy Policy, the Notice on Personal Data Processing, and the Personal Data Protection Rulebook, all of which are published on the Bank's website and available at all Bank branches.

2.4. Bank's Obligations

The Bank undertakes the following:

1. To ensure that the personalized security elements of the payment instrument are accessible exclusively to the User to whom the instrument has been issued, without prejudice to the User's obligation to take all reasonable and appropriate measures for the protection of such personalized security elements (e.g., personal identification number) immediately upon receipt of the payment instrument;
2. To notify the User of any executed transaction;
3. To ensure that the User may, at any time, immediately after becoming aware of the loss, theft, or misuse of the payment instrument, notify AikBank as the payment service provider, or request that the use of the payment instrument be restored or replaced with a new one – once the reasons for its blocking no longer exist;
4. To prevent any further use of the payment instrument after the User has informed the Bank, without delay, about its loss, theft, or misuse;
5. To notify the User on a monthly basis of the account turnover by delivering an account statement, as agreed under the Framework Agreement on the use of the account and/or payment card.

The Bank may not issue a payment instrument to the User if it was not requested by the User, unless an already issued payment instrument needs to be replaced.

The Bank bears the risk associated with the delivery of the payment instrument and its personalized security elements to the User.

The Bank is obliged to provide the User with proof that the User reported the loss, theft, or misuse of the payment instrument, if the User submits a request for such proof within 18 months from the date of the notification.

By introducing unconditional SIM verification, the Bank establishes mandatory registration of the User's mobile phone number in the Bank's system, which includes SMS notifications for each approved payment card authorization, including wallet transactions. The User agrees and acknowledges that SMS notifications related to the use of the digital wallet application cannot be disabled.

2.5. Exclusion of the Bank's Liability

The Bank shall not be liable for:

a) Payments executed using the token if such payments were made by other persons with the consent of the User (via the digital wallet);

b) Any loss or damage (material or non-material) resulting from the User's failure to comply with these Terms and/or any applicable provision governing the relationship between AikBank and the User;

c) Any direct or indirect damage, including but not limited to loss of profit, lost earnings, or any other similar losses incurred by the User due to technical deficiencies in the use of the application or services, or due to inadequate application quality;

d) Any circumstance that interrupts, prevents, or affects the functioning of any card stored in the application, including but

not limited to application or internet service unavailability, communication failures, network delays, limited internet coverage, system outages, and other technical issues.

2.6. Token Removal and Card Blocking

By removing a token from the digital wallet, the token is removed only from that specific device. In the event of card blocking, actions are carried out in accordance with the agreed documentation and business terms and conditions. If the User notifies the Bank of the loss of the device containing the token (digitalized payment card of the Bank), the Bank shall block the token (digitalized payment card) on that device. After such blocking, the User may continue to use the payment card and digital wallet on another device (owned by the User). If the payment card itself is reported lost, the Bank will block the payment card, which will also result in the blocking of all related tokens on all devices.

In the case referred to in section 7.1, if the User wishes to reactivate the token (digitalized payment card) on the same device, they must go through the registration process again in accordance with these Terms of Use.

If the card is deactivated, the Bank will remove all tokens related to that card from all devices used by the User.

2.7. Processing of Personal Data and Payment Transactions Initiated via the Digitalized Card

By registering a debit card in the Digital Wallet through the mobile banking application, the User authorizes the Bank to provide the Service Provider with the User's identification data and the registered debit card information, including the card's expiration date, for the purpose of concluding a contract between the User and the Service Provider. The Service Provider is the data controller with respect to the personal data of the User with whom it has entered into a Digital Wallet agreement, and as such, is responsible to the User for the lawful processing of their personal data necessary for the conclusion and performance of the Digital Wallet service agreement, during its term and after its termination.

The Bank has no influence over and is not responsible for the manner in which the Service Provider collects and processes such data.

During the validity and use of the Digitalized Card, the Bank provides the Service Provider with non-personalized information regarding payment transactions initiated via the digitalized card, for the purpose of fulfilling the agreement between the User and the Service Provider.

The conclusion and use of the Digital Wallet service involves the secure transmission of information via electronic communication networks, the availability of which is ensured by providers of electronic communication services beyond the control of the Bank, including the User's own electronic communication service provider. The Bank is not responsible for the availability and functionality of such services, for the transmission of data via these services between the Service Provider and the User's Mobile Device, or vice versa, nor for the storage and archiving of data on the User's Mobile Device.

3. Choice of Payment Brand and Payment Application (Co-badging)

The Bank has the right to include two or more different payment brands or payment applications on a payment instrument based on a payment card. A payment instrument based on a payment card refers to any payment instrument, including a payment card, computer, mobile phone, or any other technical device containing a payment application, that enables the payer to initiate a payment transaction based on a payment card.

The Bank is obligated to provide the consumer, within a reasonable time before concluding the payment services agreement, with clear and objective information on the payment brands associated with the service, including their features, applicability, fees, and protection measures.

4. Confirmation of Availability of Funds

The Bank managing the User's account is obliged to immediately, upon receiving a request from the payment services provider that issued the payment instrument based on a payment card, confirm whether there are sufficient funds available in the User's payment account for the execution of the payment transaction based on the payment card, provided the following conditions are met:

1. the User's payment account can be accessed online at the time of receiving the request;
2. the User has given explicit consent to the Bank managing the account to respond to such requests from a specific payment service provider for the purpose of confirming the availability of a certain amount of funds for a payment transaction based on a payment card;
3. the consent referred to in item 2) above was given prior to the first such request.

The payment service provider issuing the payment instrument based on a payment card may submit a request referred to in paragraph 1 above if the following conditions are met:

1. the payer has explicitly consented to the submission of such a request;
2. the payer has initiated a payment transaction in the amount referred to in paragraph 1 using a payment instrument based on a payment card;

3. the payment service provider issuing the payment instrument based on a payment card authenticates itself before the payment service provider managing the account prior to each individual request and establishes secure communication and data exchange.

The response referred to in paragraph 1 above shall contain only 'yes' or 'no,' without indicating the account balance, and may not be stored or used for any purpose other than the execution of the payment transaction.

The Bank managing the User's account may not, based on the response referred to above, prevent the User from accessing the funds in their payment account.

The Bank managing the User's account must, at the User's request, inform the User of the payment service provider that submitted the request referred to in paragraph 1 above and of the response provided.

The provisions of paragraphs 1 to 5 of this article do not apply to payment instruments based on cards that store electronic money.

5. Authentication

The Bank is obligated to apply strong customer authentication in cases where the User:

1. accesses the payment account via the internet;

2. initiates an electronic payment transaction;

3. performs any activity via remote communication that may affect the risk of fraud or abuse in connection with the execution of a payment transaction.

If the payer initiates an electronic payment transaction remotely as per item 2) of paragraph 1, the Bank must apply strong customer authentication, which includes elements dynamically linking the transaction to a specific amount and payee.

In the cases referred to in paragraph 1 of this article, the Bank is required to establish appropriate security measures to protect the confidentiality and integrity of the User's personalized security credentials.

The provisions of paragraphs 2 and 3 of this Article shall also apply to payment transactions initiated through a payment initiation service provider.

The provisions of paragraphs 1 and 3 shall also apply to account information service providers.

The Bank managing the User's account is obligated to allow the payment initiation service provider and the account information service provider to comply with the authentication procedure made available to the User by the Bank in accordance with paragraphs 1 and 3 of this Article, and for the payment initiation service provider also in accordance with paragraph 2.

6. Conditions for Amendment, Supplement and Termination of the Agreement

6.1. Amendments and Supplements to the Agreement

All amendments to the Agreement must be made exclusively in writing and duly signed by both contracting parties, except for those that are in the User's favour and which may, under applicable law, be amended and applied immediately without the User's prior consent.

If the Bank proposes amendments and supplements to the provisions of the Agreement, it must deliver the proposed changes to the User in written form no later than two months prior to the proposed effective date in the case of entrepreneurs, or no later than 15 (fifteen) days prior to the proposed effective date in the case of legal entities. The User may accept or reject the proposal before the proposed effective date.

By way of exception to the above paragraph, if the Bank proposes a change in the fees for payment services in favour of the User or introduces a new free service or functionality of an existing service, such change may be applied immediately without prior delivery of the proposed amendments to the User in the relevant section of the Framework Agreement.

The User shall be deemed to have agreed to the proposed amendments and supplements to the Agreement if they do not notify the Bank of their disagreement prior to the effective date. The Bank is obligated to inform the User of this in a clear and conspicuous manner when delivering the proposed amendments.

At the same time as delivering the proposed amendments, the Bank must inform the User of their right to terminate the Framework Agreement without charge or other costs at any time before the proposed effective date and specify the date from which such termination will take effect.

6.2. Conditions for Unilateral Termination, Nullity of Provisions

The User has the right to terminate the Agreement at any time with a 30 (thirty) day notice period, without charge.

The User may also terminate the Agreement in other cases prescribed by the law governing obligations or any other applicable law, by submitting a request to close the account in

the format determined by the Bank. In such cases, the Bank must immediately, or after the settlement of obligations on the account, enable the User to withdraw the total amount of funds in cash or transfer the funds to another bank without charge and close the account.

In the event of termination of the Agreement, the User is obliged to pay the Bank only for the payment services rendered up to the day of termination. If such fees were paid in advance, the Bank must refund the proportional amount of the prepaid fees.

The User may request that any provisions of the Agreement that contradict the information provided during the pre-contractual phase in accordance with the Law, or provisions concerning information on mandatory elements of the Agreement which were not previously disclosed, be declared null and void.

The Bank has the right to terminate the Agreement with a notice period of 2 (two) months, as well as in other cases prescribed by the law governing obligations or other applicable regulations, by delivering written notice to the other contracting party.

In addition to the above, the Bank may unilaterally terminate the Agreement and close the User's accounts in the following cases:

- If it is determined that the User is listed on official terrorist or other negative watchlists, in accordance with domestic and international anti-money laundering and counter-terrorism financing regulations;
- If the User fails to provide requested data about themselves, authorized persons on their current or other payment accounts, additional card users, source of funds, or the nature/purpose of the business relationship or specific transaction within a reasonable time set by the Bank;
- If the User's account remains inactive for 12 (twelve) consecutive months, meaning no incoming or outgoing payments, excluding postings of interest, fees, or charges, or other postings initiated by the Bank itself. This does not apply to basic payment accounts.

The Bank may unilaterally terminate the basic payment account agreement if at least one of the following conditions is met:

1. The User used the account for unlawful purposes;
2. No payment transaction has been executed from the account for more than 24 consecutive months;
3. The User obtained the right to a basic payment account based on inaccurate information;
4. The User has subsequently opened another payment account;
5. The User no longer has legal residence in the Republic of Serbia.

If the Bank terminates the basic payment account agreement due to conditions under items 2), 4), or 5), it must provide the User, free of charge, with a written notice of termination stating the reasons, no later than two months before the termination takes effect, unless such notice is prohibited by law.

If termination occurs due to conditions under items 1) or 3), the agreement shall be deemed terminated at the moment such conditions are confirmed. The Bank must inform the User in the notice of termination about their right to file a complaint and initiate alternative dispute resolution in accordance with applicable consumer protection laws.

6.3. Termination of Debit Card Usage

A User who no longer wishes to use a debit card must cancel the use of the card and return it to the Bank in the manner and within the deadline defined in the Agreement with the Bank.

The User has the right to cancel the use of an individual debit card by submitting a request to the Bank in a format prescribed by the Bank, indicating the date on which use of the card shall cease.

The User is obligated to return the card to the Bank along with the cancellation notice.

If the User does not cancel the use of the debit card at least 60 days prior to the expiry date and continues to use the card in accordance with this Annex and the Agreement, the Bank will automatically renew the right to use the debit card and issue a new one with a new validity period. The card's validity date is printed on the debit card itself.

If the User fails to comply with this Annex or the Agreement or acts in contravention of legal regulations, the Bank may terminate the debit card agreement and prohibit further use of all issued debit cards or block them.

In the event of cancellation or prohibition of debit card usage, the User must settle all obligations arising from the use of the debit card.

If the User cancels the use of a debit card that is processed, cleared, and settled for domestic payment transactions within the national payment system of the Republic of Serbia, this will automatically cancel the use of any debit card whose settlement is not performed within the Republic of Serbia. In this case, both debit card agreements shall be deemed terminated as of the date of cancellation of the debit card used for domestic payment transactions.

7. Transaction Protection

For the purpose of protecting and securing transactions, the User is informed that they may be recorded by a camera during card transactions (if such technical capabilities exist).

8. Confidentiality and Personal Data Protection Related to Payment Services

The Bank processes the User's personal data in accordance with the applicable Law on Personal Data Protection of the Republic of Serbia and the General Terms and Conditions of AikBank a.d.

The User's personal data is processed for the purpose of fulfilling the contractual relationship between the User and the Bank, for fulfilling the Bank's legal obligations, as well as for marketing purposes if the User has given explicit consent.

More detailed information on personal data processing, the data controller, the data protection officer, and the rights of data subjects is available in the General Terms and Conditions and the Privacy Notice, which are published on the Bank's website and available in all Bank branches, and are regularly updated.

The Bank and participants in the payment system may collect, process, and exchange data related to the payment service user, including personal data, as well as data on the payment transaction and the status and changes on the user's payment account, for the purpose of preventing, investigating, or detecting fraudulent actions or abuses related to payment services.

9. Entry into Force

This Annex 3 to the General Terms and Conditions enters into force on the date of its adoption and shall apply as of 6 May 2025.