AikBank

ANNEX 4

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

1. INTRODUCTORY PROVISIONS

These Special Terms and Conditions for the Use of Credit Cards for Entrepreneurs and Legal Entities govern the mutual rights and obligations between the Bank and payment service users – entrepreneurs and legal entities, in relation to the provision of payment services in accordance with the Law on Payment Services (hereinafter: the Law), as well as the terms under which the Bank provides credit card issuance and usage services, fees, interest rates, and foreign exchange rates, information on the methods and means of communication, and the terms for amending, supplementing, and terminating the Framework Agreement.

The Special Terms and Conditions for the Use of Credit Cards for Entrepreneurs and Legal Entities, together with the following documents:

- The Framework Agreement on the Issuance and Use of Credit Cards
- General Terms and Conditions of Aik Banka a.d. Beograd (hereinafter: GTC),
- The Bank's Price List for Services Provided to Legal Entities and Entrepreneurs (hereinafter: the Extract from the Price List),
- The Schedule of Receipt and Execution of Payment Transactions for Legal Entities and Entrepreneurs, which forms an annex to these Special Terms and Conditions (hereinafter: the Transactions Schedule),
- The Limits for the Use of Payment Instruments,
- The Mandatory Elements of the Agreement, where the User is an entrepreneur,

constitute the Framework Agreement (hereinafter: the Framework Agreement or the Agreement).

The terms used in these Special Terms and Conditions shall have the following meanings:

1. **User** means a private individual or legal entity that uses or has used a payment service as a payer and/or payee, or has contacted the Bank with the intention of using such services;
2. **Credit Card** is a payment instrument – a payment card issued by the Bank to the Cardholder for the use of a credit limit to purchase goods and services and/or withdraw cash;
3. **Credit Limit** means the total amount up to which the Cardholder (of the primary or additional credit card) may carry out transactions;
4. **Additional Credit Card** means a payment card issued by the Bank, at the request of the Cardholder, to a person designated by the Cardholder, and which is linked to the credit card account;
5. **PIN** means a personal identification number known only to the User, which is used by the User to authorize payment transactions, including when using the credit card at ATMs and POS terminals;
6. **Payment Transaction** means the deposit, transfer or withdrawal of funds initiated by the User as payer or as payee, or initiated on behalf of the payer, carried out regardless of the legal relationship between the payer and the payee;
7. **Remote Payment Transaction** is a payment transaction initiated via the internet or a device that can be used for remote communication;
8. **Payment Order** means an instruction from the User, as payer or payee, to the Bank requesting the execution of a payment transaction;
9. **Execution of a Money Remittance** is a payment service in which the payment service provider receives the payer's funds without opening a payment account for either the payer or the payee, solely for the purpose of making the funds available to the payee or transferring them to the payee's payment service provider, who makes them available to the payee;
10. **Initiation of a Payment Transaction** means undertaking actions that are a prerequisite for initiating the execution of a payment transaction, including issuing a payment order and conducting authentication;

11. **Payment Instrument** means any personalized device and/or set of procedures agreed upon between the User and the Bank and used to issue a payment order or to initiate a payment transaction;

12. **Payment Instrument Based on a Payment Card** means any payment instrument, including a payment card, computer, mobile phone or any other technical device containing a payment application, which enables the payer to initiate a payment transaction based on a payment card.

13. **Issuance of Payment Instruments** is a payment service in which the payment service provider issues a payment instrument to the payer, based on an agreement, for the purpose of initiating and processing payment transactions with that provider.

14. **Payment Brand** means any material or digital name, expression, designation, symbol, or combination thereof that identifies the card payment system within which a payment transaction is executed based on a payment card.

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

16. **Acceptance of Payment Transactions** is a payment service under which, based on an agreement between the payment service provider and the payee regarding the acceptance and processing of payment transactions, the transfer of funds is made to the payee.

17. **Payment Initiation** is a service under which, at the request of the payment service user, a payment order is issued debiting the payer's payment account held with another payment service provider.

18. **Payment Initiation Service Provider** is a payment service provider that performs a service under which, at the request of the payment service user, a payment order is issued debiting the payer's payment account held with another payment service provider.

19. **Account Information Service Provider** is a payment service provider that provides, via the internet, aggregated information about one or more payment accounts held by the payment service user with another or multiple payment service providers.

20. **Payer** means a private individual or legal entity who issues a payment order debiting their payment account or gives consent for the execution of a payment transaction based on a payment order issued by the payee; if no payment account exists – a private individual or legal entity who issues a payment order.

21. **Payee** means a private individual or legal entity designated as the recipient of funds that are the subject of a payment transaction.

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

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

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

25. **Sensitive Payment Data** means any data, including personalized security credentials, that can be used to execute fraudulent actions; however, in the context of payment initiation and account information service providers, the account holder's name and account number do not constitute sensitive payment data.

26. **POS Terminal** means a device installed at a point of sale or service counter of the payment service provider, enabling the use of payment cards, where transaction information is recorded electronically (EFTPOS).

27. **ATM (Automated Teller Machine)** means an electromechanical device that enables cardholders to deposit and/or withdraw cash, and/or use other services (funds transfer, balance inquiry, etc.).

28. **Reference Exchange Rate** means the rate used for currency conversion, which is made available by the Bank or sourced from a publicly available reference (e.g., the official middle exchange rate of the National Bank of Serbia).

29. **Durable Medium** means any medium that allows the User to store data addressed to them, access it for future reference, and reproduce it in an unaltered form for a period of time adequate for the purpose of the information.

30. **Domestic Payment Transaction** means a payment transaction in which both the payer's and the payee's payment service providers offer the service within the territory of the Republic of Serbia.

31. **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 a transaction where the same payment service provider renders the service for one user in Serbia and for the same or another user in a third country. Dinar-denominated transactions between residents and non-residents and between non-residents are considered international payment transactions.

For the purpose of these General Terms and Conditions, a domestic transaction executed in a foreign currency is also deemed an international payment transaction. The Bank does not execute international payment transactions in virtual currencies.

32. **Virtual Currency** is a type of digital asset that is neither issued nor guaranteed by a central bank or other public authority, is not necessarily tied to a legally established currency, and does not have the legal status of money or currency, but is accepted by private individuals or legal entities as a medium of exchange and may be bought, sold, exchanged, transferred, and stored electronically.

33. **3D Secure Service** means a service provided by the Bank to the User when making payments with a payment card on websites of merchants participating in the Mastercard SecureCode and/or Verified by Visa programs, which provides additional protection against unauthorized card usage during internet transactions.

34. **One-Time Password (OTP)** means a one-time numeric code created by the User when making a payment on 3D Secure online merchant sites.

35. **Transaction Date** is the date on which the Cardholder initiated or gave consent for the execution of the payment transaction.

36. **Value Date** is the date on which the Bank debits the User's credit card account in connection with the execution of the payment transaction.

37. **Monthly Statement** is a written summary of expenditures made with the primary and additional cards, including interest, fees, payments made, total debt, the minimum monthly payment due, the statement date, and the due date.

38. **Billing Period** means the period between two consecutive statement dates.

39. **Due Date** means the date by which the Primary Cardholder is required to settle the due obligation, i.e., the minimum monthly payment or installment due.

40. **Standing Order** is a payment service for the execution of a recurring payment order – an instruction by which the Cardholder gives prior consent to the Bank to debit their current account held with the Bank for the amount of due obligations arising from the credit card issuance and usage agreement.

41. **Slip** means a receipt confirming that a payment card transaction has been executed.

42. **Point of Sale** means a merchant's location at which credit cards must be accepted as a means of cashless payment for goods and services.

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

44. **Cash Disbursement Point** means a location at which a business entity is authorized to accept a credit card for the purpose of providing cash disbursement via a POS terminal.

45. **Digital Wallet** means a mobile payment application solution provided by a digital wallet service provider, which allows the User to register data related to one or more payment cards within the application and thereby tokenize the card(s) for the purpose of initiating payment transactions. In addition to the contractual relationship with the Bank, the terms and conditions for the use of the digital wallet are agreed upon separately between the User and the service provider, particularly with regard to the type and specifications of the mobile device on which the digital wallet application can be contracted and installed. The User may consult the Bank's website to find out in which digital wallets they can add one or more credit cards issued by the Bank.

46. **Digitized Card** means the digital representation of a credit card within the Digital Wallet and/or within the Bank's electronic and mobile banking applications, which enables the User to perform contactless payment transactions at points of sale, cash disbursement locations, and ATMs that support short-range wireless data transmission between two devices and/or at online points of sale that support such payment methods. The Bank, as the card issuer, determines the types of cards that may be digitized.

47. **Mobile Device** means a device on which the Digital Wallet contracted by the User with the Digital Wallet Service Provider has been installed.

48. **Digital Wallet Service Provider (Service Provider)** means a legal entity that provides the Digital Wallet service within which, based on a cooperation agreement between the Bank and the Service Provider, the Bank enables the User to register one or more credit cards issued by the Bank.

49. **End User** means a third party in whose favour, and at the request of the User, the Bank issues a card.

2. Terms of Use for Credit Cards

Based on the User's submitted request, the Bank issues a card in favour of a third party (hereinafter: the End User), which remains the property of the Bank, is issued in the name of the End User, and is non-transferable. The End User is obligated to use the card in accordance with applicable law and exclusively for the purchase and payment of goods and services not prohibited under current regulations, as well as for cash withdrawals at ATMs.

The User shall inform the End User of the obligations and rights defined in the Agreement, the General Terms and Conditions, and these Special Terms and Conditions.

Upon approval of the request, the Bank issues the card to the End User based on the written consent of the User.

The Bank may deliver the credit card and personal identification number (PIN) to the User either at a Bank branch or by mail to the User's address, provided that technical conditions allow for such delivery. In the case of delivery to the User's address, the Bank bears the risk related to the delivery of the card and the PIN; however, the User assumes the risk of failed delivery if they have not provided an accurate address to the Bank or have failed to notify the Bank in a timely manner of any address change.

Correspondence between the Bank and the User is conducted via monthly statements, SMS, email, mail, and push notifications, in accordance with technical capabilities.

Upon receipt of the card, the End User is obliged to immediately sign it in the designated area on the back of the card. The card remains the property of the Bank and may be used only by the End User, while any use by other persons is strictly prohibited. The Bank assumes no liability for any damage resulting from the use of the card by unauthorized persons.

Each card remains valid until the end of the month indicated on the card. The card may be used domestically and abroad for payment of goods and services and for cash withdrawals at points of sale, ATMs, and bank counters that visibly display the logo of the card organization.

Pursuant to paragraph 2 of this Article, the Bank may issue a card to a third party, which is issued in accordance with this Annex of the General Terms and Conditions. Transactions made by End Users shall be debited from the User's card account.

The use of the credit card is permitted within specific daily limits prescribed by the Bank, which form an integral part of the agreement on the issuance and use of credit cards for legal entities and entrepreneurs.

The Bank charges the User fees for services rendered, in accordance with the Price List of AikBank AD Beograd, as determined by the Bank's internal acts (hereinafter: the Price List). The Bank reserves the right to grant the User more favourable fees than those defined in the Price List.

3. Repayment of Outstanding Balance

The User is obliged to settle the outstanding balance or the minimum payment within the deadline specified in the monthly statement, in full, by the date indicated as the payment due date.

Payments made by the User shall first be applied to all due fees and charges, followed by any accrued interest, if applicable, and finally to the principal amount due.

4. Delivery of Documents

The User accepts that monthly statements and extracts from the Bank's accounting records maintained in its IT system constitute valid proof of the User's obligations incurred through card usage.

It is explicitly agreed that voluntary and full repayment of the debt by the User, based on the monthly statement, shall be considered unconditional acceptance of the contents of the statement and the amount of debt incurred through the ownership and use of the card, all in accordance with the information contained in the statement.

The data of each transaction performed with the card is recorded in the Bank's systems and will be stated on the slips issued at the point of sale or ATM. These slips shall be considered valid proof of the executed transactions.

5. Terms of Use of Payment Services

5.1. Personalized Security Element

The Bank issues the User a personalized security element (personal identification number), which is a numeric combination (hereinafter: PIN) used for the authentication of the User when using the credit card.

Upon approval of the request, the PIN code is delivered to the User/End User and may be used only in conjunction with the card for the purpose of conducting transactions, as regulated by these Special Terms and Conditions.

The PIN code, considered the electronic signature of the End User, is generated under conditions ensuring complete data confidentiality. The End User is obligated to memorize the PIN code and further undertakes not to store it in written form near the card.

For security purposes, the End User is required to keep the card and personal identification number (PIN), as well as other personalized elements (card number, expiration date, security code on the back of the card, name on the card, and account number), separate and handle them responsibly.

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

The End User is obliged, immediately upon receiving the card and PIN, to take all reasonable measures to protect them, to safeguard the card and the confidentiality of the PIN and other personalized security elements of the card, and to take all necessary actions to prevent the card and/or PIN code and/or other personalized security elements from being accessed by third parties, as well as to prevent unauthorized access, theft, or misuse thereof.

If the End User believes their PIN code is no longer confidential, they are advised to immediately change their PIN at an ATM. If the End User is unable to change the PIN code, they are advised to immediately contact the Bank and block the card.

When changing the PIN code, the End User is advised not to choose easily guessable numbers (e.g., parts of birth dates, postal codes, first four digits of a phone number, etc.).

In the event of card usage for transactions where the card is not physically present, the End User is required to take basic precautionary measures, which include the following:

- Not sending sensitive card information or other personalized security elements via email, SMS, telephone, fax, or any other communication channels;
- For such transactions, only three pieces of information are typically required – card number, expiration date, and security code;
- It is recommended to use only verified and trusted websites.

The End User is obligated to immediately notify the Bank or a designated party of any loss, theft, or misuse of the credit card.

The User is obligated to notify the Bank of any unauthorized, unexecuted, or incorrectly executed payment transaction.

The User is also required to notify the Bank, in writing and without delay, of any circumstances that may hinder the fulfillment of their obligations under the Agreement.

5.2. Form and Method of Granting and Revoking Consent for the Issuance of Payment Orders or Execution of Payment Transactions

The Bank shall execute a payment transaction only if the End User has given consent for its execution.

It is deemed that the End User has given consent for the execution of a payment transaction if, during the transaction, validation of the card data or personalized security elements has been performed by one of the following methods:

- Reading the chip or contactless reading of the chip and entering the PIN on the POS terminal, or on certain POS terminals with or without a signed slip;
- Contactless reading of the card chip without entering the PIN at the merchant's point of sale or ATM;
- Signing a slip when using the magnetic stripe;
- In the case of payment transactions where the card is not physically present (e.g., internet transactions), by entering the required security elements (card number, expiration date, CVV/CVC code, and one-time password (OTP));
- Using the Digital Wallet in the manner described in item 2 of this Annex.

The PIN entered during the execution of the transaction and confirmed as correct is considered the End User's electronic signature for that transaction.

A payment transaction for which the End User has given consent in one of the ways described above shall be considered an authorized payment transaction.

The End User must give consent for the execution of a payment transaction prior to its execution.

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

If the End User does not provide consent for the execution of the payment transaction in the form and manner stipulated by the Agreement and this Annex, the payment transaction shall be deemed unauthorized.

The Bank may refuse to execute a payment order if the conditions under this article are not met, or if so provided by applicable regulations, or if the Bank has reasonable doubts regarding the authenticity of the payment order or any of its elements, or if the Bank suspects card misuse. In such cases, the Bank shall inform the User of the refusal to execute the payment order or initiate the payment transaction (orally, via slip, email, or SMS, using the communication channel selected in the credit card issuance request), including the reasons for the refusal and instructions for correcting the issue that led to the refusal, within the timeframe set for the execution of the payment transaction—unless such notification is prohibited by law.

5.3. Transactions Executed at Points of Sale

The End User may, depending on the type of card, use it domestically and/or abroad to pay for goods and services at points of sale that accept cards bearing the visibly displayed logo of the card organization.

The Bank provides credit to the User by making payments on behalf of the User to the merchant at the point of sale for the amount specified on the slip, provided that such amounts remain within the approved credit limit. The Bank shall not be liable for any obligations arising from transactions exceeding the credit limit for which a slip was issued, nor for any payment obligations resulting from such transactions.

The End User receives a copy of the slip issued in connection with such transactions. The card is merely a technical tool for making payments. Under no circumstances shall the Bank be liable for any errors, omissions, or improperly executed transactions by the point of sale with regard to transactions made by the End User, nor for any complaints and/or claims that may arise in connection with transactions carried out at points of sale.

Complaints regarding the quality of goods and services paid for with the card must be submitted exclusively to the point of sale where the transaction occurred (the merchant). The Bank is

not responsible for the accuracy or quality of goods and services paid for using the card.

5.4. Transactions Conducted via ATMs (Automated Teller Machines)

The Bank's services are available to the End User via ATMs, depending on the technical capabilities of the device. These services primarily include cash withdrawals, PIN changes, and account balance inquiries. The End User may withdraw cash at ATMs displaying the relevant card symbol and/or logo by using the card and entering the PIN (chip read and PIN entry).

Only amounts composed of whole divisible numbers in dinars (RSD) (or other currencies if the card is used abroad) may be withdrawn using the card, up to the credit limit approved by the Bank. The withdrawn amount and the User's debt must not exceed the credit limit established by the Bank in accordance with Article 5.6 of this Annex.

The ATM will, upon the End User's request, issue a receipt for each executed transaction, confirming the instructions given by the End User. If a receipt is not issued due to a technical error of the ATM, the End User may contact the Bank's Customer Service Center using the phone numbers listed on the back of the card.

The Bank may, at any time, block ATM transactions to protect the interests of the Cardholder or in the event of a breach of the General Terms and Conditions, with notification provided to the User in accordance with this Annex.

The Bank may suspend the operation of any ATM, temporarily or permanently, without prior notice.

5.5. Time of Receipt of a Payment Order and Deadline for Execution of Payment Services or Individual Payment Transactions

The time of receipt of a payment order is the moment when the User has given consent for the execution of the payment transaction, i.e., when the Bank has carried out the authentication process.

A business day of the Bank is any working day except: Saturday, Sunday, public holidays, and non-working days (in accordance with the applicable regulations of the Republic of Serbia).

Transactions initiated with a credit card on POS terminals or ATMs of the Bank, or on third-party networks, will be executed immediately. Posting and settlement with the merchant will depend on whether the transaction was initiated during or outside the Bank's business day.

5.6. Credit Limit

End Users may use funds up to the approved credit limit determined by the Bank and defined in the Agreement with the User. Transactions executed by the End User with the card must not exceed the maximum limit, referred to herein as the credit limit.

Within the credit limit, the Bank may establish a maximum monthly amount of available funds (for payments and cash withdrawals) upon the User's request.

The Bank reserves the right to reduce the amount of the credit limit, taking into consideration the User's current financial situation, creditworthiness, compliance with the provisions of this Annex and the General Terms and Conditions, as well as the overall risk. The User will be notified of any new credit limit via the monthly statement.

If the User exceeds the approved credit limit, the Bank shall charge a fee in accordance with the Price List.

During the validity period of the agreement on the issuance and use of the credit card, the Bank may increase the approved credit limit if the User's creditworthiness improves and if the User duly fulfills their obligations under the credit card agreement and other Bank products (e.g., loans, overdrafts, etc.).

The Bank will notify the User in writing of the increased credit limit and the date from which the new limit may be used, via the monthly statement. The User may state their refusal of the change within 15 days, or 60 days in the case of entrepreneurs.

If the User does not accept the increased credit limit, they may notify the Bank within 15 (fifteen) days from the statement date, in which case the card(s) shall continue to be used under the previously applicable credit limit.

The User may inform the Bank of their decision not to accept the change (limit increase) verbally by calling the Bank's Contact Center, by email at kontakt.centar@aikbank.rs, in person at the nearest Bank branch, or in writing to the Bank's registered address.

6. Transaction Limits for Credit Card Use

The Bank determines daily spending and cash withdrawal limits, as well as the maximum number of daily transactions. These are published on the Bank's website and displayed in the Bank's business premises, within the document titled *Limits for the Use of Payment Instruments*.

Upon the User's written request, the Bank may approve changes to these limits, either increases or decreases.

The Bank reserves the right to amend the limit amounts. The User will be notified in advance of any new limit.

7. Information and Data on Fees, Interest Rates, and Currency Exchange Rates

7.1. Currency Exchange Rate

The Bank executes payment orders in the currency and currency code in which they are denominated. Transactions initiated using a credit card within the country are calculated in dinars and debited from the User's card account up to the available credit limit. Transactions initiated using a credit card

in a foreign currency are debited from the User's card account in dinar equivalent, at the Bank's selling exchange rate on the date the transaction is posted. The country of transaction execution is considered to be the country in which the payee is registered in the card scheme system.

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

7.2. Fees

The amount of fees for performing payment services and executing other payment transactions is available on the Bank's website and in its business premises.

At the time of signing the Application, the User is informed of the Bank's Price List, which forms an integral part of the Framework Agreement, and is informed of the types and amounts of fees charged by the Bank. Fees are charged by directly debiting the credit card account.

The Bank has the right to amend the amounts of fees and other charges or introduce new ones, of which the User will be notified in accordance with the provisions governing amendments to the Agreement.

The type and amount of fees for services provided by the Bank to the User, including those related to the method and frequency of providing or making available information in accordance with the Law, are defined in the agreement with the User, in accordance with the applicable Bank Price List.

Fees are determined as a fixed amount, as a nominal value and/or as a percentage of the transaction amount.

In the case of partial or delayed payment of the minimum monthly amount by the due date indicated in the monthly statement, the User will be charged a fee for sending a written reminder, in accordance with the Price List.

7.3. Interest

The Bank calculates and charges interest on the utilized portion of the credit limit at the nominal interest rate specified for each individual type of credit card in the Agreement on the Issuance and Use of Credit Cards concluded between the User and the Bank.

Interest on purchase transactions is calculated from the date the transaction is posted until the date the debt is settled. For cash withdrawal transactions, interest is calculated from the date of execution (for transactions conducted on the Bank's ATM network) or from the posting date (for transactions conducted on other banks' networks) until the date the debt is settled.

If the total amount of purchases and charges from the previous month is paid in full by the due date, no interest shall be charged on the purchase transactions referred to in paragraph 1 of this Article, unless otherwise agreed.

The Bank applies the proportional interest calculation method based on a 360-day year, unless otherwise agreed.

The outstanding balance is reduced with each payment made by the User, in the following order: due fees, default interest, regular interest, purchase transactions, and finally, cash withdrawal transactions.

For due and unpaid claims, the Bank charges statutory default interest from the moment they become due. If the agreed interest rate is higher than the statutory default rate, the agreed interest rate shall apply. The statutory default interest rate is variable and is published by the National Bank of Serbia on its website, becoming effective the day after publication.

The Bank does not calculate contractual interest on fees or previously calculated interest from a prior billing period. Interest is calculated only on the amount of the executed transaction, i.e., the purchase or cash withdrawal amount, and on due but unpaid instalments.

The Bank is authorized to amend the interest rate during the term of the Agreement. Such changes may be applied immediately and without prior notice to the User if based on changes to the agreed reference interest rate.

If the interest rate is changed in favour of the User, such changes may also be applied immediately and without prior notice.

8. Information on the Means and Methods of Communication between the User and the Bank

8.1. Notifications

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

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

- **Verbally** – by visiting a Bank branch or calling the Bank's Contact Center
- **In writing** – notifications, letters, and other written correspondence
- **Electronically** – including the Bank's website, chat, email, electronic and mobile banking applications (and their in-app or push message options depending on technical capabilities), communication via applications and social networks such as Viber, WhatsApp, Facebook, etc., SMS messages, and other applications that allow for direct communication with the User, or any other application-based solutions made available by the Bank in accordance with technical capabilities.

If the User provides the Bank with an email address, the Bank may use that address to deliver, among other things, the following:

- Reports on charged fees, in accordance with the Law on Payment Services
- Notifications regarding variable interest rates on credit cards
- Monthly credit card statements
- Records of transactions, as well as any other notifications relating to all currently used and newly introduced products, in accordance with applicable legal regulations and contractual provisions
- Other legally required notices

Delivery by the aforementioned means is considered to fulfill the Bank's legal and contractual notification obligations.

The User is obliged to promptly inform the Bank of any changes to their address, email address, or phone number. If the User fails to comply with this obligation, any documents sent by the Bank to the last known address, email, or phone number stated in the application shall be deemed properly delivered.

By signing the application in the designated space, 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 arising from the Agreement shall be conducted in the **Serbian language**. This does not exclude the possibility of using other languages, in line with good banking practices.

The Bank is authorized to use all contact details provided by the User at the beginning of the business relationship or later during its course (e.g., mobile phone number, email address, phone number, postal address, etc.). In addition to the selected communication channel, the Bank may notify the User via phone, SMS, electronic or mobile banking, voice assistants, email, or other electronic channels that allow direct communication with the User (e.g., applications and social networks such as Viber, WhatsApp, Facebook, push and in-app messages, etc.), or via chat and online portals made available by the Bank. The Bank may use one or a combination of these communication methods.

The User may indicate their preferred communication method with the Bank and/or request a change to it by notifying the Bank in a way that allows their identity to be reliably confirmed (e.g., sending an email from the registered email address, sending an SMS from the registered mobile number, calling the Contact Center from the registered phone number, visiting a branch in person, or using electronic/mobile banking apps or communication applications like Viber, WhatsApp, etc.).

The Bank guarantees the confidentiality of data in accordance with the Law on Banks and will use the data only for the stated purposes. In the event that the User is unable to receive notifications due to their own fault (e.g., unpaid bills to the provider, provider system errors, 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 the Bank's communication addresses, can be found on the Bank's website.

The User has the right to receive one copy of the Agreement in written form or on another durable medium, and during the contractual relationship, the User may request copies of the Agreement and pre-contractual information deemed as mandatory elements of the Agreement, in a format that enables the User to review the terms related to the provision of payment services, compare offers from different service providers, and assess whether these terms and services meet their needs.

Any notification, request, or reminder regarding payment obligations issued by the Bank, including those related to an additional card, will be sent to the Primary Cardholder at the address provided in the card issuance application or the updated address if the User has submitted a change of address in writing.

It is explicitly agreed that the last reported address by the User shall be deemed the valid and irrevocable legal address for all purposes, including delivery of notifications and documentation.

Any request, notification, card return, or potential claim by the User in connection with the use of the card shall be submitted to the Bank using the addresses and phone numbers provided in the Bank's informational brochures or monthly statements.

8.2. Receipt of Information by the User

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

- If posted in the electronic or mobile banking application – on the day of posting
- If sent by email – on the day the email was sent
- If sent by postal mail – on the day it was handed over to the postal service or a registered delivery service
- If sent by SMS – on the day the SMS was sent
- If sent via another electronic communication channel or tool allowing individual communication with the User (e.g., Viber, WhatsApp, push message, etc.) – on the day the message was sent

The Bank is not liable for delivery or functionality of electronic communication channels that are not part of the Bank's information system and that the User has selected (e.g., when the User's antivirus program blocks emails sent from the Bank's email address, etc.).

The User is responsible for ensuring all technical and other prerequisites for the functioning of the selected electronic communication channels (e.g., that the provided email address is active, that the Bank is not blocked as an SMS or Viber sender, that push notifications are enabled in the mobile banking app, etc.).

8.3. Additional Services and Special Use of Provided Contact Information

The Bank may enable the User to access and use additional services where the provided contact information is used during the identification or authorization process—either independently or in combination with other identification or authorization methods—based on user instructions for these services, including:

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

8.4. Monthly Statements

Each month, free of charge, the Bank sends the User a statement of indebtedness and credit card account balance—referred to herein as the *monthly statement*—by post or email. The statement is generated based on the Bank's accounting records and includes all transactions made with the card, as well as any other accounting entries on the card account, including:
a) All transactions executed using the card (purchases of goods and payment for services, cash withdrawals);
b) Fees charged by the Bank for card usage (membership fees, cash withdrawal fees, and other fees prescribed in the Price List);
c) All payments made by the User;
d) Dates of execution and posting of the listed transactions;
e) The balance from the previous monthly statement;
f) The new balance, including associated fees;
g) Interest;
h) Payment due date;
i) Credit limit;
j) Nominal interest rate; and
k) Date of the billing period.

Transactions that, for any reason, were not recorded in the current monthly statement will be recorded in the next one.

9. Information on Protective and Other Measures Regarding the Execution of Payment Transactions

9.1. Procedure in the Event of Loss, Theft, or Misuse of the Credit Card

The User is obligated to notify the Bank or an entity designated by the Bank immediately upon becoming aware of the loss, theft, or misuse of the card. In the event of theft or misuse, it is recommended that the User also report the incident to the Ministry of the Interior.

If the report is made by phone, it will be electronically recorded, and the Bank is obliged to block further use of the card. The User shall bear any material damage incurred due to the loss, theft, or misuse of the card up until the time the loss, theft, or misuse is reported. If the User finds the card after reporting it lost, stolen, or misused, they must not use it and must return it to the Bank without delay.

The User is required to notify the Bank immediately upon receiving a message about a transaction they do not recognize, as well as in the event of loss or theft, by calling the Bank's Contact Center or visiting a Bank branch, and must initiate a block on their credit card.

In case of a damaged card or if the card is lost/stolen, the User is obligated to submit a request at a Bank branch for the issuance of a new card to replace the damaged one.

When signing the request for a new card, the User must return the damaged card to the Bank.

If the Bank does not enable the User to report the loss, theft, or unauthorized transaction at any time, the User shall not be held liable for any consequences of unauthorized use—unless the User themselves committed the misuse.

9.2. Bank's Right to Block the Credit Card

The Bank may disable the use of the card if there are justified reasons relating to the security of the card, if there is suspicion of unauthorized use or fraudulent use of the card, or if there is an increased risk that the User will not be able to fulfill their payment obligations. This also applies in accordance with the applicable laws of the Republic of Serbia when the card is linked to a credit facility or an approved overdraft.

The Bank is obligated to inform the User of its intent to block the card and the reasons for doing so, prior to the block—or at the latest, immediately after the block—via SMS, email, written notice, or another durable medium.

The Bank shall re-enable the use of the card or replace it with a new one once the reasons for the block no longer exist.

The Bank may also block the payment card if there are justified reasons related to card security, suspicion of unauthorized or fraudulent use, or a violation of applicable laws or regulations by the Client or a third party.

The Bank is additionally authorized to block the card and all associated services if any of the following circumstances occur or are suspected to have occurred:

- If it is established in appropriate proceedings that the User/End User was involved in fraud or misuse of the card;
- If the User fails to settle due monetary obligations under the card within the deadlines set out in the Agreement;
- If it is determined that the card was approved based on inaccurate, false, or forged data that were material to the Bank's decision to issue the card, and which were discovered after the conclusion of the Credit Card Agreement;
- If the User/End User uses the card for purposes other than those described in the Credit Card Agreement;
- If the Bank activates any of the security instruments defined in the Agreement;
- In other cases provided for by law.

9.3. Payment Transactions Where the Transaction Amount Is Not Known in Advance

If a payment transaction based on a payment card is initiated by or through the payee, and the exact amount of the transaction is not known at the time the User gives consent to execute it, the Bank may not reserve funds on the User's account unless the User has given consent for a specific amount to be reserved.

The Bank is obligated to release the reservation of funds on the User's payment account without delay upon receiving information about the exact amount of the payment transaction, and no later than upon receipt of the payment order.

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

In the case of an unauthorized, unexecuted, or incorrectly executed payment transaction—and without prejudice to the obligations under Articles 5.1, 9.5, and 9.6 of these Special Terms and Conditions—the Bank is obligated, regardless of responsibility for proper execution, to promptly take appropriate measures to trace the payment transaction and provide the User with information on the outcome without delay.

The Bank may not charge the payer any fee for the actions taken under the previous paragraph.

The payment service user has the right to request compensation from their Bank or from the payment initiation service provider—if the transaction was initiated through such a provider—in accordance with the law, for any damage caused by the execution of an unauthorized, unexecuted, incorrectly executed, or delayed payment transaction for which the provider is responsible.

If the User claims that they did not authorize a transaction, or that it was not executed or was executed incorrectly, the Bank (for the portion of service it provided) is obligated to prove that the transaction was authenticated, accurately recorded, posted, and not affected by any technical malfunction or other deficiency.

If the transaction was initiated through a payment initiation service provider, the provider must prove that, in the portion of the service it provided, the transaction was authenticated, properly recorded, and unaffected by any technical malfunction or other deficiency.

A payment transaction is considered authenticated if the payment service provider, by applying appropriate procedures, has verified and confirmed the use of a specific payment instrument, including its personalized security elements.

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

In such cases, the Bank (or the payment initiation service provider, where applicable) is required to provide evidence that reasonably supports the claim that the User acted fraudulently or with intent or gross negligence.

9.5. User Liability for Unauthorized Payment Transactions

The User shall bear the loss resulting from unauthorized payment transactions up to the amount of RSD 3,000, if such transactions were made using:

1. a lost or stolen payment instrument, or
2. a payment instrument that was misused.

Exceptionally, the User shall bear all losses resulting from unauthorized payment transactions if such transactions were caused by fraudulent actions by the User, or by the User's failure to fulfil obligations to use the payment instrument in accordance with the prescribed or agreed terms of issuance and use, due to intent or gross negligence.

The User shall not bear losses in the following cases:

1. If the User could not have detected the loss, theft, or misuse of the payment instrument before the unauthorized transaction occurred, except in cases referred to in paragraph 2 above;
2. If the unauthorized transaction was caused by an action or omission by an employee, agent, or branch

of the payment service provider, or another entity to which the provider's activities were delegated—except in cases referred to in paragraph 2 above;

3. If the Bank did not ensure that the User could notify it, at any time and free of charge, of the loss, theft, or misuse of the payment instrument—unless the losses were caused by the User's fraudulent actions;
4. If the Bank did not require Strong Customer Authentication, unless the losses were caused by the User's fraudulent actions.

If the Bank requires strong authentication, and the payee or the payee's payment service provider fails to apply it, they shall be liable to compensate the Bank for any resulting damages.

The User shall not be liable for losses resulting from unauthorized transactions that occurred after the User has notified the Bank that the payment instrument was lost, stolen, or misused—unless such losses were caused by the User's fraudulent actions.

Exceptionally, 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 elements of the payment instrument and the circumstances under which the instrument was lost, stolen, or misused.

9.6. Bank's Liability for Unauthorized Payment Transactions

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

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

1. Provide justification to the User for denying the refund and report the fraud or misuse to the competent authority; or
2. Refund the transaction amount to the User if, after additional verification, the Bank concludes that the User did not commit fraud or misuse.

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

The Bank is also obligated to refund all fees charged to the User and to pay any interest the User would have been entitled to had the unauthorized transaction not occurred.

If the payment transaction was initiated via a payment initiation service provider, these provisions apply to the Bank in its capacity as the account servicing payment service provider.

9.7. Liability for Non-Execution, Incorrect Execution, or Delay of a Payment Transaction Initiated by the User (Payer)

If the payment transaction is initiated directly by the User, the Bank is liable to the User for its correct execution up to the payee's payment service provider.

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

In such cases, the value date for crediting the User's payment account must be no later than the date the account was debited for the incorrectly executed transaction.

If the Bank provides proof—either to the User or to the payee's payment service provider—that the payee's provider has received the transaction amount, the responsibility for execution lies with the payee's provider.

The payee's payment service provider must then ensure that the value date for crediting 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 transaction was executed after the legally prescribed time limit, the payee's payment service provider must, at the Bank's request (acting on behalf of the User), ensure the value date is no later than the business day the funds would have been credited under correct execution in accordance with the Law and these Special Terms.

If the Bank is liable for non-execution, incorrect execution, or delay, it is also obliged to refund all fees charged to the User and pay any interest to which the User is entitled in connection with the error.

If the User initiated the transaction through a payment initiation service provider, the Bank is considered the User's payment service provider for the purposes of paragraphs 1 to 4 and paragraph 6 of this Article.

In such cases, the payment initiation service provider must prove that it submitted the payment order to the Bank in accordance with Article 5.5 of these Special Terms, that the transaction was authenticated and properly recorded, and that no technical failure or deficiency occurred in the part of the

service for which it is responsible. It must provide this evidence to the Bank without delay upon request.

If the payment initiation service provider is responsible for the non-execution, incorrect execution, or delay, it must compensate the Bank immediately, upon request, for any loss or refund the Bank has paid to the User.

9.8. Liability for Non-Execution, Incorrect Execution, or Delay of a Payment Transaction Initiated by the Payee or by the User (Payer) via the Payee

If the payment transaction is initiated by the payee or by the User through the payee, the payee's payment service provider is liable to the payee for the correct submission of the payment order to the User's bank.

If the provider fails to submit or properly submit the payment order, it must—immediately upon discovering the issue—submit or resubmit the order to the User's bank.

If the payment order is submitted after the deadline agreed between the payee and their provider or the Bank, the payee's provider must ensure that the value date for crediting the payee's account is no later than the date on which the account would have been credited had the transaction been executed on time.

If the amount of a transaction initiated by the payee or by the payer via the payee is credited to the account of the payee's provider, that provider is responsible to the payee for the proper execution of the transaction.

If the payee's provider is found responsible, it must ensure that the value date for crediting the payee's account is no later than the business day on which the funds would have been credited under proper execution.

If the payee's provider can prove—to the payee and, if necessary, to the Bank—that it is not responsible under paragraphs 1–4 of this Article, then the Bank is liable to the User for the non-executed or incorrectly executed transaction.

In such cases, paragraphs 2 and 3 of Article 9.7 shall apply accordingly.

The Bank shall not be liable under the previous paragraph if it proves that the payee's provider received the funds, and there was only a minor delay in execution. In that case, the payee's provider must ensure that the value date for crediting the payee's account is no later than the date it would have been credited under proper execution.

The payment service provider liable under this Article must also refund to its payment service user all fees charged and pay any interest to which the user is entitled in connection with the non-executed or incorrectly executed transaction.

9.9. Notification or Request as a Condition for Refund or Proper Execution of a Payment Transaction

The Bank is obligated to provide a refund or ensure the proper execution of a payment transaction if the User notifies the Bank of an unauthorized, unexecuted, or incorrectly executed payment transaction—or requests correct execution of a payment transaction—immediately upon becoming aware of the transaction, provided that the notification or request is submitted no later than 13 months from the date of the debit.

If the Bank failed to provide the User with information about the payment transaction, it shall be liable for the unauthorized, unexecuted, or incorrectly executed payment transaction and must provide the User with a refund even after the 13-month period, provided that the User notified the Bank immediately after becoming aware of the transaction.

If the payment transaction referred to in paragraph 1 of this Article was initiated via a payment initiation service provider, the User shall request the refund from the Bank that holds their account.

9.10. Rights and Obligations of Payment Service Providers in the Case of Fraud, Misuse, or Certain Instances of Incorrectly Executed Payment Transactions

If the Bank receives a request for the refund of funds, accompanied by data, information, and documentation indicating that the payment transaction was likely the result of fraud or misuse, the payee's payment service provider shall be obligated not to credit those funds to the payee's account or to restrict access to those funds for a period of three business days from the date of receipt of the documentation.

If, during this three-day period, the payee's payment service provider subsequently receives from the Bank additional data, information, and documentation—including an official report submitted to the competent state authority—that together reasonably indicate the transaction was fraudulent or abusive, the payee's payment service provider must:

1. Immediately refund the funds to the User if the payee, within 15 business days of being notified, fails to prove or make it likely that the funds were lawfully obtained, or refuses to provide appropriate evidence;
2. Allow the payee to access the funds after 30 business days from the expiration of the period from paragraph 1 of this Article, if the payee has proven or made it likely that the funds were lawfully obtained, and the competent authority has not issued a decision prohibiting access to those funds.

The payee's payment service provider shall be liable to the payer for any loss resulting from a transaction referred to in paragraph 1 of this Article if it enabled the payee to access the funds in violation of paragraphs 1 and 2 and it is later determined that the payee committed or participated in the fraud or misuse.

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

1. Overpayment or duplicate execution: If the payer's payment service provider transfers an amount that exceeds the amount specified in the payment order or mistakenly executes the order multiple times, the payee's provider, upon receipt of evidence from the payer's provider acknowledging the error, must immediately return the excess funds.
2. Underpayment: If a smaller amount than specified in the payment order is transferred, the payer's provider may, on the same business day, transfer the difference to the payee's provider, without a request from the User for correct execution.
3. Incorrect payee: If the funds were transferred to an incorrect payee, the payer's provider may, on the same business day it received the order, correctly execute the payment transaction without a User's request, and the payee's provider that incorrectly received the funds must, upon receipt of evidence from the payer's provider, immediately return (transfer back) the funds.

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

9.11. Refund of the Amount of an Authorized and Correctly Executed Payment Transaction to the User

The Bank shall, at the User's request, refund the full amount of an authorized and correctly executed payment transaction (hereinafter: Refund Request) that was initiated by the payee or by the User through the payee, provided the following conditions are met:

1. The User gave consent for the execution of the payment transaction without the exact amount being specified in advance;
2. The amount of the payment transaction exceeds the amount the User could reasonably have expected, considering their previous spending patterns, the terms of the Agreement, and the specific circumstances of the case.

The Bank may request the User to provide evidence of the facts relevant to meeting the conditions referred to in paragraph 1 above. The User may not invoke the condition under item 2 if the increased amount of the transaction resulted from currency conversion using a reference exchange rate.

The User may submit a Refund Request within 56 (fifty-six) days from the debit date, and the Bank is required to either refund the full transaction amount or inform the User of the reasons for refusing the request within 10 (ten) business days from the day the request is received. The value date for crediting the User's payment account shall be no later than the date on which the account was debited for the relevant transaction.

If the Bank denies the Refund Request, it must inform the User of the reasons for the refusal and of the available procedures for the protection of their rights and interests, including out-of-court dispute resolution procedures, and the options for initiating proceedings due to a violation of the Law on Payment Services and the competent authority for such proceedings.

The User shall not be entitled to a refund of the payment transaction referred to in paragraph 1 if the following conditions are met:

1. The User directly gave the Bank consent for the execution of the payment transaction;
2. The Bank or the payee provided the payer, at least 28 (twenty-eight) days before the due date, with information about the future payment transaction in the agreed manner.

9.12. 3D Secure Protection

To provide additional security to the User when making payments online, the Bank's payment cards may support online transactions in a 3D Secure environment. If the website supports 3D Secure protection, the Bank may require additional user authentication through a one-time password (OTP – One Time Password).

10. Digital Wallet

The rules and conditions for executing cashless payment transactions using the Digital Wallet functionality are defined in these Special Terms and in the Rules and Conditions of Aik Bank for using this functionality, which form an integral part of the Framework Agreement for the issuance and use of payment cards.

10.1. Digital Wallet Activation, Use, and Execution of Payment Transactions with a Digitalized Card

The User concludes a Digital Wallet service agreement directly with the Service Provider. The Bank is not a party to this agreement, does not assume, nor can it assume, any rights or obligations arising from it, and is not responsible for the availability or functioning of the service.

The User may register their eligible credit card in the Digital Wallet either through the Service Provider's application or through the Bank's mobile banking application, if enabled by the Bank. By registering a credit card in the Digital Wallet, a digitalized card is created, to which all terms and conditions applicable to the physical credit card (of which it is the digital equivalent) apply, in accordance with the Framework Agreement concluded between the User and the Bank.

If the User has multiple cards registered in the Digital Wallet, they may independently select which card will be used to initiate the payment transaction.

Consent for executing payment transactions initiated through the Digital Wallet is given by presenting the mobile device to a POS terminal or ATM, or by selecting the Digital Wallet payment option on an online point of sale and entering personalized security elements chosen or contracted with the Service Provider. The Bank will debit the User's credit card for the amount of such executed payment transactions.

Information regarding transactions executed through the Digital Wallet may be obtained by the User from both the Bank and the Service Provider.

It is not possible to make instalment payments using the digitalized card at the partner network.

10.2. Conditions for Using Digital Wallet Services

The digital wallet service is free of charge. Fees and costs incurred by the User in connection with transactions are governed by the Framework Agreement and the agreement for issuing the respective Card.

To add a Card to the digital wallet on their mobile device, the User must have previously registered the mobile phone number used on that device with the Bank. If the User has not registered their mobile number with the Bank, the Bank reserves the right to further identify the User or to reject the registration. A User may add one Card to a maximum of nine devices.

The service provider will enable payments using the digital wallet on the User's mobile device. The digital wallet service allows Users to register their Card in the application and manage a token. A token is a surrogate for the Card, created when the Card is registered in the digital wallet application on a mobile device.

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

Once the Card is saved in the digital wallet application, the User may securely make payments in stores, in mobile apps, and on web locations that support the service provider's application and accept the Bank's payment cards.

The User provides consent for payment transactions by presenting the device with the digital wallet application to the POS terminal and, if necessary, authenticating themselves in a manner previously agreed with the Service Provider.

The service allows Users to register their payment Card in the digital wallet application and manage the token. The token is created when the Card is registered and saved in the digital wallet application and enables secure payments at retail locations that support NFC technology and 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 payment card, which the User may later change at any time.

By using the digital wallet service, the User may make transactions up to the limit approved by the Bank, in accordance with the agreement concluded with the Bank.

The User may request the registration of a Card in the digital wallet only on devices that are legally owned or held by them. Registration of the Card may be initiated directly from the digital wallet application. Cards may be registered only on iOS/Android devices with original software compatible with the specific provider's application, equipped with NFC technology, and running the operating system specified by the provider.

The service provider may set its own limitations or restrictions on the use of the digital wallet. To register a card in the digital wallet, the User must cumulatively meet the conditions set by the service provider under a separate agreement concluded between the User and the provider. Aik Bank is not responsible for the establishment or modification of the service provider's conditions under that agreement.

The Bank reserves the right to unilaterally disable the execution of transactions in the digital wallet or prevent token creation (card digitization) in case of suspected misuse of Card data, suspected fraud by the User or third parties, or suspected unauthorized transactions by the card scheme. If the User's mobile number is not registered in the Bank's system, Card registration in the digital wallet will not be possible.

If the Bank becomes aware that the security settings (password, PIN, default pattern, etc.) of the mobile device containing or intended to contain a digitalized card have been compromised or made known to others, the Bank will block the Card, thereby blocking all associated tokens across all devices and promptly notify the User.

10.3. User Obligations

The user of the digitalized card service is required to:

1. Register the Card in the digital wallet application only on devices legally owned and used solely by the User;
2. Set a strong password for securing the device and keep the password in a safe place;
3. Avoid using security settings (passwords, PINs, default patterns, etc.) on the mobile device that could easily be guessed or associated with the User;
4. After registering the Card in the digital wallet application, protect the device with the same care as the physical Card, preventing unauthorized use, loss,

or theft, and protect the device containing the token from abuse in case of loss or theft;

5. Prevent other persons from accessing the mobile device, especially by storing their biometric data (fingerprint, face scan, etc.);
6. Immediately notify the Bank in the event of loss or theft of the Card, or theft of Card data necessary for using the service;
7. Notify the Bank of the loss, destruction, theft, unauthorized access to, or unauthorized use of the device in which the token is stored;
8. Monitor the account linked to the Card and check transactions performed using the digitalized card service, and immediately report any irregularities or discrepancies to the Bank;
9. Prevent any third party from executing transactions, and ensure that only the User's biometric data is stored on the device for authentication and confirmation of transactions;
10. Protect the device's security features (PIN and other security elements) from exposure and abuse.

Removing a token from the digital wallet application deletes the token only from that specific device. If the User notifies the Bank of the loss of a device containing a token, the Bank will block the digitalized card on that device only (not on other devices). To reactivate the digitalized card on the lost device, the User must initiate a new registration in accordance with these Terms.

If the User notifies the Bank of the loss, destruction, theft, or unauthorized use or access of the device by a third party, the Bank will remove the token only on that device, deactivating the digitalized card on it. The User may continue to use the card and digital wallet if it is installed on another device owned by the User.

If the User wishes to block the digitalized card on all devices where it is installed, they must explicitly request this from the Bank.

If the Card is permanently blocked, the Bank will deactivate all tokens associated with that Card on all devices used by the User, rendering the Card unusable for digital wallet payments on all devices where it was registered.

If the User requests a replacement Card after a block, the Bank shall activate a new token without requiring a new registration process and shall enable the User to use the replacement Card in the digital wallet.

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

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

10.4. Obligations of the Bank

The Bank undertakes to:

1. Ensure that the personalized security elements of the payment instrument are available exclusively to the User to whom the instrument was issued, without prejudice to the User's obligation to take all reasonable and appropriate measures to protect the personalized security elements upon receipt of the payment instrument (e.g., personal identification number);
2. Inform the User about the executed transaction;
3. Enable the User, at any time, to immediately notify Aik Bank (the payment service provider) upon becoming aware of the loss, theft, or misuse of the payment instrument, or to request the reactivation or replacement of the payment instrument once the reasons for its blocking cease;
4. Prevent any further use of the payment instrument after the User has promptly notified the Bank of its loss, theft, or misuse;
5. Notify the User monthly about account activity by sending a statement, as agreed in the framework agreement for the use of the account and/or payment card.

The Bank may not issue a payment instrument to the User unless it has been requested, except in cases where the previously issued payment instrument needs to be replaced.

The Bank assumes the risk of delivering the payment instrument and its personalized security elements to the User.

The Bank is obliged to provide the User with proof that they notified the Bank of the loss, theft, or misuse of the payment instrument, if requested by the User within 18 months of the date of such notification.

By introducing unconditional SIM verification, the Bank requires mandatory registration of a mobile phone number in its system, which includes SMS notifications for each approved authorization using the payment card or digital wallet. The User agrees and accepts that such SMS notifications cannot be disabled for digital wallet users.

10.5. Exclusion of Bank Liability

The Bank is not liable for:

1. Payments made using a token if executed by third parties with the User's consent (via digital wallet);

2. Any loss or damage (material or immaterial) resulting from the User's failure to comply with these Terms or any applicable provision governing the relationship between Aik Bank and the User;
3. Any direct or indirect damage, including but not limited to loss of profit, missed earnings, or other similar losses suffered by the User due to technical shortcomings or poor quality of the application or services;
4. Any event that disrupts, prevents, or affects the functionality of any card registered in the application, including but not limited to application or internet service unavailability, communication disruptions, network delays, network coverage limitations, system interruptions, and other technical issues.

10.6. Token Removal and Card Blocking

Removing a token from the digital wallet deletes the token only from that specific device. In case of card blocking, the procedures outlined in the contractual documentation and terms of business will apply.

If the User notifies the Bank of the loss of the device containing the token (digitalized payment card), the Bank will block the token on that specific device. The User may continue to use the payment card and digital wallet if installed on another device owned by them.

If the Card itself is reported as lost, the Bank will block the payment card, thereby blocking all associated tokens across all devices.

In the case referenced in Section 7.1, a User who wishes to reactivate the token (digitalized payment card) on the same device must repeat the registration process in accordance with these Terms.

If the card is permanently deactivated, the Bank will remove all associated tokens from all devices used by the User.

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

By registering a credit 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 credit card details, including the card's expiration date, for the purpose of concluding an agreement between the User and the Service Provider.

The Service Provider is the controller of personal data in relation to the User's personal data under the agreement for the use of the Digital Wallet, and as such, is responsible to the User for the lawful processing of their personal data during the term and after the termination of the agreement.

The Bank does not influence and is not responsible for how the Service Provider collects or processes data.

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

Contracting and using the Digital Wallet includes secure transmission of information via electronic communication networks provided by electronic communication service providers, which the Bank cannot control, including the User's own providers. The Bank is not responsible for the availability or functioning of these services, for the transmission of data between the Service Provider and the User's mobile device, or for the storage and archiving of data on the User's device.

11. Selection 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 is any payment instrument, including a payment card, computer, mobile phone, or other technical device containing a payment application, which allows the payer to initiate a payment transaction using the payment card.

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

12. Confirmation of Availability of Funds

The Bank maintaining the User's account shall, immediately upon receipt of a request from a payment service provider that is the issuer of a payment instrument based on a payment card, respond whether the funds required to execute a payment transaction initiated using a payment card are available on the User's payment account, provided the following conditions are met:

1. The User's payment account can be accessed via the Internet at the time the request is received;
2. The User has given explicit consent to the Bank maintaining the account to respond to such a request from a specified payment service provider, confirming the availability of funds corresponding to the specific payment transaction initiated using a payment card;
3. The consent referred to in item 2) of this paragraph was given prior to the submission of the first such request.

A payment service provider that is the issuer of a payment instrument based on a payment card may submit the request referred to in paragraph 1 of this Article only if the following conditions are met:

1. The payer has given explicit consent for such a request to be sent;
2. The payer has initiated a payment transaction in the amount referred to in paragraph 1 of this Article using a payment instrument based on a payment card;
3. The payment service provider that is the issuer of the payment instrument based on a payment card authenticates itself with the payment service provider maintaining the account before each such individual request is submitted and establishes secure communication and data exchange.

The response referred to in paragraph 1 of this Article shall only contain a 'yes' or 'no' without disclosing the account balance and must not be stored or used for any purpose other than to execute the payment transaction.

The Bank maintaining the User's account may not restrict the User's ability to dispose of funds on the payment account based on the response provided under paragraph 1 of this Article.

At the User's request, the Bank maintaining the account is obligated to inform the User of the payment service provider that submitted the request referred to in paragraph 1 and of the response provided.

Provisions of paragraphs 1 through 5 of this Article shall not apply to payment instruments based on cards containing stored electronic money.

13. Authentication

The Bank is obligated to apply strong customer authentication in the following situations:

1. When the User accesses a payment account online;
2. When the User initiates an electronic payment transaction;
3. When the User, through a remote communication channel, performs any activity that may pose a risk of fraud or abuse in relation to the execution of a payment transaction.

In cases where the payer initiates an electronic payment transaction remotely as defined in item 2) above, the Bank is required to implement strong customer authentication that 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 must 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 also apply to payment transactions initiated through a payment initiation service provider.

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

The Bank maintaining the User's account must allow the payment initiation service provider and the account information service provider to comply with the User authentication procedures provided 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 of this Article.

14. Conditions for Amendments and Termination of the Agreement

14.1. Amendments to the Agreement

All amendments to the Agreement must be made exclusively in writing and duly signed by authorized representatives of both Contracting Parties, except for those that are in favor of the User and which, in accordance with regulations and this Annex, may be amended and applied immediately without the prior consent of the User.

If the Bank proposes amendments to the provisions of the Agreement, it is obliged to deliver the proposal for such amendments to the User in written form no later than two (2) months prior to the proposed effective date of their application, during which time the User may agree to the amendments before the proposed effective date. For entrepreneurs, the Bank must submit such a proposal no later than fifteen (15) days prior to the proposed effective date of their application. The User may accept or reject the amendments before their effective date.

As an exception to the previous paragraph, if the Bank proposes a change in fees for the provision of payment services in favor of the User, or introduces a free new service or a functionality of an existing service, such change may be applied immediately without the prior delivery of a proposal for amendments to the User, with respect to the part of the Framework Agreement related to such change.

The User shall be deemed to have accepted the proposed amendments if they do not notify the Bank of their disagreement before the proposed effective date. The Bank is obliged to inform the User of this right in a clear and visible manner when delivering the proposal.

At the same time the proposal is delivered, the Bank is also obliged to inform the User of their right to terminate the Framework Agreement without charge or any additional costs if they do not agree with the proposed amendments, at any time before the effective date. The Bank must also specify the date prior to the effective date of the proposed amendments on which the termination will take effect.

14.2. Conditions for Unilateral Termination and Nullity of Provisions of the Agreement

The User has the right to terminate the Agreement at any time by providing written notice to the Bank, with a one-month notice period and without any fee. In such case, the User is required to settle the utilized credit limit and pay fees only for payment services provided until the termination date. If such fees have been paid in advance, the Bank is obliged to refund the proportional amount of the prepaid fees.

The Agreement shall be considered terminated once the following conditions have been cumulatively fulfilled:

1. the Bank receives the written termination request;
2. the card is returned to any branch office of the Bank;
3. the card is cut into two parts; and
4. all obligations arising from the possession and use of the card have been settled.
   The User is also obligated to settle any charges recorded with delay due to technical reasons.

The User is obliged to return to the Bank all cards whose use has been cancelled, along with a written notice of cancellation, and to settle all liabilities incurred or that may arise from the use of the cancelled cards.

If the User refinances the card through a loan from another bank, they undertake to visit a branch of the Bank after the other bank transfers the funds, and submit a written request for early repayment and closure of the card. If the User fails to submit such a request, the Bank is not authorized to unilaterally carry out early repayment and cancellation of the card without the User's written request.

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

14.3. Termination of the Agreement by the Bank

The Bank may terminate the Agreement with a notice period of two months and is obliged to deliver a written notice of termination of the Framework Agreement to the User.

In addition to the aforementioned cases, the Bank has the right to unilaterally terminate the Agreement with the User and declare the Card invalid, whereby the User is obliged to return to the Bank all Cards issued under this Agreement without delay, and no later than three days from the receipt of the termination notice, and to settle all obligations incurred or that will be incurred from the use of the Cards, in the following cases:
a) if the User fails to pay the minimum monthly instalment for two consecutive monthly statements;
b) if any court decision, enforcement order, or enforcement action is issued or carried out against significant funds of the User, which materially affects their ability to repay the credit;
c) if the User acted dishonestly by concealing data provided in the Card Application or by providing false information, as well as in other cases provided for in the Agreement.

In case of termination by either the Bank or the User, the further use of all Cards issued under this Agreement is prohibited, and the Cards shall be considered blocked.

Upon termination of the Agreement by the Bank, the entire outstanding debt shall become immediately due and payable.

If the Bank terminates the Framework Agreement, the User is required to pay fees only for payment services provided until the date of termination. If such fees have been paid in advance, the Bank is obliged to refund the User the proportional part of the prepaid fees.

The Bank and the User have the right to terminate the Agreement in other cases provided by the law governing obligations or any other applicable law.

14.4. Card Retrieval

In the event of a breach of any provision of these General Terms and Conditions, delay in payment of the minimum monthly obligation, or any other due amount, the Bank shall have the right to reduce the credit limit and/or suspend the use of the Card until full settlement of all outstanding amounts, with notice delivered in accordance with Article 3.1 of this Annex.

In accordance with the above, the User is obliged to return the Card upon the Bank's request.

14.5. Renewal of the Card and Selected Related Services

The validity of the Card shall be automatically extended upon expiry. Each new Card shall represent a continuation of the validity period of the previous Card and shall be subject to the same General Terms and Conditions and the Annex to the General Terms of Business of the initially selected related service, unless duly amended and the User has been informed thereof.

Upon receipt of the new Card, the User shall immediately invalidate the old Card by cutting it and returning it to the Bank.

If the User does not wish to renew the validity of the Card and the selected related services, they shall notify the Bank in writing no later than 60 days prior to the Card's expiration date. In such case, the validity of the Card and any additional Cards shall not be extended.

14.6. Transaction Protection

In the interest of protecting and securing transactions, the User is informed that video surveillance may be used during Card transactions, provided such technical capabilities exist.

15. Collateral

As security for the proper fulfilment of all obligations arising from the use of the Card, the User undertakes to provide, upon the Bank's request, collateral as defined in the Agreement.

16. Confidentiality and Protection of Personal Data Related to Payment Services

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

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

Detailed information on the processing of personal data, the data controller, the data protection officer, and the rights of the data subject are available in the General Terms of Business and the Privacy Notice, published on the Bank's website and available in all branches of the Bank, 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, transaction data, and data on the payment account status and changes, for the purpose of preventing, investigating, or detecting fraudulent activities or misuse in connection with payment services.

17. ENTRY INTO FORCE

This Annex 4 to the General Terms of Business shall enter into force on the day of its adoption and shall apply as of 6 May 2025.