AikBank

ANNEX 7

SPECIAL TERMS AND CONDITIONS FOR THE USE OF ELECTRONIC AND MOBILE BANKING SERVICES FOR INDIVIDUALS

1. INTRODUCTORY PROVISIONS

These Special Terms and Conditions for the use of electronic and mobile banking services for individuals of AikBank a.d. Beograd (hereinafter referred to as Special Terms) govern the mutual rights and obligations of the Bank and the Customer regarding the use of electronic and mobile banking services in accordance with the Payment Services Act (hereinafter referred to as the Act).

Through these Special Terms, the Bank provides the Customer with information about products, services, and functionalities available via electronic and mobile banking.

Following the development of technology and services offered to the Customer, the Bank may integrate new products, services, and functionalities within digital channels. Transactions carried out via new services will be executed according to the instructions provided by the Bank.

The Bank charges fees for services rendered to the Customer in accordance with the Bank's Price List for Services (hereinafter referred to as the Price List). The Bank reserves the right to offer the Customer more favourable fees than those defined in the Price List.

These Special Terms apply to the business relationship between the Bank and the Customer regarding the use of electronic and mobile banking services for individuals and form an integral part of the Framework Agreement for the use of electronic and mobile banking.

The Bank may, in accordance with technical possibilities and development, change existing and introduce new functionalities within digital services for individuals, while notifying the Customer of these changes and new features via mobile and/or electronic banking applications or other agreed communication channels. By using any functionality, the Customer confirms consent to the terms of use and is responsible for acting in accordance with the user instructions.

The Special Terms for using mobile and electronic banking services for individuals, together with:

- General Terms and Conditions of AikBank a.d. Beograd (hereinafter referred to as the GTC),
- Special Terms and Conditions for payment accounts and payment services for individuals of AikBank a.d. Beograd (hereinafter referred to as Special Terms),
- Price List for services rendered to individuals by the Bank (hereinafter referred to as the Price List),
- Transactions Schedule for the acceptance and execution of transactions for private individuals, which is an annex to these Special Terms (hereinafter referred to as the Transactions Schedule),
- Limit for Transaction Execution

Form the Framework Agreement (hereinafter referred to as the Framework Agreement/Agreement).

2. TERMS OF PROVIDING PAYMENT SERVICES

2.1. Basic conditions under which the Bank provides payment services

The Bank provides payment services in accordance with the Act, which applies to domestic payment transactions executed in dinars, as well as international payment transactions regardless of the currency of payment.
The mutual rights and obligations of the Bank and the Customer regarding the provision of payment and other services in connection with the payment account are governed by the Framework Agreement on the Payment Account, the General Terms and Conditions, and these Special Terms.

3. TERMS AND DEFINITIONS

Digital Banking refers to a set of services and functionalities provided by the Bank, including:

- **Electronic Banking,**
- **Mobile Banking,**
- **Contact Centre Service and SMS Service.**

Private Individuals in the context of these Special Terms refer to:

- **Consumer** refers to an individual who enters into a payment services agreement or an agreement related to electronic money for purposes not related to their business or other commercial activity;
- **Registered Agricultural Holding** refers to an individual farmer engaged in agricultural production, registered in the Agricultural Holdings Register as the holder of the holding, and is not a Consumer.

Electronic Banking refers to a service that enables the use of services related to a payment account through the Bank's electronic platform, using appropriate software on a computer.

Mobile Banking refers to a service that enables the use of services related to a payment account through the Bank's mobile application, using appropriate software on a mobile telecommunications device.

Contact Centre Service refers to a set of services provided by the Bank that the Customer can access via information and telecommunications technology and includes:

- **Voice Response System (IVR),**
- **ChatBot service,**
- Communication with Contact Centre operators.

Voice Response System refers to the Contact Centre service that allows access to information about the Bank's products and services.

ChatBot Service refers to the Contact Centre service that allows access to information about the Bank's products and services and submission of requests for the Bank's products and services.

SMS Service refers to the service that allows receiving information about the Bank's products and services and notifications about executed payment transactions, as well as due obligations on products the Customer holds with the Bank.

User Manual refers to the document provided by the Bank that explains how to use a particular service or feature within Direct Channels for individuals, which is available on the Bank's website.

Payment Services User - **User** refers to an individual (resident or non-resident under the provisions of laws regulating foreign exchange operations) who has entered into an agreement with the Bank regarding the use of electronic and/or mobile banking for individuals in accordance with these Special Terms.

Payment Application refers to computer software or an equivalent installed on a computer, mobile phone, or any other device that enables initiating a payment transaction based on a payment card and allows the payer to issue a payment order.

Authentication refers to the process that allows the Bank to verify the identity of the payment services user or the validity of using a particular payment instrument, including the use of personalized security elements as defined by the law. The identification of the User can be carried out in different ways in accordance with the technological solutions provided by the Bank and through a combination of two or more independent elements (e.g., mPIN, biometrics, QR code).

Reliable Authentication refers to authentication using two or more elements, which are categorized as knowledge (something only the User knows), possession (something only the User possesses), and inherence (something the User is), which are independent of each other, meaning that revealing one element does not reduce the reliability of the others. This system is designed to protect the confidentiality of authentication data.

Authorization refers to confirming the desired and initiated action by the user in accordance with the technological solutions provided by the Bank (e.g., confirming a payment, accepting an offer, signing agreement documents).

Personalized Security Elements refer to personalized data and identifiers assigned by the payment service provider to the User for authentication.

Sensitive Payment Data refers to any data, including personalized security elements, that can be used for fraudulent activities. In the case of the payment initiation service provider and the account information service provider, the account holder's name and account number are not considered sensitive payment data.

Payment Transaction refers to the deposit, transfer, or withdrawal of funds initiated by the User as the payer or as the payee, or initiated on behalf of the payer, carried out regardless of the legal relationship between the payer and the payee.

Remote Payment Transaction refers to a payment transaction initiated via the internet or any device that can be used for remote communication.

Payment Order refers to the instruction from the User, either as the payer or the payee, to the Bank, requesting the execution of a payment transaction.

Transaction refers to a payment transaction executed using electronic or mobile banking.

Instant Transfer Approval refers to a domestic payment transaction up to RSD 300,000 (inclusive), marked as urgent, initiated via paper-based payment orders or other payment instruments at any time of the day, during any day of the year, where the transfer of funds occurs in real-time or nearly real-time.

Payment Account refers to an account used for executing payment transactions, used for issuing payment orders or initiating payment transactions.

Initiating a Payment Transaction refers to actions taken as prerequisites for the execution of a payment transaction, including issuing a payment order and performing authentication.

Payment Instrument refers to any personalized means and/or set of procedures agreed between the User and the Bank, which the User uses to issue a payment order or initiate a payment transaction.

Payment Instrument Based on a Payment Card refers to any payment instrument, including payment cards, computers, mobile phones, or any other technical device containing a payment application, that allows the payer to initiate a payment transaction based on a payment card.

Issuing Payment Instruments refers to a payment service where the payment service provider issues a payment instrument to the payer for initiating and processing payment transactions for the payer with that payment service provider.

Payment Brand refers to any material or digital name, expression, mark, symbol, or their combination that represents the card payment system within which the payment transaction is executed based on a payment card.

Co-branding of a Payment Instrument (eng. cobranding) refers to including at least one payment brand and at least one non-payment brand on the same payment instrument based on a payment card.

Acceptance of Payment Transactions refers to a payment service where the provider of payment services with the payee agrees to accept and process payment transactions, transferring funds to the payee.

Payment Service Provider refers to the provider of payment services who opens and maintains a payment account for the payer, i.e., the Bank.

Payment Initiation Service Provider refers to the provider of payment services who provides a service where, upon the request of the payment services user, a payment order is issued from the payer's account held with another payment service provider.

Account Information Service Provider refers to the provider of payment services that offers a service provided via the internet, which provides grouped information on one or more payment accounts held by the payment services user with another payment service provider or multiple payment service providers.

Identification, Authorization, and/or Signing Means refers to the data and/or procedures: for identifying the User required for accessing electronic and mobile banking services through digital channels for individuals; for authorizing transactions; for signing electronic documents and/or granting consent to establish a contractual relationship with the Bank (e.g., Username, password, PIN, User's phone number, one-time password, tokens, qualified electronic certificate, and/or other identification devices), as well as for changing agreed conditions and delivering information and notifications regarding the Bank's products and services.

LIB (Activation Code) refers to numbers or alphabetical symbols or a combination of both that the Bank assigns to the User during the activation and/or registration process for electronic and mobile banking.

PASSWORD refers to a combination of numbers, letters, and special characters that the User selects independently.

mPIN refers to a numeric password defined by the User that serves to identify the User and authorize a transaction.

mTOKEN refers to a program that is connected to the User's mobile device via the mobile banking application, which enables authorization and authentication.

QR Code refers to a standardized two-dimensional label, a two-dimensional barcode, that contains information that can be read by a QR code scanner.

Authorization using a QR Code refers to an option within the mToken service that allows the user to log into the electronic banking application or sign a payment order or any other request within the electronic banking application by scanning a QR code.

Biometrics refers to the use of facial scanning or fingerprint recognition depending on the method supported by the device and activated on the device for logging into the application or for authorizing a transaction or other request within the application.

When using biometrics in the mobile banking application, the device's functionality is used, and no biometric data is exchanged with the Bank, meaning the Bank does not have access to your biometric data.

Digital Wallet refers to an application solution for mobile payments provided by the digital wallet service provider, which allows the User to register data related to one or more payment cards within the application and tokenizes the card(s) for initiating payment transactions. In addition to the contractual relationship with the Bank, the conditions and manner of using the digital wallet are agreed between the User and the service provider, particularly regarding the type and characteristics of the mobile device on which the digital wallet application can be installed. The User can find information on which digital wallets support adding one or more payment cards issued by the Bank on the Bank's website.

Digitalized Card refers to the digital representation of the payment card within the Digital Wallet and/or electronic and mobile banking applications, enabling the User to perform contactless payments at sales and withdrawal points and ATMs

that allow wireless data transmission over short distances between two devices and/or at internet sales points that support this type of payment. The Bank, as the card issuer, determines the types of cards that can be digitized.

5.

One-Time Password (OTP) refers to a one-time code with a time limit made up of numbers and/or letters or a combination of both (alphanumeric characters) assigned by the Bank to the User during the activation process for electronic and mobile banking and/or for authorizing a transaction.

Framework Agreement refers to the framework agreement for providing payment services in accordance with the regulations governing the field of payment services.

Sender of an Electronic Message refers to the entity that sent the electronic message or the message sent on their behalf, with the intermediary of the electronic message not considered the sender, where the intermediary refers to the entity that sends or receives electronic messages on behalf of the authorized entity.

Receiver of an Electronic Message refers to the entity that received the electronic message, or the message received on their behalf, with the intermediary of the electronic message not considered the receiver.

Push Message (Push Notification) refers to a message through which information is delivered to the application installed on a particular device.

In-App Messages refer to messages through which information is delivered within the electronic or mobile banking application and are accessible to the User after logging into the application.

The **Payment Services Agreement** is concluded as a **Framework Agreement for Payment Services** (hereinafter: Framework Agreement) or as an **Agreement for a One-Time Payment Transaction**, and pertains to banking operations provided under the law governing payment services.

A **Financial Services Agreement** refers to a specific agreement for the use of a product offered by the Bank in the area of financial services, which is not a payment service.

A **Request for Activating Electronic/Mobile Banking** refers to the document through which the User, who has not otherwise contracted the use of digital banking services for individuals, submits a request to the Bank for the use of electronic and mobile banking services for individuals.

In line with the further technological development of its solutions, the Bank may allow the User to use additional or modified means of identification, authorization, or signing, as defined in the user manual for the selected application solution.

4. ELECTRONIC AND MOBILE BANKING

4.1. Agreement

By entering into the Framework Agreement for a payment account/account package or the Framework Agreement for the use of mobile and electronic banking, the User acquires the right to use the services offered by the Bank.

The User accesses electronic and mobile banking in the following manner:

- **Electronic banking** – using an internet browser,
- **Mobile banking** – using the application downloaded from the publicly available location secured by the Bank.

The User is obligated to ensure, at their own cost, the minimal technical conditions required to use the services, as outlined in the user manual.

The **user manual** for electronic and mobile banking includes a description of how to use the services and is strictly for educational purposes. The manual is available to the Users on the Bank's website and/or within the electronic or mobile banking platform itself.

The services will be available to the User from the moment of activation, 24 hours a day, seven days a week, in the scope and manner defined in the Agreement, the user manual available on the Bank's website, and the provisions of the Framework Agreement.

The Bank is not responsible in the event the User is unable to use the service due to disruptions in internet traffic.

In the case of damage, blocking, loss, theft, or expiration of the identification, authorization, and/or signature means, the Bank may, upon the User’s request, replace them.

4.2. Features of Electronic and Mobile Banking

Electronic and mobile banking services enable the User to:

- View the balance and transaction history for all current and other payment accounts with the Bank, including deposit accounts, and accounts where the User has authorization to manage the funds;
- Transfer funds from one payment account to another (internal and external payment transactions);
- Transfer funds to and from deposit accounts (deposit placements);

- Transfer funds to credit product accounts;
- Buy and sell foreign currency;
- Make payments at merchant points equipped with contactless POS terminals via the **Electronic Payment Card** in accordance with card scheme rules;
- Issue payment requests at merchant points via standardized two-dimensional codes (QR codes) within the **instant approval transfer system**;
- Transfer funds to the recipient/payment recipient via the **"SEND"** service within the **instant approval transfer system** by entering the recipient's mobile phone number;
- Check the status and transaction history of credit products held at the Bank;
- Use other features based on the Bank's project solution and further developments of these services.
-

Additionally, electronic and mobile banking serve as communication channels with the Bank regarding all contractual relationships established between the User and the Bank.

Furthermore, through electronic and mobile banking, the User can:

- Initiate requests to change the terms of a product and/or service they are using, using the appropriate means for identification, authorization, and/or signing;
- Initiate, approve, and complete the use of Bank products and/or services from the Bank's offer using the appropriate means for identification, authorization, and/or signing.

The Bank may allow the User to view the status and transaction history of financial instruments, as well as issue orders for trading financial instruments (if the User holds such accounts with the Bank), depending on the Bank's technical capabilities and the development of application solutions.

To use **electronic and mobile banking**, the User must ensure the necessary computer, hardware, software, and communication equipment, which may vary depending on which of these services the User wishes to use. The Bank has the right to establish specific technical requirements for using **electronic or mobile banking** (temporary or permanent) under special circumstances, and will notify the User in the manner defined in the General Terms and Conditions, Payment Services Agreement, or other relevant documents, with which the User agrees (including, but not limited to, sending emails, SMS messages, Viber, WhatsApp messages, and others, which may include links to documents or files for download, or notifications via the Bank's electronic or mobile banking platforms).

The User is deemed to have consented that by registering their phone number, mobile phone number, and/or email address with the Bank, the Bank may identify the User based on this registered data via WAP protocol, SMS, and/or email messages, and other available methods, thus making account information, credit and debit card details, and other products and services the User has with the Bank available in the scope and manner defined in the **User Manual**. The User is obligated to treat all passwords used with these services as confidential. Payment orders made through any of the services will be processed in accordance with the applicable regulations and these Special Terms.

Telephone conversations related to the use of services are recorded and may serve as evidence of given orders and completed transactions. The Bank may use these voice records exclusively for resolving User complaints and in court proceedings.

Both the Bank and the User agree that electronic documents and electronic messages cannot be contested in terms of validity or evidential value simply because they are in electronic form. Furthermore, the **electronic signature**, which can be verified based on an electronic certificate, mPin, mTOKEN, OTP via SMS, or a qualified certificate, will have the same legal effect as a handwritten signature, in accordance with applicable law.

4.3. Distance Contracting

The User can submit a request for the approval of a Bank product and/or service or for a change in the terms of a product and/or service being used via electronic or mobile banking. Additionally, the User can, using electronic or mobile banking, give their consent to the Bank to conduct a creditworthiness assessment when submitting a request for the approval of a credit product.

Once the User submits a request for approval to use a product and/or service or to change the terms of a product and/or service being used via electronic or mobile banking, the request can, for products/services where the Bank enables this, be processed electronically, with the entire approval and implementation process being carried out through electronic or mobile banking.

In this case, the User gives consent through the use of a qualified electronic certificate or by consenting to establish a contractual relationship via two-factor authentication or by using high-level reliable electronic identification schemes, in accordance with the law governing electronic documents, electronic identification, and trusted services in electronic business, and the regulation of the National Bank of Serbia governing the minimum standards for financial institution

information system management.

If the User decides to complete the entire process from submitting the request for the approval of a product and/or service or change in the product/service terms to the approval and implementation through electronic or mobile banking, the contractual documentation will be made in electronic form (electronic documents) and signed with the User's qualified electronic signature or confirmed by giving consent through two-factor authentication (or optionally with another identification, authorization, and/or electronic signature method where allowed by law), in accordance with applicable regulations governing this area and the General Terms and Conditions for distance contracting.

The Bank has the obligation to apply appropriate technological procedures and equipment when handling electronic documents to ensure the protection of these documents, in accordance with applicable laws governing this area and the General Terms and Conditions for distance contracting.

The User is obligated to protect the means and data for identification, authorization, and/or forming a qualified electronic signature from unauthorized access and use. The User must immediately request the revocation of their certificate in cases of loss or damage to the means or data for forming the qualified electronic signature. The User is required to promptly inform the Bank of any changes that may affect the accuracy of their identity determination.

When the User's consent to establish or modify a contractual relationship or to execute a transaction is given using the appropriate means for identification, authorization, and/or signature, both the Bank and the User agree that the established or modified contractual relationship or executed transaction is deemed valid, with legal effect, and written form in accordance with the regulations governing this area of business and the General Terms and Conditions for distance contracting.

4.4. Unique Identification Code

The Bank issues the User a unique identification code (account or card number) upon concluding the Agreement, which the User is required to provide for the proper issuance or execution of a payment order and which serves to identify the account holder and the payment card holder (e.g., account number or card number).

By correctly indicating the unique identification code (account number) of the payment recipient in the payment order, it is considered that the payment order has been properly executed in relation to the recipient of the payment. The Bank is not responsible for an unexecuted or incorrectly executed payment transaction if the User provides a payment order with an incorrect unique identification code of the recipient (account number).

In such cases, upon the User's request, the Bank is obliged to immediately take all reasonable measures to ensure that the amount of the payment transaction is refunded to the User. The payment service provider of the recipient is obliged to cooperate with the Bank of the payer in this regard and to provide all necessary information to facilitate the refund of the payment transaction amount. If the refund of funds to the payer is not possible, the Bank is obliged to provide the payer, upon written request, with all available information necessary for claiming the refund of funds (e.g., information about the recipient's payment service provider and/or the payment recipient, including the information the recipient's payment service provider is required to provide to the payer's payment service provider in accordance with this paragraph).

In the case of an unexecuted payment transaction due to an incorrect unique identification code (account number), the Bank is obliged to immediately refund the amount of the unexecuted payment transaction to the User upon learning of the issue.

The services must not be used for illegal purposes, including the acquisition of goods or services prohibited by law. Any illegal use, such as purchasing pornographic content, engaging in prostitution, drug trafficking, or other unlawful activities, is punishable and will result in the termination of the right to use the service.

Upon assigning unique secret elements such as the PIN for identification, one-time OTP passwords, user certificates, access passwords, security questions and answers, and other identification and authorization means provided by the Bank, depending on the chosen application solution, the User is granted identification and access to services or parts of services. The User is responsible for maintaining the confidentiality of all the aforementioned security elements, for their distribution to individuals the User deems trustworthy, and for the costs incurred from their use.

4.5. Electronic Payment Orders

Using electronic or mobile banking, the User manages the funds in their accounts up to the available balance by issuing an electronic payment order. The electronic payment order is issued using a form provided in the electronic and mobile banking platforms, where the User must fill in all the necessary details for executing the transaction in accordance with the General Terms and applicable regulations.

The Bank will execute the electronic payment order of the User requesting the transfer of funds if:

a) The User has ensured sufficient funds for executing the order, which includes b) The amounts of fees, which are calculated and charged in accordance with the Bank's Price List; c) The User has given consent for the execution of the payment order (which meets the conditions from the previous paragraphs); d) No legal obstacles exist to the execution (according to other regulations).

The User is responsible for the accuracy of the information entered in the electronic payment order. The Bank is not liable if the electronic payment order is rejected or not executed due to improperly filled-in electronic payment orders by the User.

4.6. Issuance of Payment Orders – Non-Resident Users

A non-resident User, as defined by the provisions of the foreign exchange regulations, is allowed to view the accounts they hold with the Bank.

4.7. Form and Method of Providing Consent and Revocation of Consent for Issuing Payment Orders or Executing Payment Transactions

The User manages the funds in all Accounts opened based on the Account Opening and Maintenance Agreement concluded with the Bank, for which the use of specific services is foreseen.

When, according to special regulations, certain documents or specific data are required for the execution of an electronic payment order, the Bank will execute the payment order only if these documents or data are provided or presented in the prescribed form and within the required timeframe.

The Bank will execute the transaction if, prior to the execution, and depending on the Bank's established technical solution, the User:

- Is identified using identification and authorization means and/or signature in one of the following ways:
    - By username and password: entering a combination of a unique username and password created by the User.
    - By username and mToken: entering a combination of a unique username and a one-time password generated by the mToken.
    - By PIN: entering a unique PIN created by the User.
    - By qualified electronic certificate: using the medium on which the User's qualified electronic certificate is stored and entering the PIN.
    - By biometric characteristics (fingerprint, facial recognition, etc.). These biometric data are registered by the User on the device from which the services are accessed, while the Bank neither collects nor stores them in the Bank's information system.
- Has given consent for execution in one of the following ways:
    - By PIN: entering a unique PIN created by the User.
    - By biometric characteristics (fingerprint, facial recognition, etc.). These biometric data are registered by the User on the device from which the services are accessed, while the Bank neither collects nor stores them in the Bank's information system.
    - By m-token: entering the One-Time Password (OTP) generated by the mToken.
    - By qualified electronic certificate: the transaction/request is authorized using the medium containing the qualified electronic certificate and entering and confirming the User's PIN.

The User may give consent for the execution of the payment transaction either through the recipient of the payment or through the payment initiation service provider.

Consent may be revoked by withdrawing consent for the execution of a payment transaction or a series of payment transactions through a statement of withdrawal (via the communication channel selected by the User in the request or through the application itself), or by contacting the Bank's Contact Centre, until the moment the Bank receives the electronic payment order. If the User and the Bank determine that the execution of the payment order is to begin on a specific day or at the end of a specified period or on the day when the User makes the funds available to the Bank, the electronic payment order may be revoked by the end of the business day preceding the specified execution day.

The Bank may refuse to execute a payment order if the conditions outlined in this Article are not met, or if it is established by regulations, or if there is reasonable doubt regarding the authenticity of the payment order or some of its elements.

The Bank where the User holds an account cannot refuse to execute a payment order when all the conditions set forth in the agreement on payment services are met, except in the cases mentioned in the previous paragraph.

The Bank will notify the User of the refusal to execute the payment order in dinars (through the application itself, orally, by phone, or by another agreed method) of the reasons for the

refusal, when possible, and the procedure for correcting the deficiency that caused the refusal on the same business day the payment order was submitted to the Bank, unless notification is prohibited by law. Exceptionally, the deadline for notifying the User about the refusal to execute a payment order in foreign currency is established by law or other regulations.

4.8. Time of Receipt of the Electronic Payment Order and the Execution Deadline for Payment Services and Individual Payment Transactions

The time of receipt of a payment order and the deadlines for the execution of payment transactions are further regulated by the Transactions Schedule.

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

4.9. Transaction Limits

The Bank has established limits for transactions through electronic and mobile banking, which are available on the Bank's website and in the Bank's business premises, within the document Limits for the Use of Payment Instruments, as well as within the electronic banking system and mobile banking application. The User may modify the transaction limits at any time by calling the Contact Centre with additional identification or by submitting a request at a branch or through the mobile banking application if technical capabilities allow it. The Bank reserves the right to change the limits, and the User will be notified through the agreed communication channel or via the mobile banking application.

4.10. Digitalized Payment Card

The User can perform the tokenization process of the payment card issued to them in accordance with the Framework Agreement on the Issuance and Use of Credit and/or Debit Payment Cards, so that it can be used as a Digitalized Payment Card. The tokenization process of the payment card is carried out in mobile banking on a device that supports the tokenization option or within the digital wallet available on the User's mobile device.

The use of the digitalized payment card is supported exclusively at merchant points of sale that accept payment cards from the same card scheme under which the Digitalized Payment Card was issued. The digitalized payment card can also be used without internet access.

The Bank sets transaction limits for the digitalized payment card, which are published on the Bank’s website and form an integral part of the Framework Agreement.

If the tokenized payment card is blocked, deactivated, or expired, the use of the digitalized payment card will not be possible.

The conditions for using the digitalized payment card are governed by the Special Business Terms for Payment Cards, as well as the Rules and Conditions for the Use of Digital Wallets.

4.11. Consent for the Execution of Services

The Bank performs the aforementioned services through the Voice Automated Service and ChatBot Service if, prior to the execution of the transaction, the User is identified with an identification, authorization, and/or signature means as follows:

- Identification by PIN: entering the unique PIN created by the User.
- Identification by entering and confirming the One-Time Password received from the Bank.

5. Information about Communication Methods and Means Between the User and the Bank

For all communication between the Bank and the User, regarding rights and obligations from the Agreement, the Serbian language will be used. This does not exclude the use of other languages at the User's request, according to the capabilities and good banking practice.

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

- Verbally: visiting the branch, calling the Bank's Contact Centre.
- In writing: notices, letters, and other written documents.
- Electronic communication: including the Bank’s website, chat, email, applications for electronic and mobile banking, and options within them depending on technical possibilities (in-app messages, push notifications), using applications and social media platforms such as Viber, WhatsApp, Facebook, etc., sending SMS messages, or using applications that enable individual communication with the User, as well as using other application solutions made available by the Bank in accordance with technical possibilities.

Information and notifications will be provided through the agreed method of communication. All relevant data related to the execution of payment transactions, as well as communication addresses for contacting the Bank, can be found on the Bank’s website.

The User has the right to request one copy of the Agreement in

written form or on another durable medium, and to request, during the duration of the contractual relationship, a copy of the contract or the information provided during the pre-contractual phase, in the form of the contract draft, in a way that allows the User to familiarize themselves with the terms related to the provision of payment services and to compare the offers of different payment service providers to assess whether these conditions and services meet their needs.

Upon the User's request, the Bank is obliged to provide precise information about the execution period for a specific payment transaction the User initiates under the Agreement, as well as any fees that will be charged. If the Bank charges these fees collectively, the Bank must also provide information about the type and amount of each individual fee that makes up the total fee.

6. Information on Protective and Other Measures in Case of Loss, Theft, or Misuse of Payment Instruments

The User is obliged to use the payment instrument in accordance with the prescribed or agreed conditions governing the issuance and use of that instrument, including the details mentioned in the user instructions. The User must, in particular, immediately after receiving the payment instrument, take all reasonable and appropriate measures to protect the personalized security elements of the instrument (e.g., security letter). The User must immediately notify the Bank or the designated person upon learning of the loss, theft, misuse of the payment instrument, unauthorized use of equipment and/or mobile devices, or any suspicion of unauthorized use of the Bank's services. Additionally, the User must take care to protect and use the mobile device used together with the mobile/electronic banking application as a payment instrument to prevent loss, theft, or misuse. The User must immediately notify the Bank upon learning of the loss, theft, or any misuse of the mobile device or other devices and/or mobile phone data or anything that could indicate unauthorized use.

In cases mentioned above, the User must immediately notify the Bank by calling the Customer Centre or in writing, and request that the services be blocked. In case of a telephone report, the notification will be electronically recorded, and the Bank is obliged to block the further use of the services.

Any material damage caused by the loss, theft, or misuse of the payment instrument or unauthorized use of equipment and/or mobile devices or suspicion of unauthorized use of the Bank's services up to the moment of reporting the loss, theft, or misuse shall be borne by the User. If, after reporting the loss, theft, or misuse, the User finds the payment instrument, they must not use it and must immediately return it to the Bank. If the Bank does not allow for the timely reporting of the loss, theft, or unauthorized transaction using the payment instrument or data from it or unauthorized use of equipment and/or mobile devices or suspicion of unauthorized use of Bank services, the User will not bear the consequences of unauthorized use unless the misuse was done by the User.

The User additionally agrees to:

- Use the identification, authorization, and/or signature means in a manner that ensures their secrecy, and not to write, disclose, or make available to third parties the username, password, PIN, or data generated by mToken.
- Bear responsibility for unauthorized transactions in accordance with the **General Terms**.
- Immediately notify the Bank of the loss, theft, misuse, or unauthorized use of identification, authorization, and/or signature means, any other form of misuse, or any actions that are not in line with the **General Terms**, **Special Terms**, **Payment Service Agreement**, **Other Financial Services Agreement**, and **User Instructions** by calling the Contact Centre at 0800 10 10 15 or by visiting the nearest Bank branch.
- Enter correct data when performing transactions via electronic or mobile banking and the **Contact Centre Service** and bear the risk of entering incorrect or unnecessary data.
- Report any changes to personal data necessary for using digital channels for physical persons by submitting a request for data changes to the Bank.
- Execute all transactions in accordance with the **Framework Agreement**, legal and sub-legal regulations governing this area, and fulfill all contractual obligations in accordance with applicable laws.
- Ensure control over access to devices from which they use digital channels for physical persons.
- Behave responsibly and reasonably on the internet, not open emails with unknown links or malicious programs, and prevent their device from being infected with malware that could cause financial damage.
- Implement security measures on devices used for accessing digital channels for physical persons, use programs for protection from malicious software, and access digital channels only from devices that are free from malicious programs.
- Regularly update the operating system of the device used to access digital channels for physical persons.
- Regularly monitor the Bank's website, especially notices related to digital channels for physical persons, and respond appropriately.

The User agrees to check the accuracy of the data on the account statement and, if discrepancies are found, to file a

complaint with the Bank. The Bank will examine any dispute or discrepancy in charges or credits on the account reported by the User, provide relevant information available to the Bank, and, based on the verification results, make necessary adjustments and corrections to the account.

The User bears losses resulting from unauthorized transactions up to the amount of RSD 3,000 if the transactions were executed due to the use of:

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

Exceptionally, the User bears all losses arising from the execution of unauthorized payment transactions if those transactions were executed due to fraudulent actions of the User or the User's failure to fulfil their obligations under this Article due to their intent or gross negligence.

The User will not bear losses under this Article in the following cases:

1. If the loss, theft, or misuse of the payment instrument could not have been detected before the unauthorized payment transaction, except in the case specified in paragraph 2 of this Article;
2. If the unauthorized payment transaction is a result of an action or omission of an employee, representative, or branch of the payment service provider or another person to whom activities of the payment service provider were entrusted, except in the case specified in paragraph 2 of this Article;
3. If the Bank has not ensured at all times that the User could notify it about the lost, stolen, or misused payment instrument in a proper and free manner, unless these losses were caused by fraudulent actions **8.** of the User;
4. If the Bank did not request reliable authentication of the User, except if these losses were caused by fraudulent actions of the User.

If the Bank requests reliable authentication of the User, and the recipient of the payment or the payment service provider of the recipient does not apply the required reliable authentication of the User, they must compensate the Bank for any damages incurred.

The User will not bear losses incurred due to unauthorized payment transactions executed after they have immediately notified the Bank that the payment instrument was lost, stolen, or misused, unless those losses were caused by fraudulent actions of the User.

Exceptionally, the National Bank of Serbia may prescribe that the User bears losses arising from the execution of unauthorized payment transactions up to an amount lower than RSD 3,000, especially considering the nature of the personalized security elements of the payment instrument and the circumstances under which the payment instrument was lost, stolen, or misused.

6. Bank's Exemptions from Liability:

The Bank shall not be liable:

- In case of failure to execute transactions due to incorrect data entry/errors made by the User.
- For the unavailability of digital channels for individuals caused by technical issues on the User's equipment, interruptions or disturbances in telecommunication channels, electrical power failures, or force majeure.
- For the computer, hardware, software, and communication equipment used by the User to access digital channels for individuals.
- If the User does not immediately notify the Bank about the misuse, invalidity, revocation, theft, loss, or unauthorized use of the Identification, Authorization, and/or Signature Means.
- In case of unavailability of mobile banking to a User who attempts to install the service on a device running an operating system older than the last two available versions.
- In case of unavailability of mobile banking to a User attempting to install the service on a device that has been illegally unlocked or is intended for a foreign market (e.g., jailbroken or rooted device).

7. Instant Transfer Approval at the Merchant's Point of Sale

A Merchant refers to the recipient of payment designated to receive the funds subject to the instant transfer approval initiated by the payment request at the merchant's point of sale. A Payment Request at the Merchant's Point of Sale refers to a payment order issued by the payer from their payment account using a payment instrument for instant transfer approval at the merchant's point of sale.

IPS QR Code refers to a standardized two-dimensional barcode containing elements to present the payment order.
The Bank allows the User to issue a payment request at the merchant's point of sale by accessing the mobile banking application, generating their IPS QR code, or scanning the merchant's IPS QR code.

The User, through the mobile banking application, selects the checking account to be debited based on the completed instant transfer approval, up to the amount of available funds.

The User can initiate an instant transfer approval at the merchant's point of sale using the mobile banking application or by exchanging data between the User's (payer's) electronic devices in one of the following ways:

1. By presenting the User's data through the standardized two-dimensional IPS QR code (presenting the payer).
2. By retrieving merchant data from the standardized two-dimensional IPS QR code (presenting the merchant).

The User can also initiate an instant transfer approval at a virtual merchant point of sale (e.g., a web shop) by uploading the merchant's IPS QR code.

Each merchant sales and payment location (including virtual sales points, e.g., web shops) where the User can initiate an instant transfer approval is clearly marked with the "IPS" symbol.

Depending on the presentation method chosen by the merchant (presenting the payer or presenting the merchant), each payment point will be marked with the applicable method, enabling clear identification of whether the IPS QR code needs to be presented or the merchant's IPS QR code scanned.

The User provides consent for the payment request at the point of sale in the manner specified in the user instructions.
Once the instant transfer approval request has been executed, the User will immediately receive a notification from the Bank about the execution.
After the payment request at the merchant's point of sale, the Bank initiates the refund of the amount from the request due to the User's dispute of the charge on their payment account for one of the following reasons:

1. The User was informed about the completed payment request, but the merchant denies receiving the information and has not delivered the goods or services.
2. The User denies receiving or delivery of goods or services after payment at the point of sale.

Complaints regarding the quality of goods and services paid for via instant transfer approval at the merchant's point of sale should be addressed exclusively to the merchant (acquirer) where the transaction occurred. The Bank is not responsible for the correctness or quality of goods and services paid for via instant transfer approval at the merchant's point of sale.

9. Fees

The type and amount of fees for services provided by the Bank, including those related to how and how often information is made available in accordance with the Law, are determined by the Framework Agreement with the User in accordance with the applicable Bank's Price List. Fees for the use of electronic and mobile banking services for individuals, and for executing transactions using electronic and mobile banking, are calculated and charged from the User's account in accordance with the Price List.

Fees for executing payment transactions issued through electronic and mobile banking are charged automatically before the execution of payment transactions, in accordance with the Price List. The User is obligated to ensure that sufficient funds are available on the account from which the payment transaction is being executed, to cover the fees for the transaction.

The Bank reserves the right to charge for sending SMS messages in accordance with the applicable Price List for all mobile phone numbers registered by the User for the SMS service.
The Bank is authorized to collect any monetary obligations of the User towards the Bank from available funds across all accounts opened with the Bank through automatic account debiting.

When the User holds multiple accounts (dinars or foreign currency), the Bank is authorized to determine the order in which it will transfer funds to collect its receivables from the User, including the purchase of funds from foreign currency accounts at the Bank's buying rate for cash on the day the Bank purchases funds for the collection of the User's due obligations. In the case of collecting foreign currency claims from the User's dinar accounts, the Bank's selling rate for foreign currency will be applied on the day of the debit. If foreign currency claims are collected by the Bank from accounts held in a currency different from the currency of the User's account being debited, both the buying and selling rates for foreign currency will apply on the day of the debit (the buying rate for foreign currency when converting foreign currencies to dinars, and the selling rate for foreign currency when converting dinars to foreign currencies).
The cost of sending SMS messages by the User for account balance and transaction change inquiries is charged by the mobile operator.

Changes in interest rates and exchange rates can be applied immediately and without prior notice to the User if they are based on changes in the agreed reference interest rate or reference exchange rate. The Bank will promptly notify the User in writing of any change in the interest rate, either on paper or on another permanent data carrier.

For services that provide the possibility of executing payment

transactions via payment orders to transfer funds from the payer's account to the payment account of the payee, the Bank charges a fee for each such individual payment transaction, in accordance with the Price List.

9. Currency Exchange Rate – Currency of the Payment Transaction

The payment transaction is executed in the currency agreed upon between the user of the payment services and the payment service provider, in accordance with regulations governing foreign exchange operations.
The Bank executes the payment order in the currency specified in the payment order.

Execution of the payment order may require the purchase and/or sale of domestic or foreign payment means (currency conversion). For these conversions, the Bank will use the buying/selling exchange rates from the Bank's daily EXCHANGE RATE LIST for foreign currencies.

When converting domestic currency into foreign payment means (purchasing foreign currency), the Bank will use the selling exchange rate for foreign currencies. When converting foreign payment means into domestic currency (selling foreign currency), the Bank will use the buying exchange rate for foreign currencies.

The BANK'S EXCHANGE RATE LIST is available at the Bank's branches and on the Bank's website, with the possibility that the Bank may apply a more favourable exchange rate determined by mutual agreement between the Bank and the user (verbally or via email).

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

10. Blockage/Unblocking of Services

Upon the User's request, the Bank may block the use of electronic/mobile banking services, either partially (for a specific service) or in full.

The Bank has the right to block the service without the User's consent, partially or fully, in the following cases:

1. If it is assessed that the security of the User's data and funds is endangered for any reason.
2. If the Bank suspects that the User or a third party is abusing these services.
3. If the use of these services by the User, in the Bank's exclusive assessment, poses a security threat or jeopardizes the Bank's operations.
4. If the User does not adhere to the agreed terms and the User's instructions.
5. In other cases provided by law.

The Bank will suspend the services upon the User's request, which can be submitted at any branch of the Bank, in writing, or via a method specified in the User's instructions for each of the individual services.

The User may block any individual service or specific electronic and mobile banking services for individuals at any time:

- By calling the Contact Center.
- By submitting a request at any Bank branch.

In such cases, access to electronic and mobile banking services for individuals can be unblocked by submitting a request at any Bank branch or by calling the Bank's Contact Center with additional identification.

For security reasons, the Bank will automatically block the Token and/or mToken if, during transaction authorization, the User enters the incorrect one-time password generated by the mToken five times. Once blocked, the Token cannot be unblocked, and the User must request the issuance of a new mToken device. The blocked mToken can be unblocked personally at a Bank branch or through the Bank's Contact Centre.

The Bank will notify the User about the intended blockage of the electronic and mobile banking services for individuals immediately before blocking, as well as the reasons for the blockage. If it is not possible to notify the User before the blockage or if the reasons for the blockage require it, the Bank is obliged to notify the User immediately after the blockage. The notification about the intended blockage or the blockage itself will be sent in accordance with the General Terms and Conditions. Exceptionally, the Bank will not notify the User if such notification is prohibited by law or if there are legitimate security reasons.

The Bank will allow the use of the services again when the reasons for the blockage cease to exist. In these cases, the User can unblock access to electronic and mobile banking services for individuals personally at the Bank branch or through the Bank's Contact Center with additional identification, provided that the Bank reserves the right to refuse unblocking if there is still a security threat.

11. Payment Instrument Based on Multiple Payment Brands

If the Bank offers this service, the consumer, upon concluding the payment service agreement, has the right to be issued a payment instrument based on a payment card with two or more payment brands. The Bank is obligated to provide the

consumer with clear and objective information about the payment brands associated with the service, as well as their characteristics, including their capabilities and applicability, costs, and protection measures, within an appropriate period before the conclusion of the payment service agreement.

12. Bank's and User's Responsibility for Initiating Payment Transactions or for Unexecuted, Incorrectly Executed, and Unauthorized Payment Transactions

In the case of unauthorized, unexecuted, or incorrectly executed payment transactions, without affecting the Bank's and the User's obligations under the provisions of Articles 4.4., 13., and 14. of these Special Terms, the Bank must, regardless of its responsibility for the correct execution of the payment transaction, immediately take appropriate measures to determine the flow of funds of the payment transaction upon the User's request and provide the User with information about the outcome of the measures taken without delay.

The Bank cannot charge the payer for taking action in accordance with paragraph 1 of this Article.

It is the right of the User of payment services to demand compensation for damages caused by the execution of an unauthorized payment transaction or the non-execution or incorrect execution of a payment transaction, or delays in the execution of a payment transaction for which the Bank is responsible.

If the User claims that they did not approve the executed payment transaction or that the payment transaction was not executed or was incorrectly executed, the Bank, if it claims otherwise, must prove that the payment transaction, in the relevant part of the service it provides, was authenticated, properly recorded, and booked, and that no technical failure or other deficiency influenced its execution.

If the payment transaction was initiated through a payment initiation service provider, the payment initiation service provider must prove that the payment transaction, in the part of the service they provide, was authenticated, properly recorded, and that no technical failure or other deficiency in their service influenced its execution.

A payment transaction is authenticated, within the meaning of this Article, if the Bank has used appropriate procedures to verify and confirm the use of the specific payment instrument, including its personalized security elements.

If the payer claims that they did not approve the payment transaction executed using the payment instrument or initiated through the payment initiation service provider, the records of the payment service provider regarding the use of that instrument, or the initiation of the payment transaction, are not necessarily and sufficiently proof that the payer approved the payment transaction, acted fraudulently, or was negligent.

The Bank and the payment initiation service provider, in the case from the previous paragraph, are required to provide evidence making it likely that the User acted fraudulently or that they did not fulfil their obligations regarding the payment instrument and personalized security instruments due to negligence or intentional conduct.

13. User's Liability for Unauthorized Payment Transactions

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

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

Exceptionally, from paragraph 1 of this Article, the User will bear all losses resulting from the execution of unauthorized payment transactions if such transactions were executed due to fraudulent actions by the User or failure to fulfil their obligations under Article 6 of these Special Terms due to their intention or gross negligence.

The User will not bear the losses from this Article in the following cases:

1. If the User could not detect the loss, theft, or misuse of the payment instrument before the execution of the unauthorized payment transaction, except in the case from paragraph 2 of this Article;
2. If the unauthorized payment transaction is a result of an action or omission by an employee, agent, or branch of the payment service provider, or another person entrusted with the payment service provider's activities, except in the case from paragraph 2 of this Article;
3. If the Bank has not ensured that the User can notify it about the lost, stolen, or misused payment instrument in an appropriate manner and without charge, unless the losses were caused by fraudulent actions by the User;
4. If the Bank did not require reliable authentication of the User, except if the losses were caused by fraudulent actions of the User.

If the Bank requires reliable authentication of the User, and the payment recipient or the payment service provider of the recipient does not apply the requested reliable authentication of the User, they must compensate the Bank for the damages it

has suffered as a result.

The User will not bear the losses resulting from unauthorized payment transactions executed after they have immediately notified the Bank that the payment instrument was lost, stolen, or misused, unless such losses were caused by fraudulent actions of the User.
Exceptionally, from paragraph 1 of this Article, the National Bank of Serbia may prescribe that the User bears the losses resulting from the execution of unauthorized payment 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 payment instrument was lost, stolen, or misused.

14. Bank's Responsibility for Unauthorized Payment Transactions

The Bank is responsible for executing a payment transaction for which there is no consent from the User (hereinafter: an unauthorized payment transaction).

In the case of an unauthorized payment transaction, the Bank is obliged to immediately upon learning, and no later than the next business day after it discovers or is informed about the transaction, reverse the amount of the transaction to the User, unless the Bank suspects fraud or misuse on the part of the User. In such a case, the Bank must, within ten days of learning about the unauthorized payment transaction, proceed in one of the following ways:

1. Provide the User with a justification for refusing the refund and report the fraud or misuse to the competent authorities, or
2. Refund the amount of the transaction to the User if, after additional checks, the Bank concludes that the User did not commit fraud or misuse.

The Bank is obliged to return the User's payment account to the state it would have been in had the unauthorized payment transaction not been executed, ensuring that the value date of the payment account approval is no later than the date the account was charged for that transaction.

The Bank is also obliged to refund any fees charged to the User, as well as pay back any interest the User would have been entitled to if the unauthorized payment transaction had not been executed.

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

15. Responsibility for Non-Execution or Improper Execution of a Payment Transaction or Delays in the Execution of a Payment Transaction Initiated by the User (Payer)

If the payment transaction was directly initiated by the User, the Bank is responsible to the User for its correct execution up to the payment service provider of the recipient.

If the Bank is responsible for the non-execution or improper execution of a payment transaction, it is obliged to immediately upon learning, refund the amount of the non-executed or improperly executed transaction to the User, or restore the User's payment account to the state it would have been in if the improper payment transaction had not occurred, unless the User requested proper execution of the payment transaction.

In case of improper execution of the payment transaction, the Bank is obliged to ensure that the value date of the approval for the User's payment account related to the improperly executed transaction is no later than the date the account was charged for the amount of the improperly executed transaction.

If the Bank provides the User, and if necessary, the payment service provider of the payment recipient, with proof that the payment service provider's account was approved for the amount of the payment transaction, the payment service provider of the recipient is responsible to the recipient for the non-execution or improper execution of the payment transaction.

The payment service provider of the payment recipient is obliged to ensure that the value date of the approval for the recipient's payment account related to the improperly executed or non-executed payment transaction is no later than the business day when the funds of the payment transaction would have been approved if the payment transaction had been executed properly.

If the payment transaction was executed after the time set by law, the payment service provider of the payment recipient is obliged to, at the request of the Bank acting on behalf of the User, ensure that the value date of the approval is no later than the business day when the funds of the payment transaction would have been approved if the payment transaction had been executed properly, in accordance with the law and these Special Terms.

If the Bank is responsible for non-execution or improper execution of a payment transaction or delay in the execution of a payment transaction, it must refund the User for any fees it charged, as well as pay back any interest the User would have been entitled to concerning the non-executed or improperly executed payment transaction.

If the payment transaction was initiated by the User through a payment initiation service provider, the Bank shall be considered the User's payment service provider in the sense of paragraphs 1 to 4 and paragraph 6 of this Article.

In the case of the payment transaction referred to in the previous paragraph, the payment initiation service provider is obliged to prove that the Bank received the payment order in accordance with section 3.1.4. of these Special Terms and that, in the part of the service it provides, the payment transaction was authenticated and correctly recorded, and that no technical failure or other defect affected the execution or non-execution of the payment transaction or the delay in the execution of the payment transaction. It is also obliged to provide evidence of this without delay at the request of the Bank.

16. Responsibility for Non-Execution or Improper Execution of a Payment Transaction or Delay in the Execution of a Payment Transaction Initiated by the Payment Recipient or the User (Payer) Through the Payment Recipient

If the payment transaction was initiated by the payment recipient or the User through the payment recipient, the payment service provider of the payment recipient is responsible for properly submitting the payment order to the Bank, which acts as the payment service provider for the User. If the payment order is not submitted, or if it is incorrectly submitted in the case outlined in paragraph 1 of this Article, the payment service provider of the payment recipient is obliged to immediately upon learning of this, submit or resubmit the order to the Bank.

If the payment order is submitted to the Bank after the deadline agreed upon between the payment recipient and their payment service provider, or between the Bank and the payment service provider, the payment service provider of the payment recipient must ensure that the value date for the approval of the payment recipient's account is no later than the date the account would have been approved for the amount of the payment transaction if the payment transaction had been executed within the agreed timeframe.

If the amount of the payment transaction initiated by the payment recipient or the payer through the payment recipient is approved on the account of the payment service provider of the payment recipient, this provider is responsible to the payment recipient for the proper execution of the payment transaction.

If the payment service provider of the payment recipient is responsible according to paragraph 4 of this Article, they must ensure that the value date for the approval of the payment recipient's account is no later than the date the account would have been approved for the amount of the payment transaction if the transaction had been executed properly.
If the payment service provider of the payment recipient provides proof to the payment recipient, and if necessary to the Bank, that it is not responsible to the payment recipient in accordance with paragraphs 1 to 4 of this Article, then the Bank or the payer's payment service provider is responsible to the User for the non-execution or improper execution of the payment transaction.

The actions of the Bank, which is responsible under paragraph 6 of this Article, are governed by the provisions of Article 15. The Bank will not be held responsible under the previous paragraph if it proves that the payment service provider of the payment recipient received the amount of the payment transaction, and there was only a slight delay in executing the transaction. In this case, the payment service provider of the payment recipient must ensure that the amount of the payment transaction is approved on the recipient's account, with the value date for the approval of this account being no later than the date on which the account would have been approved if the payment transaction had been executed properly.

The payment service provider responsible under this Article is obliged to refund the User for all fees charged, as well as to refund or pay the amount of any interest to which the User is entitled in relation to the non-executed or improperly executed payment transaction.

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

The Bank is obliged to provide the User with a refund or proper execution of the payment transaction if the User notifies the Bank of an unauthorized, unexecuted, or improperly executed payment transaction, or if the User requests the proper execution of the payment transaction, and this notification or request is made immediately after the User becomes 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 has not provided the User with information about the payment transaction, the Bank is responsible for the unauthorized, unexecuted, or improperly executed payment transaction and must ensure that the User receives the refund of the amount mentioned in the previous paragraph, even after the 13-month period has passed, if the User notified the Bank of the unauthorized, unexecuted, or improperly executed payment transaction immediately after becoming aware of the transaction.

If the payment transaction referred to in paragraph 1 of this Article involved a payment initiation service provider, the refund of the amount mentioned in that paragraph is requested by the User from the bank that holds the User's account.

AikBank

18. Rights and Obligations of Payment Service Providers in Cases of Fraud, Abuse, and Incorrect Execution of Payment Transactions

If the Bank receives a request for a refund along with the data, information, and documentation indicating that a payment transaction is likely a result of fraud or abuse, the payment service provider of the payee must prevent the funds from being made available to the payee's account, or block the use of those funds for the payee within three business days of receiving the data, information, and documentation.

If, in the situation mentioned above, the payment service provider of the payee subsequently, but before the expiration of the three-day period, receives additional data, information, and documentation from the Bank, including a report to the competent authority, which conclusively indicates that the transaction resulted from fraud or abuse, the payment service provider of the payee must:

1. Immediately return the funds to the User if, within 15 business days of being notified of the data, information, and documentation, the payee cannot prove the origin of the funds or refuses to provide appropriate evidence;
2. Allow the payee to access the funds after 30 business days, if the payee proves the origin of the funds within the specified time frame and no restriction on the funds has been imposed by the competent authority.

The payment service provider of the payee is responsible to the payer for any loss arising from a payment transaction in case of fraud or abuse. If, contrary to the previous provisions, the payee is allowed to access the funds before proving the origin of the funds, or if fraud or abuse is involved, the payment service provider must return the funds to the payer.

The Bank has the following rights and obligations in cases of improper execution of domestic payment transactions:

1. If the payer's payment service provider transfers an amount that exceeds the agreed amount in the payment order or if the payment order is mistakenly executed multiple times, the payment service provider of the payee must immediately return the excess funds upon notification from the payer's service provider;
2. If the amount transferred by the payment service provider of the payee is less than the amount specified in the payment order, the payer's payment service provider can transfer the difference to the payee's service provider without the payer's request;
3. If the funds are transferred to a wrong payee, the payer's payment service provider can correct the transaction on the same business day by transferring the funds to the correct payee's account without a request from the payer.

The refund of funds as outlined above has priority over any other payment transactions from the account where the funds were incorrectly transferred.

19. Refund of the Amount of a Properly Executed and Approved Payment Transaction to the User

The Bank will refund the full amount of a properly executed and approved payment transaction initiated by the payee or the User through the payee's provider, if the following conditions are met:

1. The User has given consent for the execution of the payment transaction without specifying the exact amount of the payment transaction;
2. The amount of the payment transaction exceeds what the User could reasonably expect, considering the amounts of previous payment transactions, the terms established in the Framework Agreement, and the circumstances of the specific case.

The Bank may require the User to provide evidence related to the fulfilment of the above conditions. The User cannot claim that the amount of the payment transaction is higher than what could reasonably have been expected if the higher amount is the result of currency conversion at the reference exchange rate.

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

1. The User has directly given consent to the Bank for the execution of the payment transaction;
2. The Bank or the payee has provided the User with information about the future payment transaction in the agreed manner at least 28 days before the due date.

The User may submit a Refund Request within 56 days from the date of the charge. The Bank is obliged to refund the full amount of the payment transaction or inform the User of the reasons for rejecting the refund request within ten business days from receiving the Request. The value date for the User's account can be no later than the date the account was debited for the payment transaction.

If the Bank refunds the disputed amount to the User and the card organization determines in the dispute resolution process that the complaint was unfounded, the Bank will charge the User's account for the amount of the refunded funds without additional consent from the User.
If the Bank rejects the User's refund request, it must inform the

User in the notification of the rejection about:

1. The process for protecting the User's rights and interests, including out-of-court dispute resolution;
2. The procedures that can be initiated due to the violation of the provisions of the Law;
3. The authority responsible for handling such procedures.

In the case of direct debiting where a domestic payment transaction is initiated in dinars or a payment transaction in euros within the single euro payments area (SEPA), the User is entitled to a refund of the approved payment transaction executed via that direct debit even when the conditions outlined in paragraph 1 are not met.

The User will not be entitled to a refund of the amount of the payment transaction in paragraph 1 of this section if the following conditions are met:

1. The User has directly given consent to the Bank for the execution of the payment transaction;
2. The Bank or the payee has provided the payer with information about the future payment transaction in the agreed manner at least 28 days before the due date.

20. Execution of Payment Transactions Based on Bills of Exchange

A payment transaction based on a bill of exchange is a payment transaction where the payee initiates the payment transaction to debit the User's payment account based on a bill of exchange and a payment order requesting the transfer of funds from the User's account to the payee's account.

The bill of exchange referred to in paragraph 1 of this Article, including the electronic bill of exchange, is issued in accordance with the law governing bills of exchange and represents an irrevocable consent from the issuer of the bill of exchange to their payment service provider to execute the payment transaction initiated by the holder of the bill of exchange in accordance with this paragraph.

If the bill of exchange from paragraph 1 of this Article is registered in the registry of bills of exchange and authorizations maintained by the National Bank of Serbia in accordance with the regulations governing forced collection of funds on the account, the payee can, in accordance with these regulations, initiate a payment transaction to debit the payer's current account with any payment service provider that maintains such an account.

21. Authentication

The Bank is obliged to apply reliable authentication of the User in cases where the User:

1. Accesses their payment account via the internet;
2. Initiates an electronic payment transaction;
3. Performs any activity via remote communication means that could expose the transaction to the risk of fraud or misuse in relation to the execution of a payment transaction.

In case the payer initiates an electronic payment transaction from point 2 of paragraph 1 of this Article remotely, the Bank is obliged to apply reliable authentication of the User, which includes elements that dynamically link the transaction to a specific amount and payee.

The Bank is obliged to implement appropriate security measures to protect the confidentiality and integrity of the User's personalized security elements in the cases described in paragraph 1 of this Article.

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 the provider of account information services.

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

22. Payment Brand and Payment Application (Cobranding)

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 any other technical device that contains a payment application, enabling the payer to initiate a payment transaction based on the payment card.

23. Confirmation of Available Fund

The Bank managing the User's account is obliged to respond immediately upon receiving a request from the payment service provider issuing the payment instrument based on a payment card, confirming whether the required amount of funds for the execution of a payment transaction using the payment card is available on the User's payment account, provided that 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 managing the account to respond to such a request from the specified payment service provider, confirming that the required amount of funds for the specific payment transaction using the payment card is available.
3. The consent referred to in point 2 of this paragraph was given before the submission of the first such request.

The payment service provider issuing the payment instrument based on a payment card can submit the request under paragraph 1 of this Article if the following conditions are met:

1. The payer has given explicit consent to submit such a request.
2. The payer has initiated a payment transaction using the payment card in the amount specified in paragraph 1 of this Article.
3. The payment service provider issuing the payment instrument authenticates itself with the Bank managing the account before submitting each such request, establishing secure communication and exchanging messages and data.

The response in paragraph 1 of this Article contains only 'yes' or 'no,' without revealing the balance of the payment account, and cannot be stored or used for any purpose other than executing the payment transaction.

The Bank managing the User's account cannot restrict the availability of funds on the User's payment account based on the response provided in paragraph 1 of this Article.

The Bank managing the User's account is obliged to inform the User, upon their request, about the payment service provider who submitted the request and the provided response.

The provisions of paragraphs 1 through 5 of this Article do not apply to a payment instrument based on a card where electronic money is stored.

24. Termination and Cessation of the Agreement for Electronic and Mobile Banking Services for Users

24.1. Commencement of the Agreement and Amendments to the Framework Agreement

All amendments to the Agreement must be made exclusively in writing and duly signed by both parties, except for those that benefit the User and can be amended and applied immediately under the Law without their prior consent.
If the Bank proposes amendments to the terms of the Agreement, it must provide the User with a proposal for these amendments in writing, no later than two months before the proposed start date for their implementation. The User may accept or reject the proposal before the proposed start date.

Notwithstanding the previous paragraph, if the Bank proposes a change to the fees for payment services in favour of the payment service users or introduces a new free service or functionality of an existing service, such change may be applied immediately without prior delivery of the proposal for amendments to the Framework Agreement regarding that change.

It is considered that the User has agreed to the proposed amendments to the Agreement if they have not notified the Bank that they do not agree with the proposed changes before the start date of their implementation. The Bank must notify the User in a clearly visible manner when delivering such a proposal.

At the same time as delivering the proposal to the User, the Bank must inform the User of their right to terminate the Agreement without paying any fees or additional costs, should they not accept the proposal.

The Bank must also inform the User, simultaneously with delivering the proposal, of their right to terminate the Framework Agreement at any time before the start date of the proposed amendments and without paying fees or other costs, as well as of the specific date before the proposed changes take effect, when the termination will be valid.

24.2. Conditions for Unilateral Termination of the Agreement

The User has the right to terminate the Agreement at any time with a notice period of one month, without penalty.

The User also has the right to terminate the Agreement in other cases specified by the law governing obligations or other laws.
The Bank has the right to terminate an agreement concluded for an indefinite period, with a notice period of two (2) months, as well as in other cases specified by the law governing obligations or other applicable regulations. The termination must be done by providing written notice to the other contracting party using the agreed-upon communication channels.
In case of termination of the Agreement, the User is obliged to pay the Bank a fee only for the payment services provided up to the date of termination. If such a fee was paid in advance, the Bank is obliged to return the proportional part of the paid fee

to the User.
The User may request that provisions of the Agreement, which are inconsistent with the information provided during the pre-contractual phase in accordance with the law, or provisions regarding information about mandatory elements of the Agreement that were not previously provided, be deemed invalid.
Except in the cases mentioned above, the Bank may unilaterally terminate the Agreement and deactivate the User's accounts in the following cases:

- If it is determined that the User is on official terrorist or other negative lists, in accordance with domestic and international regulations on preventing money laundering and financing terrorism;
- If the User, upon the Bank's request, fails to provide the necessary data about themselves, the source of funds, or the nature/purpose of the business relationship with the Bank and/or transactions conducted through the Bank, within the allocated or reasonable time;
- If the User's account has been inactive for a consecutive period of 6 months, meaning no activities are recorded in the application.

If the Bank is unable to deliver a notice of termination/cancellation of the agreement or a request for data update to the last address provided by the User, because the User has not timely informed the Bank about the change of address or mailing address, the day the notice/request is attempted for delivery by the post office (or another legal entity specialized in delivering registered mail) will be considered the date of delivery.

25. Confidentiality and Protection of Personal Data in Connection with Payment Services

The Bank processes the personal data of the User in accordance with the applicable Personal Data Protection Law of the Republic of Serbia and the General Terms and Conditions of AikBank A.D. Beograd.

Personal data of the User is processed for the purposes of fulfilling the contractual relationship between the User and the Bank, meeting the Bank's legal obligations, and for marketing purposes, provided the User has given explicit consent.

Detailed information on the processing of personal data, the data controller, the person responsible for personal data protection, and the rights of the data subjects is available in the General Terms and Conditions (GTC) and the Privacy Notice, which can be accessed on the Bank's website and in the branches. This information is regularly updated.The Bank, along with participants in the payment system, may collect, process, and exchange data concerning the User of payment services, including personal data, as well as data about payment transactions, account balances, and changes to the User's payment account, for the purpose of preventing, investigating, or detecting fraudulent activities or abuses related to payment services.

26. ENTRY INTO FORCE

This Annex 7 of the General Terms and Conditions enters into force on the date of adoption and shall apply from 6 May 2025.