ERSTE BANK A.D. NOVI SAD
BOARD OF DIRECTORS
Number: 1436/2026-574/1-1
Date: 26.11.2026.

GENERAL TERMS OF PROVIDING PAYMENT SERVICES TO ENTREPRENEURS

I. INTRODUCTORY PROVISIONS:

Erste Bank a.d. Novi Sad (hereinafter Bank) shall, as the payment service provider, set out in the General Terms of Providing Payment Services to Entrepreneurs (hereinafter: General Terms) the mutual rights and obligations relating to payment service execution in accordance with the Law on Payment Services (Official Gazette no. 139/2014, 44/2018 and 64/2024) and the accompanying by-laws.

Basic data on the Bank:

Business name: ERSTE BANK A.D. NOVI SAD;

Head office: Industrijska 3J, 21000 Novi Sad;

TIN: 101626723;

REG. NO.: 08063818;

Giro account: 908-0000000034001-19;

Web page www.erstebank.rs;

e-mail address: info@erstebank.rs

Telephone for users: 080 0201 201

+38166/89 69 000

The operation license was issued by the National Bank of Yugoslavia under decision O no. 202 of 20 December 1989. The competent authority supervising the Bank operation shall be the National Bank of Serbia, Nemanjina 17.

II. TERMS

1) payment transaction means an act, initiated by the payer or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee;
2) payment order means any instruction by a payer or payee to his payment service provider requesting the execution of a payment transaction;
3) e-payment order means electronic message containing instruction, which is electronically generated, sent, verified, received, processed, and stored;
4) current account means payment account maintained with the Bank, used for executing payment transactions and for other purposes relating to services provided by banks to payment service users;
5) payment account means an account used for executing payment transactions, maintained by payment service provider for one or several payment service users; Payment account may be current account or other payment account;

6) payment instrument means any personalised device and/or a set of procedures agreed between the payment service user and the payment service provider and used by the payment service user in order to issue or initiate a payment order;
7) payment service user means a natural person or legal entity that uses or used a payment service in the capacity of a payer and/or payee or has addressed the payment service provider in order to make use of such services;
8) payer means a natural person or legal entity that issues a payment order from the payment account or gives consent to execute a payment transaction based on the payment order issued by a payee, or, if there is no payment account, a natural or legal person that issues a payment order;
9) payee means a natural person or legal entity designated as the recipient of funds subject to a payment transaction;
10) user (consumer) means a private individual executing payment service agreement or agreement relating to electronic money for the purposes not intended for its business or other commercial activity;
11) entrepreneur means a natural person other than a consumer, and/or a natural person with legal capacity that pursues a business activity with a view to earning income, in accordance with the law governing companies and other law;
12) funds means cash, scriptural money and electronic money;
13) cash means banknotes and coins;
14) electronic money means electronically (including magnetically) stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of execution of payment transactions which is accepted by a natural or legal person other than the electronic money issuer;
15) electronic money holder means a natural person or legal entity to whom electronic money has been or is being issued, and/or a natural or legal person that has addressed the issuer for the purpose of issuing the money, as well as any other natural or legal person having a claim referred to in item 14);
16) business day means a day, namely part of the day in which the relevant payment service provider of the payer or of the payee involved in the execution of a payment transaction is open for business as required for the execution of a payment transaction to its payment service user;
17) credit transfer means a payment service where the payer instructs the payment service provider to initiate the execution of one or more payment transactions, including issuing of a standing order, at the charge of payment account, including standing order issuance, after which payee’s payment account shall be approved in the amount of payment transaction;
18) credit instant transfer is a domestic payment transaction in RSD which may be initiated by a payer at any time of day, every day in year, and the transfer is executed instantly or almost instantly through the National Bank of Serbia IPS payment system.
19) NBS IPS system means a system which enables the payment service providers to execute single instant credit transfers (instant payments) 24 hours a day, seven days in week, 365 days in year (24/7/365) almost instantly, i.e. within only a few seconds.
20) direct debit means a payment service where a payee, based on the payer’s consent, initiates a payment transaction to debit the payer’s payment account. The payer may give such consent to the payee, its payment service provider or payee’s payment service provider;
21) standing order means an instruction given by the payer to the payment service provider which holds the payer's payment account to execute credit transfers at regular intervals or on predetermined dates;
22) value date means a reference date, that is, reference time used by a payment service provider for the calculation of interest on funds debited from or credited to a payment account;
23) reference exchange rate means the exchange rate which is used as the basis to calculate any currency exchange which is made available by the payment service provider or comes from a publicly available source;
24) reference interest rate means the interest rate which is used as the basis for calculating interest which is publicly available and is determined independently of the unilateral will of the payment service provider and the user which have entered into a payment service agreement;

25) unique identifier means a combination of letters, numbers and/or symbols specified to the payment service user by the payment service provider to be used in a payment transaction to identify unambiguously the respective payment service user and/or its payment account;
26) means of distance communication refers to any means which, without the simultaneous physical presence of the payment service provider and the payment service user, may be used for the conclusion of a payment service contract;
27) durable medium means any instrument which enables the payment service user to store data addressed personally to him in a way accessible for future reference for a period of time adequate to the purposes of the data and which allows for the unchanged reproduction of the data stored;
28) domestic payment transaction means a payment transaction in which the payer's payment service provider and payee's payment service provider provide the service within the territory of the Republic of Serbia;
29) payment account change means a service provided by the payment service provider to the User, in accordance with the Law on Payment Services
30) international payment transaction means a payment transaction in which one payment service provider provides the service in the territory of the Republic of Serbia, and the other payment service provider in the territory of a third country, as well as a payment transaction in which the same payment service provider provides the service in the territory of the Republic of Serbia for one payment service user, and in the territory of the third country for that same or other payment service user;
31) remote payment transaction means a payment transaction initiated via internet or through a device that can be used for distance communication;
32) payment transaction initiation means the taking of actions which are a precondition for starting the execution of a payment transaction, including payment order issuance and authentication;
33) payment transaction initiation provider performs the service where, upon the request of payment service user, payment order shall be credited to the payer's payment account held with other payment service provider;
34) Provider of service of account information shall perform the service provided through the Internet, providing grouped information on one or multiple payment accounts a payment service user holds with other payment service provider or multiple payment service providers
35)) authentication means a procedure which allows the payment service provider to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials;
36)) strong customer authentication means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data;
37)) personalised security credentials mean personalised data and features provided by the payment service provider to a payment service user for the purposes of authentication;
38) Issuing of payment instruments means a payment service by a payment service provider contracting to provide a payer with a payment instrument to initiate and process the payer's payment transactions with such payment service provider;
39) Acquiring of payment transactions means a payment service provided by a payment service provider contracting with a payee to accept and process payment transactions, which results in a transfer of funds to the payee.
40) IBAN (International Bank Account Number) means the international identification number of a payment account, used to designate a payment account in accordance with the decision establishing the unique structure for the identification and classification of accounts and the chart of accounts for the application of international rules and the IBAN standard, which is used for the unambiguous identification of a payment account.
41) 3D Secure (3DS) is a security protocol used for the protection of on-line payment using cards (debit and credit). The purpose thereof is to provide an additional authentication layer to reduce the risk of non-authorised transactions.

42) Single Euro Payments Area – SEPA (hereinafter: SEPA area) means the territorial area comprising the Member States of the European Union and other states or territories that have met the criteria for accession to the SEPA area, as well as the regulations of the European Union and the rules, practices, standards, and guidelines contained in the SEPA rules for the execution of payment transactions, within which payment transactions are carried out in a mutually harmonised manner, under equal conditions and with equal rights and obligations, in accordance with those acts. **The list of the SEPA area countries is available at** https://www.europeanpaymentscouncil.eu/document-library/other/epc-list-sepa-scheme-countries;
43) SEPA rules for the execution of payment transactions (payment scheme) denote a unified set of rules, practices, standards and/or operational guidelines for executing payment transactions – agreed upon by payment service providers for the purpose of executing payment transactions – which is separate from any payment infrastructure or payment system that supports the implementation of that set of rules, practices, standards and/or operational guidelines.
44) SEPA Credit Transfer means a domestic and international payment transaction executed via a credit transfer in euros within the SEPA area. Credit transfer means a payment service whereby the payer, with their payment service provider, initiates the execution of one or more payment transactions to debit their payment account, after which the payee's payment account is credited with the amount of that payment transaction or those payment transactions.
45) 46) mTOKEN means a program connected to the User's mobile device through the mobile banking application, which enables authorisation and authentication.

III. PAYMENT SERVICES

The Bank shall perform the following payment services:

1) services of account opening and maintaining and closing
2) services of incoming payment of cash on payment account, services necessary for such account opening, maintaining, and closing;
3) services of outgoing payment of cash on payment account, as well as any services necessary for such account opening, maintaining, and closing;
4) fund transfers from/to a payment account, in one of the following ways:
   (1) credit transfers,
   (2) using a payment card or similar means;
5) execution of payment transactions where funds are covered by a credit line for a payment service user, in one of the following ways:
   (1) credit transfers,
   (2) using a payment card or similar means;
6) issuing and/or acquiring of payment instruments.

A user who has activated eBanking and/or mBanking service (has access to its payment account through Internet) shall be entitled to use the payment initiation service provided by the payment initiation service provider and the service of the provision of information on account provided by the provider of the service of providing account information. If the user intends to use these services, the User shall arrange such services with the payment initiation service provider or with the account information service provider. The Bank shall not, in any manner whatsoever, be responsible for the obligations resulting from the agreement of the User and such service provider. Regarding the payment orders received through the payment initiation service provider, the Bank will act in the same manner as in the event of the orders issues directly from the User, save for objective reasons.

ACCOUNT OPENING AND MAINTAINING

The Bank shall open current and other payment accounts – escrow accounts, etc. The Bank shall open account based on filled-in Account Opening Application, Statement on Ownership, and documentation from the List of Necessary Documentation for Account Opening, as well as other documentation the Bank deems as necessary in the process of documentation collection that it is necessary for the identification of the User and User's beneficial owner.

The Bank shall open and maintain RSD accounts and FX accounts.

FX accounts shall be opened and maintained by the Bank for each currency individually.

If the User wants to execute payment transactions in a currency which is not tied to the account, it is necessary to address the Bank, for the purpose of opening of the account in such currency.

The Bank may open specific accounts to the User for particular purposes (such as account of cover – for payment to Kosovo, account for inflows from abroad based on credits, account for inflows from abroad based on donation, account for inflows from Kosovo, etc.).

The accounts referred to in the previous paragraph shall be governed by the provisions of the account opening and maintenance agreements previously entered into with the Bank, the existing deposited specimen signatures and e-banking authorizations, as well as the applicable laws and regulations governing transactions and operations related to such accounts.

The client will be notified on transactions on specific accounts by the Bank through statements from such accounts

When on-boarding a client, the Bank shall identify the User reviewing his valid status documentation, provided for in the List of Necessary Documentation, which shall be an integral part of the Account Opening Application.

Account opening applicant shall allow the Bank to verify and further process all of the data listed in the Application, in accordance with the Law on Personal Data Protection, as well as to, upon account opening, forward his personal data to the Account Register maintained by the NBS which shall be public.

In addition to the data referred to in the above paragraph, the Bank may also request other data from the User. In the event the User fails to provide the data which would enable the Bank to implement analysis of the User in accordance with the provisions of the Law on the Prevention of Money Laundering and Terrorism Finance, the Bank will not establish business relation or execute a transaction, i.e. it will terminate already existing business relation.

Documentation provided by a client to the Bank in a foreign language will, upon the request by the Bank, be provided in certified translation into the Serbian language. Documentation shall be provided in writing (original, copy, or certified copy) according to the specification from the List of Necessary Documentation received upon request together with Account Opening Application and it may be overtaken at all of the Bank sales units as well as on the Bank web site.

The Bank shall reserve the right to reject Application without any obligation of explaining its decision to the Applicant.

When opening current account, the Bank shall provide the User with data on the number of account serving as a unique identification designation of the User in payment transactions, which is to be stated when executing payment services and used in payment transaction for unambiguous identification of such user and/or his payment account.

The Bank shall maintain the account to the User, execute payment services, and provide other banking services, in accordance with the General Terms, agreement entered into with him, and applicable regulations.

Payment Account Change

Payment Account Change means a service that the Bank will enable a User opening or holding an account at a new payment service provider (hereinafter: new payment account) to switch payment account in the same currency.
Payment account switch shall solely be made based on the authorisation of the User provided by the User to the new payment service provider (hereunder: Authorisation), with or without closing of the payment account opened with the previous payment service provider.
Based on the authorisation submitted to the Bank as a new payment service provider, the User may determine standing orders, incoming payment transfers, and other payment services the execution of which shall be switched to a new payment account provided that the Bank provides such services. The User shall provide the Bank with the Authorisation

in writing, whereby the Bank will immediately upon the receipt of such Authorisation, provide the User with the counterpart or copy as an evidence of receipt. Upon the receipt of the Authorisation, the new and previous payment service provider shall implement the activities set out in the Law, in accordance with the Authorisation.
If the Bank is the previous payment service provider, following the implementation of all necessary activities prescribed in the Law, the Bank will close the account the switch of which is requested provided that the User has provided the consent in the Authorisation for the account closing at the Bank and that the User has no outstanding liabilities on such account. Unless the conditions for closing of the account referred to in this paragraph are met, the Bank will, without delay, notify the User thereof.
Information on the obligations and responsibilities of the previous and new payment service provider, in accordance with the Law, deadlines for the implementation of actions, and the fees charged regarding payment account switch, any data the User must present to the Bank, possibility of extra judicial settlement of disputable relation, in accordance with the Law governing the protection of financial service users, shall be available free of charge, in hard copy or other permanent data carrier, at all Bank branches as well as on the Bank's web site, and, upon the request by the User, will be provided to the User free of charge.
Provisions of this item governing the account switch will also apply to the User's payment account switch with the Bank, i.e. to the payment account switch when the Bank is, at the same time, the previous and new payment service provider.

Proxy and Authorisations

When opening the account, the User may authorise other person to open the account, through the proxy certified with the relevant authority.

The User may authorise one or several persons to dispose of funds on account, by providing signatures of such persons in the Signature Specimen. Authorisation for funds disposal may be single or joint – restricted with co-signature and without any limit or including a limit in terms of the amount of funds disposal.

In the event of any change in authorisations or limits for the disposal of monetary funds, agreement execution, or other restrictions in legal dealings, the User shall report them to the Bank without any delay.

The User shall state data on the person who will, on behalf of and for the account of the User, be an authorised person to physically bring orders, in the event orders are issued by the User in hard copy.

The Bank shall be entitled to, upon bringing order, identify the person and reject order execution in the event the order provider is the person not referred as such by the User. In this manner, the Bank shall prevent any fraud and order execution not approved by the User.

For any persons authorised for using the e-banking and m-banking services, the User shall provide the Bank with the data on persons with such authorisation in accordance with the rules of the E-Bank and M-Bank use. The Bank shall not be liable or bear damage of the User arising due to the User's failure to report, in an accurate and timely manner, any data relating to the private individuals having the authorisations with the User, which may impact the execution of payment services and, in general, funds of the User held with the Bank.

Data Change

Reporting of any changes shall be made by the User to the Bank on form: Data Change Application. Data Change Application may be downloaded by the User from the web pages and at the points of sale of the Bank.

The User shall fill in and provide the Bank with the respective application, in the event of the change in: any data registered with the Agency for Business Registers and/or other relevant authorities, any data relating to ownership structure change, any data relating to the change in personal data of the persons authorised for signing and disposing of funds on account, any changes in authorisations of such persons, as well as any changes relating to the authorisations provided to special persons by representative.

Timely reporting of change means reporting of change immediately upon a change occurrence, without any delay and/or within 3 days from change occurrence and/or registration at the ABR or other official register i.e. within 3 days from the receipt of the resolution on the change if such change is registered with court or other relevant authority.

The Bank shall not be liable or bear any damage of the User arising from the User's failure to report, in an accurate and timely manner, any data relating to private individuals having any authorisations with the User, which may impact the execution of payment services and, in general, any funds of the User held with the Bank.

Delivery of Notices

It shall be deemed that the Bank has performed the obligation of the delivery of any notifications to the User based on the registered or reported mailing address or e-mail address, and it will not be liable for any damage arisen on the side of the User due to the failure of reporting address change.

The Bank shall be entitled to reject services to the User and block the User's account in the event it is aware of any changes in the data not reported by the User to the Bank.

The User shall be liable for any failures or damage which may arise due to the non-compliance with the obligation of the submission of data on arisen changes, as well as due to the failure to be in compliance with the obligation of providing any other data requested by the Bank.

The User must immediately notify the Bank on any unauthorised use of payment services (unauthorised order issuance, internal forgeries, signature misuse, etc.) and on any other security breaches he becomes aware of.

The User shall be liable to the Bank for the damage which would arise due to unauthorised and incorrect use of service by the User.

The Bank shall be entitled to stop executing payment services to the User as well as to block the User's account in the event the Bank is aware of an unauthorised use of services or the breach of any other security form.

DEBIT/CREDT CARD

Upon opening of the account to the User, the Bank shall, upon the User's request, issue him a debit payment card which shall be the payment instrument based on which the User shall dispose of funds on the account and/or initiate payment transactions up to the amount available on his account.

The User who wants payment card shall first be issued by the Bank a payment card for which processing, netting, and reconciliation of transfer orders, issued based on its use in domestic payment transactions, are executed within the payment transaction system of the Republic of Serbia, in accordance with the Law on Multilateral Interchange Fees and Special Operating Rules for Card-based Payment Transactions (“Official Gazette of the RS”, no. 44/2018).

If the User also wants a debit payment card of other payment brand, the bank will, upon the User’s request, issue other debit payment card.

Upon the expiry of the validity of previously issued card, in the event of re-issuance of the existing card, the User shall also be issued by the Bank a payment card for which processing, netting, and settlement of transfer orders, issued based on the card use are, executed in domestic payment transactions within the payment system in the Republic of Serbia (unless the User has been previously issued business debit payment card for which, processing, netting, and settlement of transfer orders in domestic payment transactions, issued based on the card use, are executed within the payment system in the Republic of Serbia).

Credit card shall be payment instrument through which approved loan shall be used up to the amount of the available balance of loan.
The Bank shall issue credit Card, upon the User's request, to the persons listed in Credit Card Issuance Application.

The Card shall be made out to the User and it shall not be transferable. The Card shall be the ownership of the Bank upon whose request it must be returned.
Holder of account the Card is tied to (hereinafter Account Holder) shall solely be liable for proper Card use.

For payment card issuance and use, the Bank shall charge fees and costs listed in the Price List of Products and Services to Entrepreneurs (hereinafter Price List). The Bank shall collect fees and other charges by debiting account the Card is tied to or in cash.

The Account Holder/Card User shall be liable for the accuracy of any data the Bank is provided with when the Card is issued and report any data change to the Bank. Any costs incurred due to the failure to report data shall be borne by the Account Holder.

The Bank shall be entitled to, during the Card validity and/or automated Card re-issuance, change a type of same or other payment Card brand, in which case, the Bank will, excluding any additional costs, make the change of the Card used by the User and ensure the functionalities that correspond to the functionalities of the card which is replaced.

The Bank shall retain the right not to issue the payment card in the event of the Card inactivity during a longer time period.

Card Issuance and Card Data Protection

The User shall be provided with the Card and PIN (personal identification number). The Bank may enable the Cardholder to use the Card in digital form prior to receiving the physical Card, in accordance with the provisions of these General Terms and Conditions governing the Digitized Payment Card and the Digital Wallet.

As a rule, the PIN is neither generated nor delivered in printed form. The Card PIN may be accessed through the George mobile application and George Web application for retail clients.

Upon the Cardholder's request, or where the Cardholder is not a user of the George mobile application and George Web application, the Bank may issue the PIN in printed form.

The Bank shall guarantee the Card User PIN issuance secrecy until the provision of the Card. The User shall sign the Card immediately upon the receipt thereof as well as protect any data therein, and keep PIN in secrecy separately from the Card. The non-signed Card shall be invalid, and any financial consequences in the event of misuse of the non-signed Card shall be borne by the User.

The User must not disclose PIN to other persons (including, without limitation, family members, merchant, bank officer). In the course of imputing the PIN on the ATM or in POS terminal, privacy should be protected with hand, otherwise it should be prevented to be seen by others. Otherwise, the User shall entirely be liable for any transactions executed due to the non-compliance with this obligation.

The User must not leave Card as pledge or collateral or provide card to be used or be in possession of other persons, otherwise, the User shall bear full material liability for any transactions executed due to the non-compliance with this obligation.

In the event the User suspects that anyone is aware of his PIN, he shall undertake to change the PIN at the Bank ATM or request card blocking or making of new card or new PIN in writing. Otherwise, the complete risk of PIN fraud shall exclusively be borne by the Holder of the Account the Card is tied to.

The User acknowledges that he is aware that the Bank will not, for security reasons, request the User to confirm data on the Card, electronically or by telephone, otherwise the User shall fully bear risks and consequences of identity theft and unauthorised use of data from card due to the provision of data on the Card as mentioned above.

Card Use

Consent for payment transaction execution shall be provided by the Card User prior to the payment transaction execution in one of the following manners:
Reading the chip by inputting the card in the reader and inputting the PIN code on the ATM or in the POS terminal, by contactless reading of the chip at ATM and input of PIN, by contactless reading of the chip, including and excluding PIN input, at the merchant's point of sale, in accordance with the restrictions for contactless payments by the Card organisation; using the card within digital wallet in the manner described in Part 6A.3 hereof; reading of magnetic tape or inputting the security elements required by the Payee (card number, validity date, CVV2/CVC2 code) for particular

POS terminals, including and excluding slip signing; in the event of the payment transactions where physical presence of the card is not necessary (Internet transactions, orders by e-mail or telephone) by inputting the security elements required by the Payee (card number, validity date, CVV2/CVC2 code). To verify the User's authenticity, the Payee may request an additional authentication of the User by inputting the One Time Password on the Internet points of sale providing payment using 3D service. Inputting an OTP password obtained through SMS, the User confirms the consent to debit the payment on the User's account, or via push notification and entry of PIN or biometric data for the George mobile application users.

To verify the User's authenticity, the Payee may request an additional authentication of the User by inputting the One Time Password on the Internet points of sale providing payment using 3D service. Inputting an OTP password obtained through SMS, the User confirms the consent to debit the payment on the User's account.
User authentication for transactions executed at on-line points of sale that enable payment using the 3DS service, for users of the George mobile application, is performed via a push notification within the George mobile application (with the entry of a PIN code or biometric data), whereby the user's consent for executing the payment debiting their account is confirmed.
User authentication for transactions executed at on-line points of sale that enable payment using the 3DS service will **solely** be made via a push notification within the George mobile application (with the entry of a PIN code or biometric data), whereby the user's consent for executing the payment debiting their account is confirmed. To be able to make payment using a card on the aforementioned on-line points of sale, the Card User must have an activated George mobile application, in accordance with item 12.1.3 and 12.4 of the General Terms of Providing Payment Services to Private Individuals and Registered Farms.

The Card User may also grant consent for payment transaction execution through payee and payment initiation service provider.

Data on the card registered for payment on a web site MAY be replaced with new card data following the activation of the re-issued card if such process is initiated by the Internet merchant with the card company.

Credit card user may not make transfer from credit card to current account or make payments by transfer of funds from the card to other accounts (through E-Bank/M-Bank) or withdraw funds from the card at the Bank teller desks.

The Bank shall not be liable if merchant does not want to accept the Card though logo of the payment card brand is displayed or if, due to incorrect terminal use and/or technical problems, it is not possible to execute transaction upon the User's request.

The User shall, upon the request of goods and service seller (hereinafter: Acquirer) provide the Card whose right of use has expired.

The User shall, when paying for goods and services, also sign appropriate slip at acquiring point. Acquirer shall issue slip/account copy to the User.

The User shall not use the Card for illegal purposes, including purchase of goods and service the sales of which is prohibited by the law in the territory of the country the Account Holder is in at the time of transaction. The User shall assume full liability in the event of an illegal purchase using the Card subject hereto.

The User must not conclude fictive cashless transactions with Acquirer with the aim of obtaining cash.

The Card whose validity period has expired must not be used, otherwise the User shall be fully liable for any transactions executed due to the non-conformance with this obligation.

The Bank shall, for security reasons, set out cash amount limit and the amount of goods and service payment which may be used at ATMs and POS terminals on a daily basis. The limits for the card use by the persons authorised by

the User shall be set out by the User in the Card Issuance Application. The User shall be entitled to request the change in daily limit level, by submitting application for the limit change, without any obligation of the execution of the Annex to the Framework Agreement.

In the course of the contactless transaction execution, there is a possibility that a POS terminal does not request either the PIN input or the User's signature. Card organisations, based on their rules, determine the maximum limit up to which it is not necessary to input the PIN for contactless transactions. Occasionally, for security reasons, the User may be requested to execute a transaction in the same manner as when paying for goods and services at a POS terminal for chip card acceptance, by entering the PIN code.

If currency exchange is made when the card is used, currency exchange rate shall be set out in accordance with these General Terms and Conditions for Payment Service Provision.

The Card validity period shall be embossed on the card. The Card shall be valid until the last day in the stated month. If the User is in compliance with the provisions of the Framework Agreement, upon validity period expiry, he shall be automatically re-issued the Card, at the fee provided for in the Price List. The Card User shall be entitled to, within 30 days prior to the Card validity, state unless he wants to be re-issued the card.

The User is aware that the amount of the provision may differ from the debit amount. In the course of the execution of payment transactions using payment card, users should also take into consideration that the date of account debit can differ from the payment transaction occurrence date for this payment transaction type.

In the event of rejection of on-line transactions executed with Debit Card (Card not present transactions), the Bank notifies the User on the rejected transactions via SMS notifications.
Notifications will be sent via SMS solely to the telephone number reported in the bank system.

Currency Exchange Rate

When exchanging the local currency into foreign currency, foreign currency into the local currency, and foreign currency into other foreign currency, the Bank shall apply the exchange rate from the Bank Exchange Rate List, applicable at the time of exchange unless otherwise is agreed by the parties on a case-by-case basis.

In the event payment card is tied to RSD Account, for the costs incurred using the card abroad, the Bank will convert the amount of such transaction in FX into RSD as follows: MasterCard International or Visa International will convert original amount in EUR at Referential Exchange Rate, and from such amount, RSD value will be calculated at the selling exchange rate for FX of the Bank for EUR, applicable on date of debiting.

In the event the card is tied to FX account, for transactions executed in RSD, the Bank will convert RSD in the currency of the Account, at the Bank’s buying exchange rate applicable on date of debiting.

In the event the card is tied to FX account, for transactions executed in RSD, if original transaction currency is one of the currencies from the Bank’s exchange rate list, identical to the currency of the Account – the account shall be charged in the amount of the original currency.

In the event the payment card is tied to the foreign currency account, if the original transaction currency is listed in the Bank's exchange rate list and differs from the Account currency, such account shall be debited in the currency of the Account, whereby the conversion shall be made based on the following sequence: at the Bank's selling exchange rate valid on the date of debiting, transaction amount in the original currency shall be converted into RSD equivalent, after which the dinar amount shall be converted into the Account currency at the Bank's buying exchange rate.

If the card is tied to the foreign currency account, whereby original transaction currency is not listed in the Bank’s exchange rate list and differs from the Account currency, MasterCard International or Visa International shall convert the original amount into EUR, from which amount the Bank will, at the selling exchange rate of the Bank valid on the date of debiting, calculate the dinar equivalence, and from such amount, at the buying exchange rate of the Bank, calculate the countervalue in the currency of the Account, and debit the Account by such amount. MasterCard and Visa exchange rates shall be publicly available on web pages www.visaeurope.com and www.mastercard.com and

they shall be variable during day, while the Bank exchange rate lists shall be available on the Bank Internet page and at all branches.

Complaints regarding Card transactions

The User shall keep the copy of a slip/account for the purposes of complaint, if any. The User shall, immediately upon becoming aware thereof, but no later than 15 days from the receipt of statement and/or date of debiting and or date of the deadline for the execution of transactions in the event of non-executed transactions, submit any complaints regarding non-approved, non-executed, and incorrectly executed transactions in writing in the prescribed form, by sending a message within the E-Bank and M-Bank, by e-mail at **info@erstebank.rs**, by telephone at no. **0800 201201** (whereby the complaint will be sent in writing as soon as possible), or at the closest point of sale of the Bank. Any complaints which are not filed within the prescribed deadline and form shall not be accepted by the Bank, and the financial loss shall be borne by the User.

For the complaints relating to the quality of goods and services paid with the Card, the User shall solely address the Acquirer.

Lost/Stolen/Misused Card

The User shall immediately, upon becoming aware thereof, report Debit Card loss/theft/misuse to the closest Bank branch, by telephone number **021/67 72 116** or sending the e-mail from the address of the User reported to the Bank, to e-mail address sigurnost.kartice@erstebank.rs The Card User shall state the Debit Card number or his personal number in order for the Bank to disable any further use thereof, and, in the event of an unauthorised payment transaction or authorised payment transaction which is the consequence of fraud or misuse, to immediately take any reasonable measures for the purpose of funds recovery.

The Card found after reporting loss must not be used and cut card must be returned to the Bank in order to be destroyed.
The User shall, without any delay, report any damage and deficiency of the Card to the Bank in the manner provided for in lost card report.

In the event of an unauthorised use of the Card and/or data from the Card, resulting in the execution of an unauthorised payment transaction, the User shall, immediately, upon becoming aware thereof, but no later than within 15 days from the date of debiting, report to the Bank any transactions executed based on any unauthorised use of the Card and/or Card data .

The Bank shall be returned by the User a damaged, technically deficient card for which he suspects that it has been used in an unauthorised manner. If, after the report of lost card, the card is found, the User shall return it, without delay, to the Bank for the purpose of destruction.

The Bank shall provide the User with the evidence that the Bank has been notified by the User, in accordance with item paragraph 1, if the Payment Service User has filed the request for the submission of such evidence within 18 months from the date of this notice.

Liability for Damage

The User shall bear any losses resulting from the execution of any non-authorised payment transactions if such transactions have been executed due to the User's fraud or his failure to meet the obligation of taking any reasonable and appropriate measures for the purpose of protecting personalised security elements of the card due to his wilful intention or gross negligence.

The User shall bear any losses relating to any transaction executed due to fraud committed by the User and the losses resulting from the failure to meet his obligations, resulting from these General Terms. misuse

The User shall not bear any losses resulting from the transactions executed upon reporting any loss, theft, or unauthorised use of the Card and/or data from the payment card unless the User has committed or participated in a fraud or acted with the intention of committing fraud.
Regarding the Card which may be used for making the Internet payment, unless the site on which payment is made supports 3-D Secure protection mechanism, the User may be exposed to higher risk of the misuse of the Card data and/or transaction elements.

If data from the card are used by the User with a view to executing telephone, e-mail, or postal purchase, the User may be exposed to an increased risk of misuse of the data from the Card and/or transaction elements.

The User shall have limited liability up to the amount of RSD 3,000 if any unauthorised payment transactions have been executed due to the use of the lost, stolen, or misused Card.

Protective and other Measures

The User shall use payment card in accordance with these General Terms governing the issuance and use of such an instrument.

The User shall, immediately upon card receipt, take any reasonable and appropriate measures to protect personalised security elements of such an instrument (PIN, card number, etc.).

The User shall, immediately upon becoming aware of loss, theft, or fraud of payment instrument, report the Bank thereof.

The User must not make personalised card elements (e.g. by forwarding card image, sending card data by SMS or via message through social networks, etc.) available to any other person. In such case, it shall be deemed that the User has acted in gross negligence, and the User shall bear all material consequences resulting from such use of the card.

The User must not write the PIN on the card or on any medium he carries with the card.

If Internet payment is enabled using the Debit card, unless the site on which payment is made supports 3-D Secure protection mechanism, the User is, based on such payment, exposed to higher risk of possible misuse of the data from the Debit Card.

If the User deals with i-commerce, the User must not communicate the card data to the customer (save for the account number). If data misuse and/or unauthorised transactions occur in such case, it shall be deemed that the User has acted in gross negligence and shall bear material consequences of such executed transactions.

If the User receives an SMS to authorise a payment transaction by inputting the code/OTP password, but the User has not initiated such transaction, the User must not verify such transaction or forward the code to a third party, otherwise his account will be debited in the amount of such verified transaction.

When making a payment using the Card on the Internet, the User shall use only verified and well-known web pages

If the card is used in the course of purchase/sales on the Internet, the User must not, in the event the User is referred to other web site, or if the User receives a message to input the personalised elements of the card on another web site (e.g. the web site of the Postal Service of Serbia), act in such manner, because, in the majority of cases, though they may seem to be the official web sites, those are false web sites used for the misuse of the data from the card, and the User shall make prior check whether this is the web site referred to in the paragraph below.

Prior to inputting personalised card elements on merchant's web site, the User shall make prior check whether this is a protected Internet connection i.e. whether a padlock or key is shown at the bottom of the web site, because those are the signs of the protected internet connection. The beginning of the web address of a merchant for protected internet connection is “https” instead of “http”.

If the User notices anything suspicious on an ATM (e.g. additionally installed equipment, advertisement box), the User shall wave the transaction and notify the closest Bank branch thereof.

Unless the Card is returned from an ATM for an unknown reason, the User should not go away from the ATM, and the User should immediately notify the Bank contact center to determine the reason of keeping of the Card.

If a POS terminal is remote, the User shall insist to be enabled by the Merchant to execute the transaction solely at the User's presence.

It is recommended that the User should, for the purpose of prevention of fraud, be informed on the security rules of using payment cards on the web site of the Association of Serbian Banks **www.ubs-asb.com/korisnici-finansijskih-usluga/bezbednost-bankarskih-klijenata**.

The User shall, on a regular basis, follow notices on the Bank's web site relating to warnings in connection with the possibilities of payment card misuse (phishing etc.) and act accordingly.

Payment Instrument Blocking

The Bank shall block the further use of the card, completely or partially (for certain transaction types based on certain parameters) if there are reasonable grounds regarding payment instrument security, if there is suspicion of unauthorised use or fraud relating to the payment instrument, or as the consequence of fraud, or if there is an increased risk that the User will not be able to meet the payment obligation when the use of such instrument is related to the approval of loan and/or overdraft to the User (blocked account the card is tied to, etc.).

The Bank shall notify the User on its intention and reasons of payment instrument blocking. Unless the Bank is able to notify the User thereof prior to payment instrument blocking, the Bank shall do so immediately upon blocking. Notification on the intention of blocking i.e. payment instrument blocking shall be provided with the User by the Bank in the manner set out in the framework agreement unless provision of such notification is prohibited based on the regulations or in the event of reasonable security grounds.

The Bank will ensure re-use or replacement of the payment instrument with a new one – when the grounds for blocking thereof cease.

DIGITAL CARD AND DIGITAL WALLET

Digital Wallet Service Provider – local or foreign legal entity providing digital wallet service, with which the Bank has set up business cooperation to enable its users to add and use the payment cards issued by the Bank in the form of Digital Card (Apple Pay, GooglePay, etc.).

Digital Wallet – software solution by the Digital Wallet Service Provider used for mobile payments, enabling adding of payment card(s) to the application for the purpose of their digitalisation and use at points of sale, at ATMs, as well as on web pages and applications of merchants supporting this payment method. Digital Wallet is an application with which a client can make payment on POS terminals having the option of contactless reading, both in Serbia and abroad, through the devices having NFC (Near Field Communication) wireless communication, as well as in the applications and web pages of the merchants accepting this payment type for specific digital wallet Service Providers.

Digitalised Card – personalised security element in the Digital Wallet that is generated in the process of the digitalisation of valid Bank payment card, which can be used as a payment instrument for initiating and executing payment transactions at points of sale, on web pages and applications of the merchants supporting this payment method. The Bank enables the digitalisation of VISA and Mastercard debit and credit payment cards issued by Erste Bank to private individuals and legal entities, entrepreneurs, and registered agricultural holdings.

The Bank shall be entitled to, during the Card validity and/or in the course of automated Card re-issuance change the type of the Card of same or other payment brand, in which case, the Card used by the User will be replaced without any additional costs and the functionalities corresponding to the functionalities of the replaced card will be ensured.

Use of Digital Wallet Functionality

To use the digital wallet functionality, a User is required to:

- Have a device with the NFC technology, supporting the digital wallet service and/or a device compatible with relevant application (hereinafter: adequate device),
- download and install the Digital Wallet application on an adequate device unless such application exists on such device,
- connect the downloaded Digital Wallet application with his/her account on the adequate device,
- set the device closing using one of the methods enabled on the device (pattern, fingerprint, PIN code, face scanner, etc.).

In order to avoid doubt, solely digital wallet Service Provider shall determine the type and characteristics of the device on which it is possible to install the application and arrange the Digital Wallet service provision. Use of the digital wallet functionality is requested by a client selecting an option for adding card and accepting these Terms and Rules in the digital wallet application.

The Bank has enabled its clients the digitalisation of the VISA debit and/or VISA credit card and Mastercard debit and/or Mastercard credit card (hereinafter: Card) issued by the Bank to its Users.

Payment Card Digitalisation Process

In order for the User to add the existing Card issued by the Bank into previously downloaded and activated Digital Wallet application, the User is required to:

- hold an activated valid Card,
- have a mobile telephone number of the mobile operator registered in the Republic of Serbia, recorded in the Bank's system,
- when adding the card in the Digital Wallet, insert the data necessary for the Card digitalisation into relevant fields (card number,
  valid thru date, and three digit CVV code).

During the card digitalisation process, the Digital Wallet application may overtake certain data from the Client's account (name, surname, state, address of residence, zip code, apartment number, and telephone number), which the User confirms or changes, as necessary. The Bank shall not have access to the aforementioned data.

Following the payment card registration, the User shall receive one-off verification code (SMS OTP) sent to the mobile telephone number registered at the Bank. With a view to successfully completing the process, the Client shall input the received code into the field provided for the input in particular box. User shall not bear the digitalisation expenses.

Digitalised Card Use

Using a digitalised card, the User may perform secure payment at stores, in applications, and web sites supporting and accepting this payment method.

Consent for the execution of a payment transaction initiated by using Digitalised Card in Digital Wallet shall be granted by the User by tapping relevant devices on POS terminal or by selecting the payment option using the Digital Wallet on the web point of sale and inputting personalised security elements determined by the user or arranged with the Service Provider.

For any transactions executed with the Digitalised Card, the Bank will debit the User's account it is tied to the Card registered in the Digital Wallet.

For payment transactions executed with the Digitalised Card, if they are provided for in the Bank Price List, collection of fees shall be made in the same manner as if a transaction is initiated with the Client's physical Card.

Since a User is able to add more than one payment cards in the Digital Wallet, historically first card added by the User into the Digital Wallet shall become a default card for making payments. If the User wants to make payment using another digitalised card, it is necessary to select it before payment transaction initiation. In the Digital Wallet application, the Client can subsequently adjust and change the default card.

If, for any reason whatsoever, the agreement based on which the User has been issued the Card based on which the Digitalised Card is generated is terminated or the Bank, for any reason whatsoever, denies the right of Card use (blocks the card), the Digitalised Card use shall be terminated at the same time.

Deletion of the Digitalised Card from the Digitalised Wallet shall not impact the possibility of the use of the Card based on which a Digitalised Card has been deleted and if the User subsequently wants to use his/her card as a Digitalised Card, it can be re-registered in the Digital Wallet.

Deletion of the Digitalised Card from the Digital Wallet shall not release the User of his/her obligation to settle all liabilities arising from the use of such Digitalised Card prior to deletion.

Obligations of the User

To prevent any cases of unauthorised use of the Digital Wallet and digitalised card as well as any fraud, the User shall:

- protect the relevant device on which the Digital Wallet application is stored against any unauthorised access and/or use, keep it with due care with a view to preventing loss or theft and setting locking of the relevant device using one of the methods enabled on the device (pattern, fingerprint, PIN code, facial scan, etc.).
- the User shall not reveal or make available to third parties any data on the card and account the digital wallet is tied to, in particular the OTP code received in SMS, security elements from the payment card – card number, CVV on the back of the card. Revealing the data, the User acts in gross negligence and is exposed to the risk of the Card/Digitalised Card misuse, which could result in unauthorised transactions up to the amount of the funds available on the account the Card/Digitalised Card is tied to, and the Bank shall not be liable to the User for any arisen damage.
- immediately upon becoming aware thereof, the User shall notify the Bank on any event the consequence of which is loss, theft, unauthorised access, or use of a relevant device on which the Digital Wallet application is stored, misuse of the Card/Digitalised Card/Digital Wallet, by contacting the Bank's Call Center on number **021/6772116** or via e-mail address **sigurnost.kartice@erstebank.rs**, in order for the Bank to prevent any further use of the Digitalised Card, and, in the event of an unauthorised payment transaction or authorised payment transaction as the consequence of fraud or misuse, take any reasonable steps for the purpose of funds recovery
- the User shall not permit any third party to use the Digital Wallet for executing transactions.
- the User shall not register his/her Digitalised Card on the mobile telephone or other relevant device of a third party;
- the User shall comply with other protective measures stated herein, which relate to the Card.

Obligations by the Bank

Starting from the fact that the Bank issues the Cards to the Client that the Client may digitalise in his/her Digital Wallet, the Bank shall, pursuant to the provisions of the Law on Payment Service, ensure the following:

- personalised security elements of the Card are made available solely to the User whom the Bank has issued such Card;

- the User may, at any time, notify the Bank on loss, theft, or misuse of the device on which the digitalised

card is stored or request re-enabling of the Digitalised Card when conditions for blocking thereof are terminated, by contacting the Bank's Call Center at number **021/6772116** or to e-mail address **sigurnost.kartice@erstebank.rs**;
- prevent any further Digitalised Card use after the User has notified the Bank on loss, theft, or misuse of the device on which the Digital Wallet application is stored, or on the Digitalised Card misuse.

Termination or Restriction of the Rights of Digitalised Card Use

The Bank shall, at any time, be entitled to prevent adding of the Card in the Digital Wallet and/or permanent or temporary Digitalised Card use if any of the following conditions is met:

• in the event of suspicion that an unauthorised person tries to add the card in the Digital Wallet;

• if, in the process of adding a Card into the Digital Wallet, the Bank obtains an information that the Mobile Device to which the Card is added has been lost or stolen;

• if the Bank prevents adding of such Card type into the Digital Wallet or the Bank does not further permit adding of the card into the Digital Wallet of the service provider;

• if there is a suspicion of an unauthorised use of the Card and/or Digitalised Card, and/or Card use with the intention of fraud;

• in the event of blocking or expiry of the Card based on which the Digitalised Card has been created;

• upon the User's request.

Card blocking and/or prevention of use by the bank shall also apply to the Digitalised Card, created based on the Card. Digitalised card blocking must not result in blocking of the Card based on which the Digitalised Card is created. If the digital wallet Service Provider, for any reason whatsoever, prevents the User to add and use the Bank's Digitalised Card, the User may also contact the Service Provider. The Bank is not able or obligated to impact the Service Provider in terms of the availability of the Digital Wallet service for the User.

General Provisions

The Bank shall not be liable for the Digital Wallet application functionality:

- if lack of the functionality of the Digital Wallet has occurred on the side of the digital wallet Service Provider, which could not be impacted by the Bank, while such lack of functionality does not relate to the part of the Bank's application for payment service provision
- when a User fails to meet the prerequisites for the Digital Wallet application, in particular those referred to in Section Use of Digital Wallet Functionality herein;
- in the event of defects or deficiencies of the User's equipment, network, or other in other events that prevent the Digital Wallet use.

The Bank shall, in accordance with and to the extent set out in the provisions of the Law on Payment Services, be responsible for the operation of the Digital Wallet application if the circumstances, interruptions, or errors result in an unauthorised, non-executed, or incorrectly made payment transaction or cause a damage to the User. In the event of loss, misuse, or theft of the data necessary for the use of the Digital Wallet or in any other case of unauthorised use of the Digital Wallet, the Bank shall reserve the right to replace the card.

In the event of suspicion about the misuse of the Card data, possibility of the misuse by the Client, or execution of unauthorised transactions received from the card association, the Bank shall be entitled to unilaterally disable further possibility of the digitalised card use.

Closing Provisions

If the User has any issue regarding the functionality use, the User can contact the Bank's Call Center via the following telephone number: **0800201201.**

The Bank shall not process the User's personal data in the process of card digitalisation and does not obtain any such data.

Inputting the personal data and initiating the Card digitalisation in the Digital Wallet application, the User shall provide the aforementioned personal data to the digital wallet Service Provider, in accordance with the rules and notice on personal data processing defined by the digital wallet Service Provider for the purpose of the card digitalisation.

Provisions herein relating to the liability for damage, protective and other measures, and payment card blocking shall accordingly apply to the Digitalised Card/Digital Wallet, as well.

Applicable agreement provisions referred to in the framework agreements executed with the payment service users and/or provisions of the General Terms relating to the Card use issued by the Bank, as well as the provisions referred to in the General Terms relating to unauthorised, non-executed, or incorrectly executed payment transactions arisen from the digital wallet use, shall apply to any rights, obligations, conditions, and responsibilities of the Digital Wallet use not defined herein.

E-BANK AND M-BANK

NovoKlik, Office Banking, and Erste eBiz (hereinafter: E-Bank Services) shall be the E-Bank services provided by Erste Bank a.d. Novi Sad (hereinafter: Bank).

Erste mBiz (hereinafter: M-Bank) means the mobile banking service of Erste Bank a.d. Novi Sad (hereinafter: Bank).

Use of Erste eBiz service is conditional upon the use of Erste mBiz service and it may not be agreed or used as a single service.

E-Bank and M-Bank shall enable the user to execute and review payment transactions and review account balance.

The options, rights, and obligations of using each of the E-Bank services are defined herein.

- Smart card means a security device with installed chip, on which the e-certificate and cryptographic keys necessary for e-banking service are stored. Smart card shall be used for the electronic identification within the card validity period.
- Smart card reader means a device for reading data from smart card.
- Personal number (PIN) means a combination of characters assigned to the User by the Bank which, together with smart card, ensures the use of e-banking.
- User identification means a set of elements necessary for E-bank service identification and use username
- The username is a parameter comprising particular number of characters, received by the User when Erste eBiz service is registered, and used for the authentication to such service.
- mToken means a solution within the Bank’s mobile application generating one-off authentication or authorisation codes and enabling log-in and verification of the account in the eBiz application.
- Registration and activation code – combination of numbers and letters, assigned to the User by the Bank.

E-Bank and M-Bank Service Use Agreement

The E-Bank and M-bank service user may become any entrepreneur and private individual performing registered activity holding the current account at the Bank (hereinafter: User), which provides the Bank with correctly filled-in and signed Application Form, which shall be an integral part of the Framework Payment Service Provision Agreement, and accompanying documentation for the approval of the E-Bank and M-Bank service use, or flags the respective field in the Account Opening Application.

The Applicant shall, by filling in certain fields of the Application Form, determine the level of authorisation of the persons accessing the E-Bank and M-Bank services. All persons listed in the Application Form shall confirm the accuracy of stated data with their signature. The authorised person shall, with his signature and stamp, guarantee the provision of authorisation to authorised users, and, at the same time, grant authorisation to the users with the right of verification

to arrange additional functionalities through the E-Bank and M-Bank services. Any authorised person shall have certain authorisation type for the E-Bank and M-Bank use assigned by the User's Legal Representative in the Application Form.

Use of the user identification submitted by the Bank shall be deemed as the consent for the use of the E-Bank/M-Bank.

Legal Representative may revoke granted authorisations and notify the Bank on any change in the level of the authorisation of the persons having access to the E-Bank and M-Bank services, by providing the bank with relevant notice.

E-Bank Services

The User may, at own choice, select using some of the E-Bank Services:

- NovoKlik
- Erste mBiz
- Office Banking
- Erste eBiz

M-Bank services:

- Erste mBiz E-Bank and M-Bank Service Scope
- Novoklik means Desktop user application enabling the User to view account balance, account turnover, account statement, execute payment using RSD (including instant – urgent payments) and FX payment orders on current date and on a future date, receive and send personal and general messages.
- Office Banking means Desktop user application enabling the User to view account balance, account turnover, account statements, execute payment using RSD payment orders on current date and liabilities payment on a future date (including instant – urgent payment orders).
- Erste eBiz service means a Web user application enabling the User to perform the following: access account balance, view account turnover statements, execute payment orders for RSD (including instant – urgent orders) and FX payment transactions on current date and on a future date, activate Erste mBiz m-banking service. The Bank shall enable the User to use all of the functionalities offered in the Erste eBiz application, and the User shall, at own discretion, determine which of the functionalities he wants to use.
- Erste mBiz service means a mobile application enabling the User to perform the following: access account balance, view account turnover, statements, execute payment orders for RSD (including instant – urgent orders) and FX payment transactions on current date and on a future date. mBiz service enables log-in to the eBiz application and order signing in the eBiz application by generating mtoken codes as the second authentication factor. The Bank shall enable the User to use all of the functionalities offered in the Erste mBiz service, and the User shall, at own discretion, determine which of the functionalities he wants to use.

The Bank shall reserve the right to change the volume and content of the E-Bank and M-Bank services on which the User shall be notified through the content of its web pages.

E-Bank and M-Bank Service Use

NovoKlik – Upon the approval of application form by the Bank, the Bank shall provide the User with the smart card reader, smart card, and personal identification number (PIN), and he shall receive instructions for downloading installation package and User Manual through link.

For the approval of the NovoKlik service use, the User shall, in addition to the Application Form, also sign the following documents:

In the event the User does not have an issued e-certificate for individual user, the User shall also provide the Bank with the following documents:

- General order for the issuance of the qualified and personal digital certificates for a legal entity

- Application for receiving digital certificate of legal entity (for each individual user for whom smart card issuance is requested).

In the event the User has already been issued Halcom e-certificate, the following is to be provided:

Confirmation in writing on the sameness of digital certificate for authorised single user.

If the User has already obtained the above-mentioned, the Bank will enable the User to use the existing smart card after the submitted documentation is approved by the Bank.

The User may begin using the service upon the installation of the programme in accordance with received instructions. The User may be provided with the necessary user support by an authorised person of the Bank.

Smart card shall be issued for the validity period of the e-certificate determined by issuer, and upon the expiry of such period, the e-certificate validity must be renewed. Card renewal means the issuance of new smart card.

Receipt and sending of E-invoices to NovoKlik service will be ensured upon the approval of application form by the Bank.

Office Banking – Upon the approval of application form by the Bank, the Bank shall provide the User with the smart card reader, smart card, and personal identification number (PIN), instructions for downloading installation package, and User Manual through link.

If the User has already obtained the above-mentioned, the Bank will enable the User to use the existing smart card after the submitted documentation is approved by the Bank.

The User may begin using the service upon the installation of the programme in accordance with received instructions. The User may be provided with the necessary user support by an authorised person of the Bank.

Smart card shall be issued for the validity period of the e-certificate determined by issuer, and upon the expiry of such period, the e-certificate validity must be renewed. Card renewal does not require that new smart card is issued.

Erste eBiz – Following the approval of the Application form by the Bank, the Bank shall provide the User with the username to the e-mail, and the User generates mtoken code in the mBiz application. Erste eBiz application may be accessed by the user with username and mtoken code generated in the Erste mbiz application. Erste eBiz application may also be accessed by the User with Halcom e-certificate and the password created in the course of the activation after PIN entry. Instruction on the Erste eBiz functionality use shall be available on the web page for the service activation.

Erste mBiz – After the consolidated application form is approved by the Bank for Erste eBiz and Erste mBiz service to the User, the registration code and activation code are sent to the User in the SMS to the registered mobile telephone number (hereinafter: user identification). The User shall start using the Erste mBiz service following the receipt of the user authentication and, when the Erste mBiz service is accessed for the first time, the User shall create mToken and generate a four-digit PIN used when logging on to the application. The instruction on the Erste mBiz functionality use shall be available on the web page for the service activation.

Following the Erste mBiz activation, the User may choose to log-in through offered biometric data as well as to grant consent to transactions in the same manner.

All of the forms of using the E-Bank and M-Bank services which are electronically executed applying the prescribed user identification shall be identical to signing.

The User shall fill in all orders and any necessary specifications in an orderly and accurate manner and authenticate them in the manner provided for in the user identification and specific application, taking available amount of funds on

accounts at the Bank into account, otherwise he shall bear the risk of non-execution, incorrect execution, and/or rejection of payment order execution.

The User may execute international payment transactions (for the E-Bank and M-Bank services supporting international payments), including the obligatory input of number and date of document based on which the international payment is executed (agreement, invoice, proforma invoice, etc.). The User is not obligated to provide the Bank with the original order. Documentation evidencing the grounds and obligation of payment to abroad shall be submitted by the User to the Bank by e-mail or E-bank (if the application supports such functionality), whereby the Bank shall be entitled to be provided with the original for examination.

The Bank shall guarantee to the E-Bank and M-Bank service User to freely dispose of funds on all demand accounts, opened based on the agreement entered into with the Bank, up to the amount of funds on account, also including overdraft on such accounts.

Payment order execution deadline shall be defined in the bank Cut-off Times.

The Bank shall not assume liability for the non-availability of the E-Bank and M-Bank services resulting from technical issues of computer equipment, breakdown, or disorders within telecommunication channels, power system outage, or as a consequence of force majeure, and it shall not assume liability for any damage resulting from any loss or destruction of any data and equipment of the User due to the installation and use of the E-Bank and M-Bank service.

Payment Instrument Data Protection – E-Bank and M-Bank Blocking and Liability for Damage

The User shall keep secrecy of the user identification and smart card and accept full liability for any obligations resulting from the attributes of the user identification and/or smart card. The User shall, immediately upon the receipt of the user identification, take any reasonable and appropriate measures for the purpose of protecting the personalised security elements of the user identification.

The User shall immediately and inevitably notify the Bank on any non-authorised use of his user identification, SMART card, or other security device and on any other form of security breach he becomes aware of and initiate blocking of the E-Bank and M-Bank service use if there are suspicions of any unauthorised use/fraud of user identification, in one of the following manners: initiating the e-bank service use blocking in the manner provided for in the application, in person at the Bank branch, or by calling contact center on 021/423-364 or 0800-201-201 on business days 8 a.m. – 5 p.m. and on Saturday 8 a.m. – 1 p.m. or by sending e-mail requesting blocking of the E-bank service to the e-mail address: blokadaplatnoginstrumenta@erstebank.rs, in order for the Bank to prevent any further use of the Digitalised Card, and, in the event of an unauthorised payment transaction or authorised payment transaction as the consequence of fraud or misuse, take any reasonable steps for the purpose of funds recovery.

The Bank may reject or delay transaction execution and/or block the use of the E-Bank and M-Bank service and any further use thereof if there are reasonable grounds relating to payment instrument security, in the event of suspicion of unauthorised use of payment instrument or the use thereof for the purpose of fraud, as well as in other cases required based on the security, or if there is an increased risk that the User will not be able to meet the payment obligation when the use of such instrument is related to the approval of loan and/or overdraft to the User.

The Bank will notify the User on the intention and reasons of blocking, and unless the Bank is able to notify the User thereof prior to blocking, it shall notify the User immediately upon blocking unless submission of such notification is prohibited under regulations or in the event of reasonable security reasons.

The Bank will automatically block the service use to the user if incorrect user data are input three times during login. In such case, the User may unblock service access in person in the Bank premises or by calling the User Support.

If the Bank, using special application, determines that the operating system used by the User for initiating payment transactions through the Officebanking/Novoklik/Erste eBiz and Erste mBiz is virus infected enabling an unauthorised person to access the security elements of the payment instrument and unauthorised use thereof, due to which payment instrument security is affected, the Bank will prevent any further use of NetBanking/Officebanking/Novoklik/Erste eBiz and Erste mBiz, and request the User to take actions to eliminate such virus.

The Bank shall not be liable for any damage arisen from the execution of unauthorised transactions for the reasons referred to in the above paragraph.

The Bank will ensure the re-use of the Officebanking/Novoklik/Erste eBiz and Erste mBiz service after the User takes actions upon its request, and after it is determined that there is no further threat to the security of the payment instrument use.

The User shall bear any losses resulting from the execution of non-authorised payment transactions if such transactions have been executed due to the User's fraud or his failure to be in compliance with the obligation of taking any reasonable and appropriate measures for the purpose of protecting personalised security elements of the user identification due to his wilful intention or gross negligence.

The User shall bear any losses relating to any transactions executed due to fraud committed by the User, as well as bear any losses resulting from the failure to meet his obligations resulting from these General Terms.

The User shall not bear any losses resulting from transactions executed after reporting loss, theft, or unauthorised use of the user identification to the Bank unless the User has committed or participated in fraud or acted with the intention of committing fraud.

The User shall have limited liability up to the amount of RSD 3,000 if unauthorised payment transactions have been executed due to the use of lost or stolen user identification, or the user identification has been misused.

The User shall be liable for the accuracy of all data of payment orders and bear the risk of inputting incorrect data and fraud of the E-Bank and M-Bank services in his own environment.

Special Security Actions Implemented by the Bank

For the purpose of protecting the security of Payment Service Users, the Bank conducts monitoring of payment transactions and, based on indicators and expert assessment, determines whether there are any security or safety threats, risks of unauthorised use of payment instruments, risks of executing unauthorised payment transactions, the presence of malware on devices through which the User performs payment transactions via electronic banking, suspicion of fraud and abuse, and any other indications that may suggest that the User’s funds are affected or that the User has already suffered harm.

If the Bank assesses that, for the purpose of protecting the User’s funds, it is necessary to take actions to eliminate the identified risks and security threats, the Bank has the right to:

– block the User’s account in order to prevent the outflow of funds resulting from the compromise of a card, eBank or mBank applications, or prevent misuse or fraud by third parties involving the User’s account funds,

- block payment instruments (cards, eBank, and mBank),

– refuse the execution of payment transactions it considers risky, or postpone their execution until it is verified with the User whether the transaction is unauthorised, or require additional authentication for such transactions,

- take other actions deemed as necessary with a view to protecting the User.

The Bank shall inform the User on its intention to implement, or of any already implemented, security actions, as well as of the reasons for taking such actions. If the Bank is not able to inform the User before taking the actions, the Bank is obliged to do so immediately after the measures have been taken unless providing such notification is prohibited by regulations or there are justified security reasons for not doing so. .

Where possible in the specific case, the Bank provides certain instructions to the User in order to eliminate the identified risks, and the User is obliged to provide additional information about the transaction and the circumstances relevant for assessing and mitigating the risks at the Bank’s request.

After the reasons for taking the actions cease to exist, the Bank enables the User to dispose of the funds in the account and use the payment instruments and informs the User thereof.

Protective Measures

The User executing payment transactions through E-Bank shall follow the security requirements:

- The User shall, on the devices from which E-bank services will be used, ensure licensed, properly configured operating system and software, as well as anti-virus programme, including set updating on a regular basis, and use of personal firewall programme is recommended, as well;

- access E-Bank application, use current Web browser version and set automated updating of the programme;

- the User shall not use the option that Web browser remembers username and password or other security element used for the E-bank application. It is recommended that the User changes password on a regular basis (e.g. on a monthly basis), and the User must not communicate the password to others. - When creating a password, frequent words, or personal data known to others should not be used (e.g. names of children, date of birth, telephone number, account number, etc.) should not be used. The User must not keep the password on his mobile devices;

- the User must not respond to messages (SMS or through social networks), requests in pop-up windows, and e-mails, or those otherwise received through the Internet, which require the disclosure of sensitive and confidential personal information, or data of financial nature.

– report to the Bank any loss or theft of mobile device, as well as change in the holder of the telephone number. Otherwise, the Bank shall not be liable for any cases of fraud.

- The User must not leave the E-Bank application turned on, and he shall be liable for the damage arising from the misuse by any persons from his environment.

- if the User notices any unusual operation or appearance of the E-Bank application, he shall immediately notify the Bank thereof.

The User executing payment transactions through M-Bank shall be in compliance with the following security requirements:

- on the devices from which M-Bank services will be used, security measures installed by the producer (such as jail break or root) must not be disabled.

Recommendations for safe M-Bank use:

- the User should activate the security functionalities offered by mobile device (for example, device screen locking after certain period of inactivity, biometric screen unlocking, etc.).

- use the programme for the protection against malware and viruses,

- the User should act carefully in the event of bluetooth connection with other devices and disable the Bluetooth connection when it is not necessary. In the course of connection of other device with mobile telephone, it is recommended to use a safe method of connection requiring PIN generation for determining the source device initiating connection. It is necessary to ignore any attempts of connection which are unknown to the User.

- the User should be cautious when his mobile device is connected to be charged on the devices of other people (such as desktop or notebook computers of others or ports for charging mobile devices in public places). By connecting mobile device to charging port, data and application on the device could be accessed under certain conditions, whereby the User is not aware thereof.

- on the devices from which M-Bank services will be used, security measures installed by the producer (such as jail break or root) must not be disabled; - The User must not leave the M-Bank application opened, and the User shall be liable for any damage resulting from the misuse by the persons from his environment.

The User must not respond to any messages in which the sender addresses the User on behalf of the Bank or asks the User to provide any of his personal data, user identification, account number, etc. The User is obligated to immediately report any such case to the Bank.

If the User notices any unusual operation or appearance of the E-Bank application, the User shall immediately notify the Bank thereof.

The User shall report to the Bank any loss or theft of mobile device, as well as change in the holder of the telephone number if it is used for executing payment transactions through the M-bank application. Otherwise, the Bank shall not be liable for any cases of damage and fraud.

The User shall follow the Bank web site on a regular basis, in particular, notices by the Bank in connection with the E-Bank and M-Bank services and adequately respond, in accordance with such notices.

The User shall, for the purpose of prevention of fraud, ensure to be informed on the security rules of using payment instruments on the web site of the Association of Serbian Banks: www.ubs-asb.com/korisnici-finansijskih-usluga/bezbednost-bankarskih-klijenata.

Notification and Complaints

The User shall be reported on payment transactions executed through the E-Bank and M-Bank services in the Statement delivered to the e-mail address reported to the Bank. The User accepts to receive additional notifications, of informative or other nature, through various Bank distribution channels.

The User may file complaint about a non-approved, non-executed, and incorrectly executed transaction set through the E-Bank and M-Bank, immediately upon becoming aware thereof, but no later than 15 days from debiting, or from the date of the term for the transaction execution, in the event of a non-executed / incorrectly executed transaction Complaint may be sent by sending a message within E-Bank and M-Bank, by e-mail to **info@erstebank.rs** or by telephone to **0800 201201** (whereby the complaint is to be submitted in writing as soon as possible), stating the number of the order, order execution date, and accurate and clear description of the transaction regarding which the complaint is filed. The receipt of the statement on the balance and changes on the account submitted by the Bank shall be the date of informing the User.

The deadline referred to in paragraph 2 of this sub-heading does not apply to the transactions defined in sub-heading Rights and obligations of payment service providers in cases of fraudulent or misused transactions.

Service Termination

The User shall be entitled to cancel the E-Bank and M-Bank service use, by filing request in writing within 30-day notice period which shall start to run from the date of request receipt. Prior to the expiry of such notice period, the User shall return any assigned user identifications and settle any outstanding liabilities to the Bank.

The Bank shall reserve the right to reject the User's Request for the E-Bank and M-Bank service use and may, at any time, withdraw any rights for using the E-Bank and M-Bank services if the User has failed to execute transactions through the Bank longer than 6 months, settle liabilities on a regular basis and at maturity, be in compliance with the General Terms, applicable regulations and instructions of the Bank, and if there are reasons of security protection due to the suspicion of the user identification fraud.

IV PAYMENT SERVICE PROVISION

Consent for Payment Transaction

Payment transaction shall be deemed authorised if the payer has granted consent for the execution of payment transaction or if payer has granted consent for the execution of a series of payment transactions such payment transaction is a part of.

Method of granting consent to the payment transaction execution shall depend on the payment instrument and order receipt channel.

The User shall give his consent for the execution of payment transaction initiated:

- at the Bank branches – by signing payment order (and using the stamp if the use thereof is arranged),

- through the E-Bank and M-Bank using one-off code sent by SMS, token, smart card, biometric data (fingerprint or facial recognition), or other security designation, and final transaction verification in the manner defined in the application for such service,

- by payment card, Reading the chip by inputting the card in the reader and inputting the PIN code on the ATM or in the POS terminal, by contactless reading of the chip at ATM and PIN input, by contactless reading of the chip, including and excluding PIN input, at the merchant's point of sale, in accordance with the restrictions for contactless payments by the Card organisation; using the card within digital wallet in the manner described in Part 6A.3 hereof; reading of magnetic tape or inputting the security elements required by the Payee (card number, validity date, CVV2/CVC2 code) for particular POS terminals, including and excluding slip signing; in the event of the payment transactions where physical presence of the card is not necessary (Internet transactions, orders by e-mail or telephone) by inputting the security elements required by the Payee (card number, validity date, CVV2/CVC2 code). To verify the User's authenticity, the Payee may request an additional authentication of the User by inputting the One Time Password on the Internet points of sale providing payment using 3D service. Inputting an OTP password obtained through SMS, the User confirms the consent to debit the payment on the User's account, or via a push notification within the George mobile application or entry of PIN or biometric data for the George mBank users.

- if a standing order or direct debit is arranged with the Bank or payee for the execution of single payment transaction or a series of payment transactions (standing order and direct debit)

- using digitalised payment card, by tapping relevant device on the POS terminal, or by selecting Digital Wallet payment option at web point of sale, and by inputting personalised security elements determined by the User or arranged with the Service Provider,

- by scanning the QR code on monthly bills or scanning the QR code at point of sale of merchant

- using the deep link technology. (when the technical conditions for this functionality are met)

-- through the payee and through payment initiation service provider)

- with a qualified electronic signature in the cloud – ConsentID – when signing a transfer order for the collection of an electronic promissory note in the Central Registry of Electronic Promissory Notes maintained by the National Bank of Serbia

Payment Order Types

Payment order may be incoming payment order, outgoing payment order, and transfer order.

Incoming payment order means a payment order used for incoming payments of cash to current account (payment of liabilities in cash or other cash incoming payments to the account of User or payee).

Outgoing payment order means a payment order used for cash outgoing payments from current account.

Transfer order means a payment order used for cash transfer from one current account to other current account.

Electronic payment orders shall include the same elements as payment order forms in hard copy.
Payment orders for payments in FX in Serbia and international payment orders, as well as payment orders in RSD and FX between non-residents and residents in Serbia are prescribed in the Law on Foreign Exchange Transactions, Decision on Conditions and Method of International Payment Execution, and Instruction on Implementing such Decision. Payment orders for payment between non-residents, residents, and non-residents in Serbia, and for payments abroad shall include Payment Order, Collection Order, and General FX Order. Documentation evidencing payment and/or collection grounds in accordance with the regulations shall be provided in addition to the above-mentioned orders.

Payment Order Receipt

The Bank shall receive payment orders through its distribution channels, in accordance with the provisions of account opening and maintaining agreement, provisions of General Agreements for payment services, and provisions of these General Terms (Erste NetBanking/Office banking/Novoklik/Erste eBiz and Erste mBiz, payment card issuance, etc.) provided by the Bank relating to such accounts.

The Bank may receive a payment order:

- by personal submission at the Bank branch, in writing;
- electronically through Officebanking/Novoklik/Erste eBiz and Erste mBiz, or by scanning and presenting QR code;
- Indirectly through the payee (using the payment card or through payment initiation service provider).

The Bank Procedure upon Order Receipt

The Bank shall determine the fulfilment of the conditions for an order execution at the time of receiving the order. If execution date is determined in an order in advance, the Bank shall verify the conditions for payment order execution at particular date of execution.

Orders referring an amount exceeding the amount set out in the Law on the Prevention of Money Laundering and Terrorism Finance must be provided together with the documentation confirming payment grounds. Original documentation shall be presented in original or certified copy to the Bank, and the Bank shall keep documentation copy.

The Bank shall be entitled to require the User to provide additional information relating to payment transaction if such obligation arises from the regulations governing the prevention of money laundering or terrorism finance or internal acts of the Bank passed based on such regulations.

Orders must be filled in legibly, clearly, and unambiguously. Any data required in the order form must be filled in, stating execution date and obligatory signature, respectively by granting consent depending on product and/or communication channel with the Bank.

Signatures on order must be identical to the signatures in signature specimen. If the User wants to use stamp in the operation with the Bank, it must be separated from signature in the order form, i.e. stamp imprint must not be put over signature.

Any orders issued through the E-Bank/M-Bank must be authenticated using the user identification elements by the person they have been issued to,

Payment code must be input in accordance with payment code list in such manner that code corresponds to payment nature.

Payments based on model 97 are input only if such model is pre-set by payee.

The User shall accurately sum up collective orders. The payee's account must be legibly and clearly completed.

The User shall be responsible for the accuracy and completeness of data in the order even in cases if the Bank is required to fill in the order in accordance with the User's instructions

The User shall be liable for the completeness and accuracy of data stated in payment order.

The Bank will not receive order if, until the time of receipt, it identifies deficiency of any of its elements or the existence of other important reasons.

Order Receipt Time

The time for payment order receipt shall be the moment when the Bank directly receives order from the User unless different agreement is made, or indirectly through payee.

Date when the Bank indirectly receives payment order from the User or when it is received through the payee shall be deemed the date of the initiation of payment transaction execution and execution condition verification.

If the payment service User and the Bank determine that payment order execution is to begin on a certain date or on the date at the end of a certain period or on the date when payer makes monetary funds available to his payment service provider – it shall be deemed that payment order is received on such determined date. Unless such date is business day of payment service provider, it shall be deemed that order is received on the next business day of such provider.

For payment transactions initiated using card, the time of order receipt means the moment at which the Bank has received the order of payee's payment service provider, after which the User's account will be debited in the amount of respective payment transaction.

Unless payment order receipt time is business day of the Bank and/or if the Bank has received order after particular deadline for payment order receipt in accordance with the Cut-off Times, it shall be deemed that such order is received on the next business day, save in the event of the instant payment when the rules for order execution apply based on the Cut-off Times for such payment type.

The User’s payment account cannot be debited prior to the receipt of payment order.

Payment Order Execution

The Bank will execute payment order if the following conditions are met:

- if order is accurate and/or contains the minimum data necessary for the order execution

- if there is cover on the account for the payment of the total amount referred to in the order and accrued fees and commissions, or the user executing incoming payment to its current account provides the Bank with the cash in the amount necessary for order execution and payment of the respective fees and commissions,

- if consent is granted for payment order as per agreement

The Bank may execute payment orders even when they do not include all prescribed elements, if it is found by the Bank that the elements referred to in the order are sufficient for the execution thereof.

Payment order may be incoming payment order, outgoing payment order, and transfer order. The Bank shall execute orders if all of the above-mentioned conditions are met, based on the time of receipt unless there are legal obstacles for the order execution.

The User shall be liable for the accuracy of all data in the Order and bear the risk of the input of incorrect data and fraud. Any damage arising from the non-compliance with this provision shall be borne by the User.

The Bank shall not be liable in the event when the Order is rejected in the payment system or in the IPS payment system of the National Bank of Serbia or when it is not possible to execute it correctly and in time due to the User's error.

Any orders referring an amount exceeding the amount set out in the Law on the Prevention of Money Laundering and Terrorism Finance must be provided together with the documentation confirming the payment grounds. Original documentation shall be presented to the Bank and the Bank shall keep the documentation copy.

Orders in which the User requires payments for which the obligatory submission of documentation is prescribed as the evidence and/or grounds relating to transaction shall be solely executed by the Bank if prescribed documentation is presented and if such documentation corresponds to the payment purpose referred to in the order.

If the User has issued several payment orders, and there are not sufficient funds for the execution of the order which has been, based on the sequence during the day, received earlier, the Bank will execute the payment order for which there is a cover on the account.

Payment Order Rejection

The Bank may reject order execution if not all of the conditions for order execution prescribed herein are fulfilled unless otherwise stipulated in the regulation or if payment service provider has a reasonable suspicion in terms of the authenticity of payment order or its particular elements.

The Bank cannot reject payment order execution, including payment order provided through provider of payment initiation, when all of the conditions set out herein are satisfied, save in the cases referred to in paragraph 1 of this item.

The Bank shall be entitled to reject order meeting all of the execution conditions if the execution thereof would be contrary to the regulations governing the prevention of money laundering or terrorism finance, or internal acts of the Bank passed based on such regulations.

In the event of instant transfer order, the Bank shall be entitled to reject such order if it receives a notification from the IPS system operator on the rejection of the execution of such order due to the failure to fulfil the conditions for the execution of such transfer, set out in the rules of such system. The Bank will not execute instant payment order in the event the payee's payment service provider is not a participant in the IPS system.

If a payment order is rejected by the Bank, it shall be deemed that the payment order has not been received. The payment service user shall be notified by the Bank on the rejection of payment order or initiation of payment transaction and, if possible, on the reasons of such rejection and procedure for correcting of the errors resulting in the rejection unless such notification is prohibited based on regulation.

The Bank shall provide the User with the notice on payment transaction rejection without delay, but no later than within the term set out for payment transaction execution.

Payment Order Recall

Payer may recall payment order – by providing the Bank with request for recall in writing or electronically depending on the method of the issuance of payment order recalled (amount, payee, payer, execution date, etc.), at the time and in the manner which ensure initiating of such recall prior to the execution of the instructions contained in such order provided that the Bank has not executed such payment order.

When Payer has specifically arranged the beginning of order execution with the Bank, order may be recalled no later than the closing time for order execution on the business day preceding the day arranged as the beginning of order execution and/or until the time of forwarding order to clearing.

When payment transaction is initiated by payment initiation service provider or payee or payer through payee – payer cannot revoke the payment order following granting of the consent to the payment initiation service provider to initiate payment transaction or granting of the consent to execute payment transaction to the payee.

For card-initiated payment transactions, payer may not recall payment order upon transaction authorisation and/or upon inputting PIN, and approve transaction.

In the event of an instant transfer, the payee may request the Bank to initiate the instant transfer refund from the payee's payment service provider due to the reasons provided for in the applicable regulations (e.g. the payer has executed instant credit transfer to an incorrect number of the payee's payment account, in an incorrect amount, etc.).

If the user recalls an order upon the expiry of the deadlines referred to in paragraph 1–3 of this Article, the Bank may take reasonable actions to prevent order execution while being in compliance with the applicable regulations and professional rules.

Recall of an order upon the expiry of the deadlines referred to in paragraph 1–3 of this Article may be charged by the Bank, in accordance with the Price List.

Upon the expiry of the recall deadline, payment service user may recall payment order only based on the agreement with the Bank or other payment service provider participating in payment transaction execution. If payment transaction is initiated by payee or payer through payee, payment order recall may not, upon the expiry of the deadlines referred to in paragraphs 1–3 of this Article, be executed without the payee's consent.

Payment Transaction Execution Deadline for Payer’s Payment Service Provider

Payment orders shall be executed by the Bank considering the time of order receipt in accordance with the Cut-off Times.

Order execution time shall be set in accordance with RTGS cut-off times and the National Bank of Serbia Clearing System.

Payment orders shall be executed in accordance with the time of receipt and execution date.

For domestic payment transaction executed in dinars, the Bank shall ensure that the value date of debiting the User's payment account in connection with the payment transaction execution is the same as or later than the date when such payment account is debited in the amount of payment transaction.

For domestic payment transaction executed in RSD, the Bank shall approve transaction amount on the account of payee's payment service provider on the same business day on which the Bank has received payment order.

In the event of domestic payment transaction up to RSD 300,000 initiated as an instant credit transfer, the Bank shall ensure that the transaction amount is instantly or almost instantly credited on the account of the payee's payment service provider, following the receipt of such an order.

In the event of international payment transactions or payment transactions in currency of third states, the Bank is not obligated to, prior to payment service agreement execution, deliver or make readily available information to the User relating to deadline for payment transaction of payment service provider of payee in a third country if, at the time of the execution of this agreement, such information is not available to the Bank. In such case, framework agreement relating to these transactions does not have to contain information on transaction execution deadline, and the Bank shall provide the payment service User with the information on expected time of payment transaction execution.

Execution of Payment Transaction to the Payee

The payee's payment service provider shall without undue delay credit the payee's payment account or, where the payee does not have a payment account with that payment service provider, make the funds available to the payee:

1) if the amount of the payment transaction for the payee has been credited to the payee's payment service provider’s account or if the payee's payment service provider received the amount in another way;

2) if the payee's payment service provider received all information necessary for crediting the payee’s payment account or making funds available to the payee.

Provisions of para 1 and 2 of this Article shall apply when payee’s payment service provider is, at the same time, the payer’s payment service provider.

After the payee’s payment account has been credited, the payee's payment service provider shall immediately make that amount available to the payee.

If the payment service user who is not a legal entity demands cash withdrawal from a payment account, the payment service provider shall pay him these funds free of charge without undue delay, but if the consumer is withdrawing cash in the amount exceeding RSD 600,000 or foreign cash in the equivalent of RSD 600,000 at the official middle exchange rate – the payment service provider may pay him these funds at the latest on the next business day.

If funds have been credited to the account of the payee’s payment service provider on the day which is not a business day for that provider, it shall be deemed that the payee’s payment service provider received the funds on the next business day.

Value Date and Disposal of Funds in the Event of Payment of Cash on the Payment Account

In case of a domestic payment transaction, where a payment service user places cash on its payment account with the payment service provider operating that account in the currency of that account, the payment service provider shall ensure that the value date of crediting the payment account is the date of the receipt of cash.

The payment service provider shall make the amount available to the payee immediately after the point of time of the receipt of funds, according to limits from paragraph 4 of the Article above.

Confirmation on the availability of funds

Upon the request of a payment service provider issuing card-based payment instruments, an account servicing payment service provider shall immediately confirm whether an amount necessary for the execution of a card-based payment transaction is available on the payment account of the payer, provided that all of the following conditions are met:

1) the payment account of the payer is accessible on-line at the time of the request;

2) the payer has given explicit consent to the account servicing payment service provider to respond to requests from a specific payment service provider to confirm that the amount corresponding to a certain card-based payment transaction is available on the payer's payment account;

3) the consent referred to in item 2) of this paragraph has been given before the first request for confirmation is made.

The payment service provider issuing card-based payment instruments may request the confirmation referred to in paragraph 1 of this Article where all of the following conditions are met:

1) the payer has given explicit consent to the payment service provider to request such confirmation;

2) the payer has initiated the card-based payment transaction for the amount referred to in paragraph 1 of this Article using a card-based payment instrument;

3) the payment service provider issuing card-based payment instruments authenticates itself towards the account servicing payment service provider before each confirmation request, and securely communicates and exchanges messages and data with the account servicing payment service provider in accordance with the regulation referred to in Article 75d of this Law.

The confirmation referred to in paragraph 1 of this Article shall consist only in a simple 'yes' or 'no' answer and not in a statement of the account balance. That answer shall not be stored or used for purposes other than for the execution of the payment transaction.

The confirmation referred to in paragraph 1 of this Article shall not allow for the account servicing payment service provider to block funds on the payer's payment account.

At the payer's request, the account servicing payment service provider shall inform the payer about the payment service provider which submitted the request referred to in paragraph 1 of this Article and the answer provided.

Rules on access to payment account in the case of payment initiation services

Where the payer's payment account is accessible on-line, the payer has the right to make use of a payment initiation service provider to obtain payment initiation services.

When providing the payment initiation service, the provider of this service shall:

1) not hold at any time the payer's funds in connection with the provision of the payment initiation service;

2) ensure that the personalised security credentials of the payment service user are not, with the exception of the user and the issuer of the personalised security credentials, accessible to other parties and that they are transmitted by the payment initiation service provider through safe and efficient channels;

3) ensure that any other information about the payment service user, obtained when providing payment initiation services, is only provided to the payee and only with the payment service user's explicit consent;

4) every time a payment is initiated, securely confirm its identity towards the account servicing payment service provider of the payer, in accordance with the regulation referred to in Article 75d of Law on Payment Services, and communicate and exchange data and messages with that account servicing payment service provider, the payer and the payee in a secure way;

5) not store sensitive payment data of the payment service user;

6) not request any data other than those necessary to provide the payment initiation service;

7) not use, store or access any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer;

8) not modify the amount of the payee or any other feature of the payment transaction.

When the payer gives its explicit consent for a payment transaction to be executed, in order to ensure the payer's right to use the payment initiation service the account servicing payment service provider shall perform the following actions:

1) communicate and exchange data and messages securely with the payment initiation service provider, in accordance with the regulation referred to in Article 75d of Law on Payment Services;

2) immediately after receipt of the payment order from a payment initiation service provider, provide or make available all information on the initiation of the payment transaction and all available information regarding the execution of the payment transaction to the payment initiation service provider;

3) treat payment orders transmitted through a payment initiation service provider without any discrimination other than for objective reasons, in particular in terms of timing and speed, priority or charges vis-à-vis payment orders transmitted directly by the payer.

The provision of payment initiation services shall not be dependent on the existence of a contractual relationship between the payment initiation service providers and the account servicing payment service providers for that purpose.

Rules on access to and use of payment account information in the case of account information services

Where a payment account is accessible on-line, the payment service user has the right to make use of account information services.

When providing the account information service, the provider of this service shall:

1) provide services only where based on the payment service user's explicit consent;

2) ensure that the personalised security credentials of the payment service user are not, with the exception of the user and the issuer of the personalised security credentials, accessible to other parties and that they are transmitted by the account information service provider through safe and efficient channels;

3) for each communication session, confirm its identity towards the account servicing payment service provider of the payment service user, in accordance with the regulation referred to in Article 75d of Law on Payment Services, and securely communicate and exchange data and messages with that account servicing payment service provider and the payment service user;

4) access only the payment accounts designated for the use of this service by the payment service user and information on associated payment transactions;

5) not request sensitive payment data linked to the payment accounts;

6) not use, store or access any data for purposes other than for performing the account information service explicitly requested by the payment service user.

When the payment service user gives its explicit consent for an account information service to be provided, in order to ensure the user's right to use the service the account servicing payment service provider shall perform the following actions:

1) communicate and exchange data and messages securely with the account information service provider, in accordance with the regulation referred to in Article 75d of Law on Payment Services;

2) treat data requests received from an account information service provider without any discrimination for other than objective reasons.

The provision of account information services shall not be dependent on the existence of a contractual relationship between the payment initiation service providers and the account servicing payment service providers for that purpose.

Limits of the access to payment accounts by payment service providers

An account servicing payment service provider may deny an account information service provider or a payment initiation service provider access to a payment account for objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access to the payment account by that payment service provider, including the unauthorised or fraudulent initiation of a payment transaction.

In the case referred to in paragraph 1 of this Article, the account servicing payment service provider shall inform the payment service user that access to the payment account is denied and the reasons therefor in the form agreed in the framework contract. If it is unable to inform the user thereof before access is denied, the account servicing payment service provider shall do so immediately after access to the payment account is denied.

By way of derogation from paragraph 2 of this Article, the account servicing payment service provider shall not inform the payer in accordance with that paragraph if providing such information is prohibited by regulations or would compromise objectively justified security reasons.

The account servicing payment service provider shall again allow access to the payment account once the reasons for denying access no longer exist.

Where the account servicing payment service provider denies access to a payment account in accordance with paragraph 1 of this Article, it shall immediately notify the National Bank of Serbia thereof and include the relevant details of the case and the reasons for denying access.

Based on the notification referred to in paragraph 5 of this Article, the National Bank of Serbia shall take appropriate measures in accordance with this Law.

Payment transactions where the transaction amount is not known in advance

If a payment transaction is initiated by or through the payee in the context of a card based payment transaction and the exact amount is not known at the moment when the payer gives consent to execute the payment transaction, the payer’s payment service provider may block funds on the payer’s payment account only if the payer has given consent to the exact amount of the funds to be blocked.

The Bank shall release the funds blocked on the User’s payment account without undue delay after receipt of the information about the exact amount of the payment transaction and at the latest immediately after receipt of the payment order.

Execution of payment transactions based on bills of exchange

A payment transaction on the basis of a bill of exchange is the payment transaction where the payee initiates a payment transaction for debiting the payer’s payment account on the basis of a bill of exchange and payment order requiring the transfer of funds from the payer’s to the payee’s account.

The bill of exchange referred to in paragraph 1 of this Article, including the electronic bill of exchange, shall be issued in accordance with the law governing bills of exchange and shall represent an irrevocable consent of the issuer given to its payment service provider to execute the payment transaction initiated by the bill of exchange holder in accordance with that paragraph.

If the bill of exchange referred to in paragraph 1 of this Article is recorded in the register of bills of exchange and mandates maintained by the National Bank of Serbia pursuant to regulations on enforced collection from funds in accounts, pursuant to these regulations the payee may initiate a payment transaction to debit the payer’s current account with any payment service provider servicing this account.

Provisions of Article 63 of Law on Payment Services shall not apply to payment transactions on the basis of bills of exchange.

Provisions of para 1–4 of this Article shall not exclude or impair the rights that a bill of exchange issuer, bill of exchange holder or other persons holding bills of exchange have under the law governing bills of exchange. In the case of an electronic bill of exchange, these rights can be exercised using the official statement of the electronic bill of exchange, instead of the original electronic bill of exchange.

The National Bank of Serbia maintains the central register of electronic bills of exchange, which is integral to the register referred to in paragraph 3 of this Article, and issues the statement referred to in paragraph 5 of that Article, which has the properties of an authentic and public instrument.

The National Bank of Serbia regulates in detail the electronic bill of exchange, the central register of electronic bills of exchange and the official statement of the electronic bill of exchange referred to in this Article, the recording of the electronic bill of exchange, its deletion and use within this register, access to the register and banks' obligations in relation to such access and use of electronic bills of exchange, and other matters relevant for the operation of this register.

Customer Operations with Electronic Promissory Notes

An electronic promissory note represents a dematerialized own promissory note in accordance with the law governing promissory notes, with a "without protest" clause. It is maintained, stored, and used as a set of data in electronic form within the Central Registry of Electronic Promissory Notes (hereinafter: the Central Registry).

The Central Registry is an integral part of the Promissory Note Register and constitutes a dedicated software solution managed by the National Bank of Serbia. It regulates the method of enforced collection from the Customer's account. The Terms of Use of the Central Registry (hereinafter: Terms of Use) define how electronic promissory notes are issued, how promissory note actions are performed, how they are registered and recorded in the Register, delivered to creditors, and used in other ways. The Central Registry also serves to centrally record and store data on electronic promissory notes and their usage in electronic form.

Access to the Central Registry is available to the Bank's clients who use the NovoKlik and E-Biz mBiz (Halcom) electronic banking applications.

The National Bank of Serbia establishes the Terms of Use and publishes them on its website, as well as within the Central Registry

Users agree to the application of the Terms of Use upon accessing and using the Central Registry.

Individuals listed in the User's Authorized Persons List (KDP) as of the effective date of these General Terms are considered authorized to perform all actions related to electronic promissory notes. This includes the right to register, issue, and sign promissory notes, as well as perform other related actions within the Central Registry. However, the User may initiate changes to the scope of authority by signing the Bank's prescribed form.

A new User, when opening an account, must indicate whether they wish to use electronic promissory notes and, using the Bank's prescribed form, define the scope of authority for the persons who will perform actions related to electronic promissory notes.

During the contractual relationship, the User may change the authorized persons or their level of authority for handling electronic promissory notes by signing the Bank's prescribed form.

When performing actions related to electronic promissory notes, the Bank's role is to verify the authority and identity of the persons performing those actions and to confirm to the Central Registry that they are authorized, enabling the actions to be executed within the Central Registry.

V INFORMATION AND COMMUNICATION METHOD BETWEEN THE BANK AND THE USER

Information in Pre-agreement Stage

The Bank shall, within reasonable term, prior to executing framework agreement, provide the User with the information stipulated in the law as the obligatory elements of such agreement, in such manner which will enable the user to become aware of the conditions relating to payment service provision, as well as to compare offers of various payment service providers and estimate whether these conditions and services meet his needs.

The Bank shall, within the appropriate term prior to the execution of the framework payment account agreement, at the same time when other information is provided as set out in the Law on Payment Services, provide the User with

the Overview of Services and Fees, free of charge – in hard copy or other permanent data carrier, in the manner ensuring the evidence on the executed delivery. The Bank will make the Overview of Services and Fees available at its teller desk facilities and publish it on the Bank's web site.

The Bank may provide the User with the information referred to in paragraph 1 of this Article by providing draft framework agreement which contains this information, in hard copy, or on other permanent data carrier. An offer the User is provided with in the form of draft shall be valid for three days from the date of delivery to the User.

Informing Payer prior to and upon Payment Transaction Execution

The Bank shall, prior to the execution of individual payment transaction initiated by payer based on framework agreement, provide the payer, upon his request, with specific information on deadline for the execution of such payment transaction and fees charged to him.

The Bank shall, immediately upon debiting the payer's payment account or upon the receipt of payment order unless the payer uses payment account, provide the payer with the following information: a reference or other data enabling the payer to identify each payment transaction and information relating to the payee; the amount of the payment transaction in the currency in which the payer's payment account is debited or in the currency that the payer has indicated in the payment order; the amount of any charges to the payer for the execution of single payment transaction and, if the payment service provider collects these charges in aggregate amount – the breakdown of the types and amounts of each individual charge making up the aggregate charge; if applicable, the interest payable by the payer; if currency conversion is applied – the exchange rate used by the payer's payment service provider in executing the payment transaction, and the amount of the payment transaction after currency conversion; the value date of debiting the payment account, and/or the date of receiving the payment order.

The Bank shall periodically provide the information referred to in the above paragraph on a monthly basis, by e-mail to the User's e-mail address. Unless the User has an e-mail address, statements with the information referred to in the above paragraph may be overtaken at the Bank teller desk.

The Bank shall provide the payer, upon his request, free of charge, in hard copy or other permanent data carrier, with the information on individual executed payment transactions, referred to in paragraph 2 of this Article, on a monthly basis.

Information to Payee upon the Execution of Individual Payment Transaction

The Bank shall, immediately upon transaction execution provide the payee with the following information: a reference or other data enabling the payee to identify each payment transaction, as well as the information relating to the payer and other data transferred with such payment transaction in accordance with the law; the amount of the payment transaction in the currency in which the payee's payment account is credited or in the currency in which the cash is made available to the payee; the amount of any charges to the payee for the execution of single payment transaction and, if the payment service provider collects these charges in aggregate amount – the breakdown of the types and amounts of each individual charge making up the aggregate charge; if applicable, the interest payable by the payee; if currency conversion is applied – the exchange rate used by the payee's payment service provider in executing the payment transaction, and the amount of the payment transaction after currency conversion; the value date of crediting the payment account of the payee, and/or the date of making funds available to the payee.

The Bank shall periodically provide the information referred to in the above paragraph on a monthly basis, by e-mail to the User's e-mail address reported to the Bank or to the e-mail address registered at the Business Registers Agency. Unless the User has an e-mail address, statements with the information referred to in the above paragraph may be overtaken at the Bank teller desk.

The Bank shall provide the payer, upon his request, free of charge, in hard copy or other permanent data carrier, with the information on individual executed payment transactions, referred to in paragraph 1 of this Article, on a monthly basis.

The Bank shall, upon the User's request, provide the User with the statement on all charged fees for the services connected to the payment account, minimum on an annual basis. (hereinafter: report on charged fees). Report on

charged fees will be delivered by the Bank to the user in accordance with the terms set out in relevant by-law of the National Bank of Serbia.

Communication Method

Unless otherwise agreed between the Bank and the user, communication during the agreement validity shall be made in the Serbian language.

The Bank and the User shall perform the communication as agreed: by exchanging notices and other letters by mail, with eBanking and mBanking application, by e-mail, SMS to the mobile telephone number provided by the User with the Bank; in electronic communication form (through Viber, WhatsApp, etc.), upon the explicit request by the User, by direct overtaking of a letter at Bank branch.

The User with whom the Bank electronically communicates shall meet minimum technical requirements for using electronic mail, as follows: possession of computer/mobile telephone, adequate operating system, hardware base, supporting respective E-Bank application, Internet browser, and possession of e-mail address.

The User shall notify the Bank in writing on any changes of personal data, and other data relating to the account, referred to in account opening application. The User shall be liable for any failures or damage arising from the failure to submit data on changes occurred.

In the event of fraud, suspicion of fraud, or security threats that may have a detrimental impact to payment service users (e.g. identity threat, phishing attacks, and BIN attacks, etc.), the Bank will perform security checks and inform the User thereof, by contacting the User personally using the contact data the Bank has been provided with, and if it is assessed that there is also a risk to other Users, the Bank will notify the Users thereof through its web site, messages within the eBanking and mBanking applications, electronically, by sending SMS messages through Viber/WhatsApp, in order to indicate to the Users, in the promptest and most efficient manner, how to act in connection with respective frauds and security threats.

VI FEES AND INTEREST RATES

Fees

For payment service execution, fees and commissions will be charged by the Bank in accordance with the Price List.

Commissions shall be defined in percentage amount, where the base for percentage application shall be the value of transaction defined by the User in an order the Bank is provided with. Commissions shall, in addition to percentage amount, always include defined minimum value in absolute amount designating the value of minimum calculated commission charged i.e. which must apply if lower value is obtained by applying percentage to value in order.

Commissions shall include defined maximum value in absolute amount designating the value of maximum calculated commission charged i.e. which must apply if higher value is obtained by applying percentage to value in order.

Fees shall be collected through the User's business account, on a monthly basis and they shall be clearly visible in Statement on Changes on Account. Commissions shall be collected upon the execution of every order by debiting the User’s account and be clearly visible in Statement on Changes on Account.

Collection of fees and commission shall, in the event the User lacks funds on account upon order execution, be made upon the first funds inflow to the User's account or at the end of the month when fee calculation and collection shall be made.

Unless there are sufficient funds on the account for the collection of fees and commissions, the account is maintained in the negative balance in the amount of overdue fees.

RSD account maintenance fee shall be charged if the User has had minimum one transaction on a monthly basis, save for the clients who have been approved specific tariffs, when the fee is charged irrespective of the number of transactions. Transactions include outflows from and inflows to the account, debits based on collection of other fees and liabilities of the User regarding other products (overdraft, loan, etc.).

Collection of fees for FX payments and covers for FX payments shall be made by debiting the User's account.

Unless there are sufficient funds for the collection of fees and FX cover referred to in the above paragraph, account will not be maintained in the negative balance.

The payer's payment service provider, the payee's payment service provider and the intermediary participating in the execution of a payment transaction shall, for the account of the payment service provider, transfer the total amount of the payment transaction specified in the payment order from the payer to the payee.

By way of derogation from the above paragraph, the payee and its payment service provider may set out that the payment service provider shall deduct its charges from the amount transferred before crediting it to the payee's account or making it available to the payee. In such case, payment service provider shall, upon the execution of payment transaction, single out the total amount of payment transaction and paid fee.

If, in the course of international payment transactions, the Bank charges fee to the payment service User for the execution of international payment transaction or payment transactions in the currency of third states are charged by other payment service provider or intermediary participating in the execution of these payment transactions – the Bank shall, prior to payment transaction initiation, notify the User on the amount of such fee. If, at the time of initiating payment transaction, it does not have available information on the exact fee amount, the Bank shall provide the User with the information on the expected amount of the fee.

Interest Rates

Interest may be accrued and paid by the Bank to the funds deposited on current or deposit account, in accordance with the agreement executed with the User.

Legal default interest in the amount and in the manner prescribed in the Law on Default Interest shall be accrued and charged by the Bank to the funds exceeding the limit of the account, as well as to the amount of the negative balance based on overdues towards the Bank.

VII LIABILITY FOR PAYMENT TRANSACTION EXECUTION

Liability for Non-approved Payment Transaction

The Bank shall be liable for the execution of payment transaction for which there is no consent by payer in accordance with the General Terms.

In the case of an unauthorised payment transaction, the Bank shall refund to the payer the amount of the unauthorised payment transaction immediately, and in any event no later than the following business day after noting or being notified of the payment transaction, except where the Bank suspects fraud or misuse by the User, in which case the Bank shall, within ten days from learning of an unauthorised payment transaction, take one of the following actions:

(1) provide an explanation to the User regarding the grounds for rejecting the refund and report fraud and/or misuse to the competent authority; or

(2) refund the amount of that transaction to the payer where, after further verification, it concludes that the payer did not commit fraud or misuse.

The Bank shall restore the payer's payment account to the state in which it would have been had the unauthorised payment transaction not taken place, so that the credit value date for the payer's payment account shall be no later than the date the amount of the payment transaction had been debited.

The Bank shall also refund to the payer all charges levied for the executed unauthorised payment transaction and refund and/or pay any related interest the payer would be entitled to if the unauthorised payment transaction had not taken place.

Where the payment transaction is initiated through a payment initiation service provider, the obligations defined in this Article shall apply if the Bank maintains the payer-s account.

Payer's Liability for Unauthorised Transaction

The Payer shall bear losses resulting from the execution of unauthorised payment transactions up to the amount of RSD 3,000 if such transactions have been executed due to:

1) use of a lost or stolen payment instrument, or

2) misappropriation of a payment instrument

The Payer shall bear any losses resulting from the execution of non-authorised payment transactions if such transactions have been executed due to the payer's fraud or failure to meet the obligation of taking any reasonable and appropriate measures for the purpose of protecting personalised security elements of such instrument due to his wilful intention or gross negligence.

If the payment service provider does not provide appropriate means of the notification of a lost, stolen or misappropriated payment instrument, the payer shall not bear any losses resulting from the use of that payment instrument, except where the payer has acted fraudulently.

The payer shall not bear any losses referred to in this Article if:

The payee will not bear losses referred to in this Article if:

1) the loss, theft or misappropriation of a payment instrument was not detectable to the payer prior to execution of an unauthorised payment transaction, except in the case referred to in paragraph 2 of this Article;

2) the loss was caused by acts or lack of action of an employee, agent or branch of a payment service provider or of an entity to which its activities were outsourced, except in the case referred to in paragraph 2 of this Article;

3) if the payment service provider does not provide at all times appropriate means of notification of a lost, stolen or misappropriated payment instrument, except where it has acted fraudulently;

4) where the payer’s payment service provider does not require strong customer authentication, unless the payer has acted fraudulently.

The payer shall not bear any losses resulting from unauthorised payment transactions executed after he has notified the payment service provider of the lost, stolen or misappropriated payment instrument, except where these losses occurred due to the payer acting fraudulently.

Liability for Non-executed or Incorrectly Executed Payment Transaction Initiated by Payer

If payment transaction is initiated by a payer, the payer's payment service provider shall be liable to the payer for the correct execution thereof up to the payee's payment service provider.

If the payer's payment service provider is liable for non-executed or incorrectly executed payment transaction, it shall, immediately upon being aware thereof, refund the amount of non-executed or incorrectly executed payment transaction to the payer, i.e. restore the payer's payment account to the balance it would have had unless the incorrect payment transaction has been executed, except if the payment service user has requested correct payment transaction execution.

The payer’s payment service provider shall ensure that the credit value date for the payer’s payment account in relation to the defective payment transaction is no later than the date the amount of the defective payment transaction was debited from the payer’s payment account.

If evidence is provided by the payer's service provider to the payer, and, as necessary, also to the payee's payment service provider, that the account of the payee's payment service provider has been credited in the amount of payment transaction, the payee's payment service provider shall be liable to the payee for non-executed or incorrectly executed payment transaction.

The payee’s payment service provider shall, in the case referred to in the above paragraph of this item, that the credit value date in relation to a defective or non-executed payment transaction is no later than the business day the amount would have been value dated had the transaction been correctly executed.

Where a payment transaction is executed after the time set out herein, the payee’s payment service provider shall ensure, upon the request of the payer’s payment service provider acting on behalf of the payer, that the credit value date is no later than the business day the amount would have been value dated had the transaction been correctly executed.

Payment service provider liable for non-executed or incorrectly executed payment transaction shall make refund to its payment service user in the amount of any fees charged to payment service user as well as refund or pay the amount of any fees such user is entitled to relating to non-executed or incorrectly executed payment transaction.

Where a payment transaction is initiated by the payer through a payment initiation service provider, the account servicing payment service provider shall be considered to be the payer’s payment service provider within the meaning of paragraphs 1 to 4 of this Article.

Liability for non-execution, defective or late execution of a payment transaction initiated by the payee or by the payer through the payee

If payment transaction has been initiated by payee or payer through payee, the payee's payment service provider shall be liable to payee for the correct submission of payment order to payer's payment service provider.

Unless payment order has been submitted or payment order has not been correctly submitted in the case referred to in paragraph 1 of this Article, payee's payment service provider shall, immediately upon becoming aware thereof, submit and/or re-submit such order to the payer's payment service provider.

Where a payment order is transmitted to the payer’s payment service provider after the timeline specified between the payee and his payment service provider, the payee’s payment service provider shall credit value date the amount on the payee’s payment account no later than the date the amount would have been value dated had the payment transaction been executed within the timeline specified between the payee and his payment service provider.

If the amount of payment transaction initiated by the payee or the payer through payee is credited on the account of the payee's payment service provider, this provider shall be liable to payee for the correct payment transaction execution.

Where the payee’s payment service provider is liable under the above paragraph 4 of this sub-item, it shall credit value date the amount on the payee’s payment account no later than the date the amount would have been value dated had the payment transaction been executed correctly.

If the payee's payment service provider provides evidence to payee, and, as necessary, to the payer's payment service provider, that it is not liable to payee in accordance with paragraphs from 1 to 3 of this Article – the payer's payment service provider shall be liable to payer for non-executed or incorrectly executed payment transaction.

If the payer’s payment service provider is responsible in accordance with the above paragraph of this sub-item, it shall act in accordance with this paragraph 2 of this Article.

The payer’s payment service provider shall not be liable under paragraph 1 of this sub-item where the payer’s payment service provider proves that the payee’s payment service provider has received the amount of the payment transaction, even if execution of payment transaction is merely delayed. If so, the payee’s payment service provider shall credit value date the amount on the payee’s payment account no later than the date the amount would have been value dated had the payment transaction been executed correctly.

The payment service provider shall, in accordance with this Article, refund to its payment service user the amount of any fees charged to payment service user, as well as refund or pay the amount of any fees such user is entitled to relating to non-executed or incorrectly executed payment transaction.

Rights and Obligations of Payment Service Providers in Case of Incorrectly Executed Payment Transactions

Rights and obligations of payment service providers in case of incorrectly executed national payment transactions shall be the following:

1) if the payer's payment service provider transfers to the payee's payment service provider the amount of the payment transaction that is higher than the amount indicated in the payment order or if it mistakenly executes the same payment order several times, the payee's payment service provider shall, based on evidence submitted by the payer's payment service provider that made the error, return such funds to the payer's payment service provider without undue delay;

2) if the amount of the payment transaction transferred to the payee's payment service provider is lower than the amount indicated in the payment order, the payer's payment service provider may, within the time limits prescribed in the Law on Payment Services, transfer to the payee's payment service provider the difference, even without the request of the payment service user for the correct execution of the payment transaction;

3) if funds are transferred to the payee other than the one indicated in the payment order, the payer's payment service provider may, within the time limits prescribed in the Law on Payment Services, correctly execute the payment transaction even without the request of the payment service user for correct execution of the payment transaction, and the payee's payment service provider whom the funds are wrongly transferred shall in any case, based on evidence submitted by the payer's payment service provider that made the error, return such funds (as recovery) to the payer's payment service provider without undue delay.

In cases referred to in item 1) and 3) of the above paragraph, the Bank shall be entitled to debit the account of the User-payee for the amount paid in excess and/or groundlessly received amount. The refund of the funds referred to in paragraph 1 item 1) and 3) of this Article shall take precedence over any other payment transaction from the payment account from which the recovery is to be made.

Rights and obligations of payment service providers in cases of fraudulent or misused transactions

If it receives from the payer's payment service provider a refund request along with data, information and documentation based on which it is determined that the payment transaction is probably fraudulent or misused, the payee's payment service provider shall not credit these funds to the payee's account, and/or shall prevent the use of those funds to the payee within the next three business days from the day of receipt of those data, information and documentation.

If in the case referred to in paragraph 1 of this sub-item, the payee's payment service provider, subsequently, but before the expiry of the deadline referred to in that paragraph, receives data, information and documentation from the payer's payment service provider, including the corresponding application to the competent government authority, which all together beyond any reasonable doubt points to the conclusion of fraud or unauthorised use, the payee's payment service provider shall:

1) without delay, make a refund to the payer, if the payee could not prove or make probable the origin of those funds or refused to provide appropriate evidence within 15 business days from the day when its payment service provider informed it of the data, information, documentation and application referred to in this paragraph;
2) enable the payee to use funds after 30 business days from the day of the expiry of the deadline referred to in paragraph 1 of this Article, if the payee has proven and/or made probable the origin of those funds within the deadline referred to in item 1) of this paragraph, and the competent government authority failed to adopt and submit an act on the prohibition of the use of those funds.

The payee's payment service provider shall be accountable to the payer for the loss arising from the payment transaction referred to in paragraph 1 of this Article, if it enabled the payee, contrary to paragraphs 1 and 2 of this Article, to use funds, and it is determined in relevant procedure that the payee committed or participated in fraud or unauthorised use.

Liability of an intermediary for unauthorised, non-executed, defective or late payment transactions

The payment service provider shall be liable to the payment service user for an unauthorised, non-executed or incorrectly executed payment transaction, or delay in payment transaction execution in dinars even if the liability is

attributable to an intermediary participating in the execution of that payment transaction among payment service providers.

Obligation to trace funds in case of unauthorised, non-executed or defective payment transactions

In case of an unauthorised, non-executed or incorrectly executed payment transaction, the payment service provider shall, regardless of the liability for correct execution of a payment transaction, upon request of its payment service user, take immediate and adequate steps to trace the funds and notify the user about the outcome of measures taken without undue delay.

Liability for Using Unique Identifier

If a payment order is executed in accordance with the payee's unique identifier referred to in such order, it shall be deemed that this order has been correctly executed relating to the payee's determination irrespective of other data provided to the payment service provider.

If a unique identifier the service user has provided with the payment service provider is incorrect, the payment service provider shall not be liable for non-executed or incorrectly executed payment transaction.

In the case referred to in paragraph 2 hereof, at the request of a payment service user, the payment service provider shall immediately take all reasonable measures in order that the payment service user receives the refund of a payment transaction amount, and the payee's payment service provider shall cooperate to this aim with the payer's payment service provider and provide all the necessary information to the provider so that the payment transaction amount is refunded. If in the case referred to in this paragraph the money cannot be refunded to the payer, the payer's payment service provider shall, upon the payer's written request, immediately submit all the available information which the payer needs to exercise the right to refund (e.g. information about the payee's payment service provider and/or the payee), including the information which the payee’s payment service provider is required to provide to the payer’s payment service provider under this paragraph.

Payment service provider may charge special fee to the payment service user for taking measures referred to in paragraph 3 of this Article, in the amount set out in the Price List.

In the event of non-executed payment transaction due to an incorrect unique identifier referred to in paragraph 2 of this Article, the payment service provider shall, immediately upon becoming aware thereof, refund the amount of non-executed payment transaction to the payment service user.

Disclaimer due to Force Majeure or Law

The Bank shall not be liable for an incorrectly, non-timely executed and/or for non-executed payment transaction in the event of force majeure which has prevented the fulfilment of obligations or if payment transaction execution is prohibited under other regulation.

The liability of the Bank when, due to the application of the regulations governing the prevention of money laundering and terrorism finance and/or due to the change in sanction related regulations, the Bank rejects payment transaction execution or prolongs the terms referred to in the Cut-off Times, shall be excluded.

Exclusion of Liability for the Actions of Intermediary Bank

For international payment transactions, the Bank shall not be liable if the intermediary bank participating in the payment chain charges its fee, thereby decreasing the amount paid to the payee (if the bank has not, in the course of initiating transaction, been aware thereof or if it has informed the client thereof), even when OUR costs are arranged.

For international transactions, the Bank shall not be liable to payment service user for a non-executed or incorrectly executed payment transaction even if the liability is attributable to an intermediary participating in the execution of that payment transaction among payment service providers.

For international payment transactions, the Bank shall not be liable if a foreign bank of the payee credits the payee's account in the local currency, not in the currency in which the User has executed transaction, or if the foreign bank of the payee executes payment transfer to the User's account in other currency, not in the one in which the payment transaction has been initiated.

Liability for losses stemming from unauthorised, non-executed, defective or late payment transactions

Provisions of Articles 14.2-14.4 hereof shall not exclude the right of the payment service user to request from its payment service provider, and/or its payment initiation service provider if the payment transaction is initiated through it, in accordance with law, a compensation for losses stemming from the execution of an unauthorised payment transaction, for non-execution, defective or late execution of the payment transaction that the provider is liable for.

Burden of proving the execution of payment transactions

If the payment service user claims that it did not authorise an executed payment transaction or that the payment transaction was not executed or was not correctly executed, it is on its payment service provider, if it claims the opposite for the service of which it is in charge, to prove that the payment transaction for that service was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or other deficiency.

If the payment transaction is initiated through a payment initiation service provider, the burden shall be on the payment initiation service provider to prove that within its sphere of competence, the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency linked to the payment service of which it is in charge.

A payment transaction is considered authenticated, within the meaning of paragraphs 1 and 2 of this Article, if the payment service provider, by applying adequate procedures, verified and confirmed the use of a specific payment instrument, including its personalised security features.

If the payer claims that it did not authorise a payment transaction executed by using a payment instrument or initiated through a payment initiation service provider, the records of the payment service provider of the use of such instrument and/or payment transaction initiation shall in themselves not be sufficient to prove either that the payer has authorised that payment transaction, or that the payer acted fraudulently or failed, with intent or gross negligence, to fulfil obligations of the protection personalised payment instrument elements.

The payment service provider and, *mutatis mutandis*, the payment initiation service provider shall, in the case referred to in paragraph 4 of this Article, provide supporting evidence to prove that the payment service user acted fraudulently or failed with intent or gross negligence to fulfil the obligations of the protection of payment instrument personalised instruments.

Execution of international payment transactions and payment transactions in currencies of third countries

Provisions of regulations governing foreign exchange operations shall apply to the execution of international payment transactions and payment transactions in the currencies of third countries.

The Bank will not execute international payment transactions for securities buying if funds are paid to a foreign broker or to the escrow account of the User managed by the foreign broker.

Provisions of these General Terms shall apply to all aspects relating to the execution of payment transactions referred to in paragraph 1 of this Article which are not specified in regulations governing foreign exchange operations.

By way of derogation from paragraph 1 of this Article, the National Bank of Serbia may prescribe operational, technical and other requirements to apply to the payment transactions executed in euros within the Single Euro Payments Area (SEPA).

SEPA Credit Transfer (SCT)

The SEPA Credit Transfer (SCT) represents a standardised method for executing payment transactions in euros within the Single Euro Payments Area (SEPA), ensuring efficient, secure, and reliable transfer of funds between users' payment accounts in the SEPA member states, in accordance with unified technical and business rules Key characteristics of the SEPA credit transfer include the following:

- Transactions are executed solely in the euro (EUR) currency;
- Payer must provide a correct IBAN (International Bank Account Number) of the payee;

• Payee must have an account at the financial institution which is a member of the SEPA system;

• Payments are made for the full original amount;

• Transactions are executed based on the “SHA” cost model – where every party bears the costs of own payment institution;

• The deadline for executing the order is no later than the next Bank business day from the date of receipt of a complete and properly filled-out payment order (D+1) The Client may request order execution on other value date (requested execution date which may the same date or a date in the future);

When issuing a payment order for the SCT execution, the Bank must obtain the following data from the User:

1) name and surname, or name of payer;

2) number of payer's account in the IBAN format;

3) data on credit transfer amount;

4) number of payee's account in the IBAN format;

5) name and surname, or business name of payee;

6) other information regarding payment transaction.

When executing a credit transfer, the Bank, as the payee’s payment service provider must provide or make available to the payee the following data:

1) name and surname, or business name of payer;

2) data on payment transaction amount;

3) payment transaction description.

Time of SEPA SCT order receipt and execution is set out in the Bank’s Cut-off Time.

The Bank will process each order for a SEPA SCT in the following case:

- when all of the prescribed obligatory elements of the order are completed,

- when the order is submitted at a time when the Bank can process the SCT order with regard to the execution date, i.e., no later than one interbank business day before the execution date,

- when the payment order is denominated in EUR,

- when the SHA option is selected as the credit transfer cost option,

The SHA cost option when executing an SCT means that the User bears the fee for executing the transaction in accordance with the Bank’s Price List, without paying the costs of foreign correspondent banks.

The Bank is obliged, when it receives an SCT from a participant in the SEPA area in favour of a payee who is its User, to ensure that if the amount of the payment transaction for the payee has been credited to its account and if it has received all information necessary to credit the payee’s payment account, it credits the funds to the payee’s payment account without delay.

User's Complaints

The User shall duly use the reports received from the Bank, review such reports, and file complaint relating to any mismatch or contest of debts and/or claims in the report sent to the User.

The User shall immediately notify the Bank on unauthorised, non-executed, or incorrectly executed payment transaction, and/or if he requires correct payment transaction execution, upon becoming aware of such payment transaction, but no later than 5 days from the date of account debiting, i.e. from the date for the execution in the event of a non-executed transaction. Complaint may be submitted at the Bank's point of sale, by sending message within the E-Bank and M-Bank, by e-mail to info@erstebank.rs or by telephone to 0800 201201 (whereby the complaint is to

be submitted in writing as soon as possible), stating the number of the order, order execution date, and accurate and clear description of the transaction regarding which the complaint is filed.

Upon the expiry of the period referred to in the previous paragraph, the User shall not be entitled to request the refund of an incorrectly executed, unauthorised transaction if he has been provided by the Bank with the information on the respective payment transaction in accordance with the law.

The period referred to in paragraph 2 of this sub-heading does not apply to the transactions defined in sub-heading Rights and obligations of payment service providers in cases of fraudulent or misused transactions.

Corrections of Account

The Bank shall be authorised to make corrections of the account without specific request by the User if the errors have occurred due to a failure by the Bank personnel.

The Bank shall be authorised to make necessary corrections, issue appropriate orders, and implement changes on the Account to adjust the Account balance which would match the Account balance unless payment transaction were executed.

The Bank shall notify the User on the corrections made by statement on balance and changes on Account or by specific notice.

VIII PAYMENT ACCOUNT DEBITING WITHOUT PAYMENT ORDER

The Bank will debit the User's account – without payment order, in the following cases:

1) in the process of enforcement and/or forced collection taken against the user, in accordance with the law;

2) for the purpose of collecting due fees for the Bank services, due claims based on loan approved by the Bank to the User, or other due claims of the Bank to the User;

3) in the event of filing bill of exchange for collection issued by the User if there are sufficient funds for the collection using the bill of exchange;

4) in other cases prescribed herein, in the agreement executed with the User, and in the law.

The executed payment transaction referred to in paragraph 1 of this Article shall not be considered an unauthorised payment transaction, and it shall have priority in relation to payment orders submitted by the User to the Bank for execution.

IX PROTECTION OF THE RIGHTS AND INTERESTS OF PAYMENT SERVICE USER

If the payment service provider or electronic money issuer fails to comply with the provisions of the law, other regulations or general terms of business governing payment services or electronic money, good business practices relating to these services or obligations arising from payment service agreements and/or agreements concerning electronic money – the payment service user and/or electronic money holder are entitled to the protection of their rights and interests.

The procedure of protecting rights and interests of payment service users and electronic money holders shall be subject to provisions of the law governing the protection of financial service consumers which relate to exercising the protection of rights and interests of financial services consumers.

Provisions of the law governing the protection of financial services consumers shall apply accordingly to unfair agreement terms and unfair business practice in the field of providing payment services and issuance of electronic money, including the procedure of their prohibition.

Right to Complaint

The User shall be entitled to file complaint to the Bank if he considers that the Bank is not in compliance with the provisions of the Law on Payment Services, general terms of business, or good business practice relating to payment services or obligations from the agreement executed with user.

The User shall be entitled to complaint within upon becoming aware of a disputable event, but, in every case within three years from the date when his right or legal interest has been breached.

The Bank shall provide provider of such claim with a clear and understandable response to claim no later than within 15 days from the day of complaint receipt, and in such response, point out his right to file claim to the National Bank of Serbia.

The Bank shall, in its business premises in which services are rendered to users, by mail, e-mail, eBanking, and mBanking, and on its web-site provide for the possibility of filing complaint and/or enable the user to be informed on the manner of filing complaint and on the method of handling complaint.

The Right to Filing Claim to the National Bank of Serbia

If he is not satisfied with response to his complaint, or response has not been provided within the prescribed term, the complaint provider may, prior to initiating legal proceedings, file claim in writing to the National Bank of Serbia.

Complaint provider may file claim within six months from the date of response receipt or the expiry of the term for providing response.

The National Bank of Serbia shall notify claim provider on finding under such claim within three months from the date of claim receipt, and in more complex cases, such deadline may be prolonged by maximum three months, on which the National Bank of Serbia shall notify claim provider in writing prior to the expiry of original deadline.

Extra Judicial Settlement of Disputable Relation

If a complaint provider is dissatisfied with response to his complaint or he has not been provided with such complaint within the prescribed term, disputable relation between complaint provider and financial service provider may be solved in extra judicial proceedings – mediation procedure.

After initiating mediation procedure, the user may not file claim thereafter unless this mediation has been completed in suspension or waiver, and if claim has already been filed – the National Bank of Serbia will stop proceedings thereunder and/or suspend the proceedings if mediation is completed in agreement.

Mediation procedure shall be initiated at the proposal of a party in dispute accepted by the other party. This proposal must also include deadline for the acceptance thereof, which may not be shorter than five days from the date of submitting such proposal.

The mediation procedure shall be confidential and urgent.

Parties in dispute may make decision to implement the mediation procedure before the National Bank of Serbia or other authority or person authorised for mediation.

Mediation procedure before the National Bank of Serbia shall be free of charge for the parties in such procedure.

Mediation procedure may be finalised with agreement between parties, suspension, or waiver.

X . CLOSING PROVISIONS

Excerpt from these General Terms shall, together with agreement and application form/specific form of the Bank for specific payment services, Excerpt from the Price List, and Cut-off Time, comprise Framework Agreement on Payment Service Provision.

Signing Agreement/Application Form/form of the Bank for specific payment services, the User shall acknowledge that he is provided with the excerpt hereof, that he is aware of the provisions of the General Terms and accepts the application thereof.

Agreement Amendments

The Bank shall notify the User on any Framework Agreement amendments no later than two months before such proposed amendments come into force.

Following the receipt of the proposal referred to in paragraph 1 of this Article, the User may accept or reject the amendments of the provisions of the framework agreement prior to the proposed date of the beginning of the application thereof.

By way of derogation from paragraph 1 of this Article, where a payment service provider proposes a change in the charge for the provision of payment services which is more favourable to the payment service user, or introduces a new service or functionality of an existing service free of charge, such change can be applied immediately, without previous submission to the payment service user of the proposal of changes to the provisions of the framework contract in the part relating to such change.

The Bank will deliver amendments to the framework agreement electronically if an e-mail address has been provided to the Bank, otherwise, if the Bank has not been provided with an e-mail address by the User, the Bank may use the User's e-mail address registered with the Business Registers Agency for sending notifications, and the User shall be considered duly notified.

If the User does not have an e-mail address for receiving correspondence, the Bank will deliver the amendments to the Framework Agreement by post, to the last known address, and the User shall be considered duly notified.

It will be deemed that the User accepts proposed amendments unless he has notified the Bank on his disagreement therewith until the date of the beginning of the application thereof, and Bank shall inform the Client in an significantly visible manner thereof.

The User shall be entitled to, prior to the date of the application of proposed amendments, terminate the agreement, excluding payment of any fee and other charges unless he/she disagrees with such amendments, as well as to determine the date before the beginning of the application of the proposed amendments from when the termination will be effective.

The User may require that the agreement provisions contrary to the information provided in the pre-agreement stage and/or unless the provisions relating to the information comprising the obligatory agreement element have previously been sent to the User – are determined null by initiating relevant legal proceedings.

Service Termination

The User may unilaterally terminate the Framework Agreement, within one month notice period which shall start to run from the date of sending notification in writing on the termination to other party.

In the event of the termination by the User, he shall settle any due liabilities to the Bank and return cards and user identification within 8 days on the notification on the Agreement termination.

The Bank may unilaterally terminate the Framework Agreement, within two-month notice period which shall start to run from the date of sending notification in writing on the termination to other party.

The Bank and the User may unilaterally terminate the Framework Agreement without any notice period if the other party fails to be in compliance with the provisions of the agreement.

The Bank may also unilaterally terminate the Framework Agreement in other cases set out in particular agreement, the law governing contracts and torts, or in other law.

Regulations Application

The applicable regulations and the Bank General Terms of Business, legislation, and other acts of the Bank governing operation with the Users shall apply to any issue not set out herein and in the agreement. These General Terms shall be an integral part of the General Terms of Business of the Bank.

Executing the Framework Agreement, the User acknowledges that he has been informed on and entirely accepts the Bank General Terms of Business.

Executing the Framework Agreement, the User acknowledges that he is informed on and has received the Excerpt from the General Terms, Excerpt from the Price List, and Cut-off Times, which shall be an integral part of the Framework Agreement on Payment Services.

Dispute Resolving

Disputes between the Bank and the User shall be solved by mutual agreement, otherwise court shall have jurisdiction in accordance with the law.

Application of the General Terms

These General Terms shall apply to users who have established business relation with the Bank, the subject of which shall include payment services before these General Terms have come into force, as well as to any users establishing business relation with the Bank after these General Terms have come into force.

The General Terms shall come into force on **27 January 2027**.