ERSTE BANK A.D. NOVI SAD
BOARD OF DIRECTORS
Number: 1436/2026-562/7-4
Date: 17.03.2026.

GENERAL TERMS OF PROVIDING PAYMENT SERVICES TO PRIVATE INDIVIDUALS AND REGISTERED FARMS

1. 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 (hereinafter: General Terms) to payment service users – consumers and registered farms (RF) (hereinafter: User), the mutual rights and obligations relating to payment service execution, in accordance with the Law on Payment Services (Official Gazette no. 139/2014 and 44/2018, and 64/2024) and the accompanying by-laws.

The basic data on the Bank which is the issuer of these General Terms:

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

Head office: Bulevar oslobodjenja 5, 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

        +38160/ 4848 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.

2 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) 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;

5) 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;

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 a payment order, i.e. payment order initiation;

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 means a natural person entering into 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) registered farm – private individual who is a holder or member of family farm in sense of the law governing agriculture and rural development;

13) funds means cash, scriptural money and electronic money;

14) cash means banknotes and coins;

15) 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;

16) 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);

17) 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;

18) 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;

19) credit instant transfer means 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. Credit instant transfer has been provided by the Bank since 1 April 2019.

20) NBS IPS system means a system the operator of which is the National Bank of Serbia 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.

21) 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;

22) 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;

23) 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;

24) 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;

25) 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;

26) 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;

27) 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 agreement;

28) 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;

29) 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;

30) legal residence in the Republic of Serbia means a natural person's residence in the Republic of Serbia in accordance with the regulations governing permanent and temporary residence of nationals, and/or residence of foreign nationals in accordance with the law on foreigners, including a foreign national residing in the Republic of Serbia in accordance with the laws governing asylum and refugees or based on the international treaty;

31) payment account change means a service provided by the payment service provider to the User, in accordance with the Law on Payment Services;

32) 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;

33) remote payment transaction means a payment transaction initiated via internet or through a device that can be used for distance communication;

34) 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;

35) 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;

36) 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

37)) 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;

38)) 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

3

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;

39)) personalised security credentials mean personalised data and features provided by the payment service provider to a payment service user for the purposes of authentication;

40) 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;

41) 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

42) eBank means the applications of mBanking and eBanking: NetBanking, mBanking, George mobile application, and George web application offered by the Bank to Users

43)   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.

44)   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.

45)   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;

46)   SEPA rules for the execution of payment transactions (payment scheme) means 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.

47)   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 the payer's payment service provider, initiates the execution of one or more payment transactions to debit the payer's payment account, after which the payee's payment account is credited with the amount of that payment transaction or those payment transactions.

3 PAYMENT SERVICES

3.1 The Bank shall perform the following payment services:

1) services of payment account opening, maintaining and closing
2) services of incoming payment of cash on current/payment account, services necessary for such account opening, maintaining, and closing;
3) services of disbursement of cash from current/payment account,

4) fund transfers from/to a current/payment account, including:

    (1)   credit transfers,

    (2)   direct debit, including one-off direct debit,

    (3)   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)   direct debit, including one-off direct debit,

    (3)   using a payment card or similar means;

6) issuing and/or acquiring of payment instruments;

7) money remittance services where a payment service provider receives funds from a payer, without any payment accounts being opened in the name of the payer or the payee, for the sole purpose of making these funds available to a payee or of transferring these funds to the payee's payment service provider, which makes such funds available to the payee.

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.

4   CURRENT/PAYMENT ACCOUNT OPENING AND MAINTAINING

4.1   Current/Payment Account Opening and Maintaining

4.1.1.   The Bank shall open current and other payment accounts – escrow accounts, etc. The account shall be opened by the Bank based on completed User's application (form of the Bank), upon the execution of the Account Opening and Maintaining Agreement.

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

If the User wants to execute payment transactions in other 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.

To such newly opened FX accounts referred to in this paragraph, the provisions of the agreement on account opening and maintaining which have been executed with the Bank shall apply.

4.1.3   When establishing business relation, the Bank shall identify the User examining his valid identification document.

4.1.4   For the purpose of disposing funds on the User's account, signatures of persons authorised for disposing such funds shall be stored with the Bank, which will be used for signing payment order forms.

4.1.5   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 Private Individual Account Register maintained by the NBS which shall not be public.

4.1.6   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 on-board such client or execute a transaction, i.e. it will terminate already existing business relation.

4.1.7   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.

4.1.8   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.

4.1.9   The User shall dispose of the account funds within the available funds through the disposal instruments. Disposal of funds on account on ATM, acceptance device, or otherwise, shall be made using card and signing and/or using the Card User's PIN, or in other manner enabled by the Bank to Users. The Bank may determine maximum number of transactions and total amount of transactions executed on a daily basis with the card when paying out cash and when purchasing goods and services, on which the User will be notified by the Bank.

4.1.a   Payment Account Change

4.1.a.1 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, consents for direct debits, 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.

4.1 b   Payment Account with Basic Services

4.1.b.1 Upon the request of the Consumer, who has a legal residence in the Republic of Serbia, but does not hold payment account, the Bank shall open the Bank account with basic services for payment transaction execution in dinars, in connection with which the Bank shall provide the User with the following payment services:

1) payment account opening, maintaining and closing;

2) payment of cash to the payment account and withdrawal of cash from payment account at teller desks, ATMs, and other similar devices of the bank with which the account is held;

3)   services of executing payment transactions, i.e. fund transfers from/to a payment account, as follows:

(1) direct debit (see note in item 7)

(2) use of payment card, payment card-based payment instrument, and instant transfer-based payment instrument at the merchant's point of sale, in sense of the decision setting out the general rules for the execution of instant credit transfer, including the use of these payment instruments for payment through the Internet;

(3) credit transfer, including standing order and instant credit transfer which is not an instant credit transfer in sense of sub-item (2) of this provision, based on the payment order issued at the bank's teller desk, within eBanking or mBanking, or by using relevant devices irrespective of whether these are the internal or external transfers, transfers to the accounts of consumers, and entrepreneurs or corporates, and irrespective of the method of initiating these transfers (e.g. use of agreed payment service user flag or standardised two-dimensional code – QR code);

4) set-up and use of eBanking or mBanking, in accordance with these General Terms;

5) issuance and use of debit payment card;

6) submission of the notice regarding executed payment transactions, in accordance with the manner arranged in the Framework Agreement. .

In sense of the above paragraph, consumer means a consumer who holds payment account at the Bank solely used for the collection of funds for loan repayment, i.e. loan service or maintenance, or as a security instrument, as well as a consumer holding an escrow account at the bank for the purpose of payment of the funds acquired based on specific regulations (i.e. one-off pecuniary aid to all adult private individuals), which is not used for the execution of other payment transactions.

A consumer referred to in paragraph 1 of this paragraph means a consumer holding a payment account with the Bank, who requests opening of payment account with basic services, at the same time, filing an application for closing of all other accounts at the Bank, save for the account referred to in the above paragraph.

Conditions for opening, maintaining (using), and closing of the Payment Account with basic services, must be non-discriminatory.

The Bank shall, upon the User's request, open the Payment Account with basic services, by executing the Framework Agreement, or reject such application, without delay, no later than ten (say: ten) business days from the date of the receipt of duly made application. In the event of the application rejection, the Bank shall provide the User with the notice in writing, free of charge, on the rejection and the reasons thereof, unless such notice is prohibited based on the regulation, including the information on the User's right to complaint and claim as well as on the possibility of extra judicial settlement of the disputable relation regarding opening of the Payment Account with basic services, in accordance with the Law governing the protection of financial service users.

The Bank shall reject application for Payment Account opening with basic services if the User has already had a payment account with other commercial bank, enabling the User to use the services enabled within the Payment Account with basic services, unless the User provides the Bank with a statement in writing and a notice by the other bank that the payment account with such other commercial bank will be closed. Prior to this, the Bank will check whether the User holds a payment account with other commercial bank or, unless the Bank performs such check, it shall obtain the statement in writing from the User whether the User holds a payment account with other commercial bank enabling the User to use the basic services prescribed for the Payment Account, including the basic services.

In terms of the Payment Account use, the User shall be entitled to:

- the execution of an unlimited number of payment transactions within the services referred to in this Chapter of the General Terms;

- file application for the overdraft of Payment Account with basic services and credit card use, in accordance with the Law setting out the protection of financial service users,

- file application for cheque issuance,

- open and hold FX payment account.

In terms of the use of the Payment Account with basic services, the Bank:

- shall make readily available the information and provide explanations to the User, free of charge, regarding the characteristics of the Payment account with basic services, terms of using such account, as well as the fees

regarding such account, which shall also include a clear indication that arrangement of overdraft and/or credit card and/or other additional services is not a condition for opening and using of the Payment Account with basic services,

- make collection for the use of the use of the Payment Account with basic services, in accordance with its Price List or applicable regulations setting out this matter,

- make free decisions on the User's application for overdraft of Payment Account with basic services and credit card use, in accordance with its lending criteria and the law governing the protection of financial service users, as well as on the application for cheque issuance if the User files the application to the Bank for the use of the aforementioned services.

4.2   Proxy

4.2.1   At the time of account opening or subsequently, the User may authorise one or several persons to dispose of the account funds through the authorisation presented to the Bank or proxy authorised with the relevant authority. Authorisation/proxy may be one-off, temporary, or permanent. Considering the right of funds disposal on account, authorisation/proxy may be general or special.

If the authorisation to dispose of the funds in the account has been granted at the Bank, the authorised person may subsequently, independently, submit a request for the issuance of a debit card.

4.2.2   If such proxy is not issued at the Bank, the User's signature must be certified by local or foreign relevant authority. Proxy holder may execute transactions on behalf and for the account of the User, in accordance with the regulations, but his rights may not exceed those of the User.

4.2.3   If the User is abroad, the proxy must be certified by notary (public notary) and include "Apostille" stamp (and be translated into the Serbian language by a certified translator). If proxy is certified at diplomatic and consular representative office of the Republic of Serbia or if there is a bilateral agreement on the release of the obligation of legalising public documents between the Republic of Serbia and the country in which such document is certified, "Apostille" stamp shall not be necessary.

4.2.4   Proxy holder may not grant proxy to a third party to dispose of funds and require account closing unless it is stated in proxy.

4.2.5   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 delay.

4.2.6   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 of the User, which may impact the execution of payment services and, in general, any funds of the User held with the Bank.

4.2.7   Permanent proxy shall cease to apply by way of revocation by the User in writing, account closing, due to death of the User or proxy holder, loss of the User or proxy holder's work capability, Agreement cancellation or termination, or account closing. If a statement on recall and/or cancellation is not made at the Bank, the signature on such document must be certified by local or foreign relevant authority.

4.3   Representation

4.3.1   For a minor or a person who is not capable of doing business, account opening shall be required by legal representative and/or guardian under decision of welfare center.

4.3.2   Legal representative may operate on the account in accordance with legislation, decisions of competent authorities, and approval of the Welfare Center.

4.3.3   Legal Representative may not arrange overdraft.

4.3.4 The right of disposal of legal representative shall be closed based on effective decision by competent authority, his death, death of represented person, and after represented person has acquired work capability.

5. PAYMENT INSTRUMENT – DEBIT CARD

5.1 Payment Instrument – Debit Card

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

The Bank shall, 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), first issue to the user a payment card where 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.

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, the Bank shall, in the course of the re-issuance of the existing card, also issue the debit card holders the card for which processing, netting, and settlement of transfer orders in domestic payments, issued based on the use thereof, are executed within the Republic of Serbia payment system (unless they have previously been issued such card.

5.1.2 FX debit card shall be issued in the currency to which FX current account is tied.

5.1.3 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.

5.1.4 For the issuance and use of payment card, the Bank shall charge fees and costs, listed in the Price List. The Bank shall collect fees and other charges by debiting account the Card is tied to or in cash.
The Account Holder 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.

5.1.5 The Bank shall be entitled to, during the Card validity and/or automated Card re-issuance, change a type of payment card of the same or other 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.

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

5.2 Card Issuance and Card Data Protection

5.2.1 A User shall be delivered re-issued cards to the User's mailing address which must be registered in the Bank's system.
Newly issued Card and PIN (personal identification number) shall be delivered to the Bank Branch and automatically activated when they are delivered to the User.

The card sent to the User's registered residential address can also be activated via the George mobile / George web eBanking application, and then by initiating the first transaction that requires PIN entry (Chip + PIN).

Reissued card shall retain the PIN of the previous card. The Bank shall guarantee the Card User the PIN issuance secrecy until the delivery of the Card. Obligation of the User shall be to sign Card immediately upon the receipt

thereof, as well as to protect any data therein and keep the PIN in secrecy separately from the Card. The non-signed Card shall be invalid, and any financial consequences in the event of abuse of the non-signed Card shall be borne by the User.

Access to the card PIN is enabled in the George mobile/Web application.
PIN can be changed on all Bank's ATMs.

The deadline for collecting the issued card and PIN is no later than 180 days from the time of receiving the SMS notification about the card being produced and delivered to the selected branch. The card is handed over to the User upon signing the Delivery Confirmation and is activated in the Bank's system by a Bank member of staff

5.2.2   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.

5.2.3   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.

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

5.2.5   The User acknowledges that it 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 the risks and consequences of identity theft and unauthorised use of data from the card due to the provision of data on the Card as mentioned above.

5.3   Debit Card Use

5.3.1   Payment Service User shall use debit card in accordance with these General Terms.

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 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) for payments at on-line points of sale that provide payment using 3DS technology by entering the OTP password that the User receives via SMS; for users of the George mobile application, for payments at online points of sale that provide payment using 3DS technology through push notification and by entering a PIN or biometric data.

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 the payer's account is confirmed.

From 30 June 2026, User authentication for transactions executed at on-line points of sale that enable payment using the 3DS service will **solely** be made via via <u>a push notification within the George mobile application (with the entry of a PIN code or biometric data)</u>, whereby the user's consent for executing the payment debiting the user's 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 hereof.

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 replaced/re-issued card if such process is initiated by the Internet merchant with the card company.

5.3.2   Debit card may be used at all points of sale and ATMs in Serbia/abroad where logo of card company is displayed for withdrawing cash on ATMs, at teller desks of banks, at post office (if appropriate terminal is installed) and for the payment of goods and services at EFTPOS terminals and by the Internet.

5.3.3   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.

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

5.3.5   Acquirer shall issue slip/account copy to the User for the purposes of complaint, if any.

5.3.6   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 card User is in at the time of transaction. The User shall assume full liability in the event of an illegal purchase using the Card subject hereof.

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

5.3.8   The Debit 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.

5.3.9   The Bank shall, for security reasons, set out the cash amount limit and the amount of goods and service payment on a daily basis. Daily limit for issued debit card shall amount to RSD 350,000.00, for the transactions of goods and service payments through POS terminal, including Internet payment, and RSD 100,000.00 for cash withdrawal on ATM. The limit in the number of daily transactions executed using the card through POS and Internet payments shall be 15 transactions, and the limit of cash withdrawal transactions shall be 5 transactions. The Card User shall be entitled to request the change in the daily limits of spending by filing the request for the limit change at the Bank's point of sale, by e-mail from the e-mail address reported by the User to the Bank, or within eBanking/mBanking application, excluding the obligation of creating annex to the Framework Agreement.

The Card User can, by using electronic banking, change the amount of daily limits for payments at POS terminals and on-line, as well as for cash withdrawals at ATMs, up to the maximum limit prescribed by the Bank. Considering that the limit for on-line payments is included in the POS terminal spending limit, if the limit for on-line payments is increased via electronic banking in such a way that the new on-line payment limit exceeds the current POS payment limit, the Bank will automatically increase the POS payment limit to match the requested on-line payment limit so that the transaction can be completed. In situations where the Card User reduces the POS spending limit via electronic banking to an amount lower than the current limit for on-line transactions, the Bank will, in order to prevent potential misuse, also reduce the on-line payment limit to the same new amount as the POS payment limit.

The Bank retains the right to, in accordance with the regulations and its internal acts, check and assess the request prior to limit change approval.

In the course of the contactless transaction execution with Card, there is a possibility that a POS terminal does not request the PIN input or the User's signature up to certain transaction amount. 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.

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

5.3.11   The Card validity period shall be embossed on the card. The Debit 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 the validity period expiry, he shall be automatically re-issued the Card, at the fee provided for in the Price List. The Bank will notify the Card User in a timely manner, prior to the card's expiration date, so that the Card User can confirm whether the User wishes to have the card reissued.

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

5.3.12 At the time of the initiation of any payment transaction with the Card or digital card, the User must have funds on the card account in the amount of the transaction amount, and for transactions abroad in currency other than the card currency which shall be additionally increased by 3% for the transactions abroad. Based on the initiated payment transactions using the card, the Bank will make the provision of the funds on the account to which the card is tied. Funds provision will last for 15 days from the transaction execution date. Following the defined term, provision will be automatically cancelled in the system, whereby provision cancellation shall not release the User of the obligation to provide sufficient funds for the settlement of the executed transaction. Upon the receipt of the order for debit by the payee's service provider, the Bank will book i.e. debit the card account even following the cancellation of the respective provision, in which case the User shall provide sufficient funds on the card account for the transaction settlement. If the User finds that the debit has been booked, but the provisioned funds have not been released, the User must immediately contact the Bank to make any necessary checks.
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.

5.3.13   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.

5.4   Currency Exchange Rate of Account Debiting

5.4.1   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.

5.4.2   In the event debit card is tied to RSD account, for the costs incurred using the card abroad, the Bank will translate the amount of 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.

5.4.3   In the event the Debit 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.

5.4.4 In the event the Debit 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 is currency of the Account – the account shall be charged in the amount of the original currency.

5.4.5 In the event the Debit 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 in RSD equivalent, after which the dinar amount shall be converted into the Account currency at the Bank's buying exchange rate.

5.4.6 In the event Debit Card is tied to the foreign currency account, if original transaction currency is not included in the Bank exchange rate list and differs from the Account currency, MasterCard International and Visa International shall translate original amount into EUR in accordance with the Referential exchange rate, and the Bank shall, from such amount, calculate RSD equivalent at the Bank selling exchange rate applicable on date of debiting, and from such amount at the selling exchange rate, the Bank shall calculate counter value the Account currency and debit the Account by such amount.

5.4.7 MasterCard and Visa exchange rates shall be publicly available on Internet pages www.visaeurope.com and www.mastercard.com and they shall be variable during day, and the Bank exchange rate lists shall be available on the Bank Internet page and at all branches.

5.4a. Exchange Rate for Credit/Inflow on the Card

5.4a.1 In the event debit card is tied to RSD account, for inflow transactions executed using the card abroad, the Bank will translate the amount of 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 buying exchange rate for FX of the Bank for EUR, applicable on date of credit.

The exception shall be the transactions where, in the course of conclusion, the client accepts the amount of dinars converted by the accepting party, in which case the client's account shall be credited in the amount of concluded transaction i.e. by the amount in dinars which the client has accepted by concluding the transaction.

5.4.a.2. In the event the Debit 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 selling exchange rate applicable on date of credit.

5.4.a.3. In the event the Debit 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 and equal to the account currency, the account shall be credited in the amount of the original currency.

5.4.a.4. In the event the Debit 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 credited in the currency of the account, whereby the conversion shall be made based on the following sequence: at the Bank's buying 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 selling exchange rate.

5.4.a.5. In the event the Debit Card is tied to the foreign currency account, if original transaction currency is not included in the Bank exchange rate list and differs from the account currency, MasterCard International and Visa International shall translate original amount into EUR in accordance with the Referential exchange rate, and the Bank shall, from such amount, calculate RSD equivalent at the Bank buying exchange rate applicable on date of debiting, and from such amount at the buying exchange rate, the Bank shall calculate counter value in the account currency and debit the account by such amount.

5.5 Complaints regarding Card Transactions

5.5.1   The User shall keep a copy of slip/account for the purposes of any complaint. The User shall file complaints under executed transactions in writing in the prescribed form to the closest point of sale of the Bank, immediately upon becoming aware thereof, but no later than 13 months from the date of debiting.

5.5.2   Date of the receipt of the Bank statement of receipt of the information on the executed transaction by SMS means the date of becoming aware of executed transaction.

5.5.3   Complaints not filed within the prescribed deadline and in the prescribed form shall not be accepted by the Bank, and financial loss shall be borne by the Debit Card User.

5.5.4   In the event the User wants to get the complete transaction documentation, he must request it from the Bank no later than 13 (thirteen) months from date of debiting.

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

5.6   Lost/Stolen/Misused Card

5.6.1.   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 User can also block the card using the eBank, thereby the temporary blocked status will be assigned to the card.

The User shall, within 2 business days, confirm the report of the lost/stolen Card in writing.

5.6.2   Debit Card found after reporting loss must not be used, and cut card must be returned to the Bank in order to be destroyed.

5.6.3   The User shall, without delay, report any damage and deficiency of the Debit Card to the Bank in the manner provided for in in the report of lost card.

5.6.4   In the event of unauthorised use of the Debit Card and/or data from the Card, resulting in the execution of unauthorised transactions, the User shall, immediately, upon becoming aware thereof, but no later than within 13 months from the date of debiting, report the Bank any transaction executed based on unauthorised use of the Debit Card and/or data from such Card.

5.6.5   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.

5.6.6. The Bank shall provide the User with the evidence that the Bank has been notified by the User, in accordance with item 5.6.1, if the Payment Service User has filed the request for the submission of such evidence within 18 months from the date of this notice.

5.7   Liability for Damage

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

5.7.2   The Debit Card User shall bear any losses relating to any transaction executed due to fraud committed by the User and the losses incurred due to failure to settle his liabilities which result from these General Terms.

5.7.3   The User shall not bear any losses resulting from transactions executed upon reporting loss, theft, or unauthorised use of the Debit Card and/or data from the card unless he himself has made fraud or participated in fraud or acted with the intention of committing fraud.

5.7.4   If data from the card are used by the Debit Card User with the aim of executing telephone, e-mail, or postal purchase, the User shall assume complete risk of possible Debit Card data misuse.

5.7.5   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.

5.8   Protective and other Measures

5.8.1   The User shall use his Debit Card in accordance with these General Terms governing the issuance and use of such an instrument.

Personalised card elements must not be made available to other person by the User (e.g. by forwarding the picture of the card, etc.). 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 made possible with 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 Postal Service of Serbia), act in such manner, because in the majority of cases, though they initially resemble 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, without delay, 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 any notices on the Bank Internet address relating to warnings in connection with the possibilities of payment card misuse (phishing etc.) and act accordingly.

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

5.8.3   The User shall, immediately upon becoming aware of loss, theft, or fraud of his Debit Card, report the Bank thereof.

5.9   Payment Card Blocking

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

5.9.2   The Bank shall notify the User on its intention of the Debit Card blocking and on the reasons of such blocking. Unless it is able to notify him thereof prior to the Debit Card blocking, the Bank shall do so immediately upon blocking. Notification on the intention of blocking i.e. the Debit Card 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.

5.9.3   The Bank will ensure re-use of the Debit Card or it will be replaced with a new one – when reasons for blocking thereof cease.

6   STANDING ORDER

6.1   The User and the Bank may agree the Standing Order execution under which the Bank shall be authorised to, at the charge of his account, execute regular or temporary payments in such manner that payment transaction shall be executed in favour of payee under the conditions defined by the user (payee's account, payment amount, duration, payment schedule).

6.2   The Bank shall agree two types of standing orders with users:

1) Contractual standing orders – opened in favour of companies with which the Bank has executed agreement on standing orders.

2) Ordinary standing orders – through ordinary standing order, the user may pay its debts to legal entities and private individuals with whom the Bank has not executed agreement, transfer funds to savings account, pay humanitarian aid, etc. if the liability settled every month is in the same amount.

6.3   The Bank shall execute standing orders in accordance with the conditions defined by the User. Unless the standing order payment date is a business day, payment will be executed on the first next business day. The User shall provide funds on his Account no later than the time defined in the Cut-off Times. The Bank shall execute standing order only if there are sufficient funds on the account to cover the total defined payment amount and accrued interest unless it is the payment based on credit liabilities to the Bank.

6.4 Standing order shall be agreed by signing Standing Order Opening form and inputting any relevant data relating to the payment transactions executed through the Standing Order.

6.5 Standing order shall cease to be valid on the date defined in the Standing Order Form, by termination by the User, as well as by closing the account at the charge of which payment is executed and/or account in favour of which payment is executed.

6A Digitalised 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.

6A.1 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 Clients.

6A.2 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 Client 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) or initiate request for adding the card in the Digital Wallet from George mobile application.

During the card digitalisation process, the Digital Wallet application may overtake certain data from the User'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.

After registering the payment card, the Card User shall receive a notification in the eBank that a request has been made to add the card to the Digital Wallet, with the option to accept or decline adding the card to the Digital Wallet. To confirm the action of adding the card to the Digital Wallet, the Card User will need to verify his/her identity by entering the PIN for accessing the George mobile application or via biometrics, if such an option has been selected for logging into the application. The User shall not bear the digitalisation expenses.

6A.3   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 Tariff 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 Client is able to add more than one payment cards in the Digital Wallet, historically first card added by the Client into the Digital Wallet shall become a default card for making payments. If the Client 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.

6A.4   Client's Liabilities

To prevent any cases of unauthorised use of the Digital Wallet and digitalised card as well as any fraud, the Client 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.

6A.5 Bank's Liabilities

Starting from the fact that the Bank issues the Cards to the User that the User 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.

6A.6 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.

6A.7   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

in accordance with and to the extent set out in the provisions of the Law on Payment Services, the Bank shall be liable for the Digital Wallet application if any circumstances, interruptions, or errors in the digital wallet result in any unauthorised, non-executed, or incorrectly executed payment transaction or cause a damage to the User. In the event of any loss, misuse, or theft of the data necessary to use the Digital Wallet or in any other case of unauthorised use of the Digital Wallet, the Bank shall retain the right not 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.

6A.7   Closing Provisions

If a 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 of item 5.7–5.9 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.

All rights, obligations, conditions, and responsibilities related to the use of the Digital Wallet that are not defined by the provisions of sub-section 6A of these General Terms of Business are governed by the applicable contractual provisions of the framework agreements concluded with payment service users, as well as by the provisions of these General Terms relating to the use of Debit and Credit Cards issued by the Bank, and the provisions of these General Terms relating to unauthorised, unexecuted, or improperly executed payment transactions arising from the use of the digital wallet.

7   DIRECT DEBIT

ERSTE ⑤
Bank

IMPORTANT NOTICE: The Bank will provide users will the direct debit service until 1 June 2026, after which provision of this service will be discontinued.

From 1 March, provisions of Chapter 7 hereof shall be repealed.

7.1   Introductory Provisions

7.1.1   The User may arrange the direct debit service with the Bank enabling him to settle his liabilities to payee based on the consent provided to the Bank by payee, payee's service provider, or payer.

7.1.2   Direct debit authorisation may be one-off or multiple, with fixed or interim maturities.

7.1.3   Direct debit authorisation on the prescribed form may be submitted by the User to his bank, payee's bank, or payee.

7.1.4   The Bank will execute direct debit in accordance with the conditions set out in direct debit form. Unless direct debit payment date is a business day, payment will be executed on the first next business day. The User shall provide funds on his Account on the date of debit, no later than the time defined in the Cut-off Times. The Bank shall execute direct debit only if there are sufficient funds on account for the cover of the total defined payment amount and accrued fee for service.

7.1.5   The Bank will fully execute individual order which is a part of a series of payment transactions, exceptionally, order will be executed in partial amount when there are insufficient funds on the User's Account for complete order execution if direct debit is agreed for the purpose of settling loan to the Bank.

7.2   Return of the Amount of Approved and Correctly Executed Payment Transaction

7.2.1   The Bank shall, upon the payer's request, refund full amount of approved and correctly executed payment transaction by direct debit if the following conditions are met:

1) that the payer has granted authorisation for the execution of a payment transaction without the exact amount of the payment transaction;

2) the amount of the payment transaction exceeds the amount the payer could reasonably have expected, taking into account his previous spending pattern, the conditions stipulated in the framework contract, and circumstances of the case.

7.2.2   The payer's payment service provider may require the payer to provide evidence about the facts relating to the fulfilment of the conditions referred to in paragraph 1 of this Article. The payer may not refer to the condition referred to in paragraph 1, item 2) of this Article if the higher amount of the payment transaction was due to the currency conversion at the agreed reference exchange rate.

7.2.3   The payer may submit the request referred to in paragraph 1 of this Article within 56 days after the debit date.

7.2.4   The payer's payment service provider shall refund the full amount of the payment transaction to the payer or inform him of the reasons for rejecting the request specified under paragraph 1 of this Article by no later than ten business days after the receipt of the request. Payer's payment account credit value date may be no later than the date when the account is debited for the payment transaction referred to in this paragraph.

7.2.5   If he rejects the request referred to in paragraph 1 of this Article, the payment service provider shall, in the notification about the reasons for the rejection, also notify the payer about the procedure for the protection of the rights and interests of payment service users, including out-of-court redress, and the proceedings that could be instituted for the violation of provisions of this Law, as well as the body responsible for conducting these proceedings.

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

1) that a payee has granted contest for payment transaction execution directly to his payment service provider;

2) information on the future payment transaction was submitted or made available in the agreed manner to the payer for at least 28 days before the due date by the payment service provider or by the payee.

7.2.7   In the event of direct debit where an initiated domestic payment transaction is executed in dinars or a payment transaction executed in accordance with the regulation applicable to payment transactions executed in euros within Single Euro Payments Area without prejudicing paragraph 6 of this Article, the payer shall be entitled to the recovery of the amount of approved payment transaction executed by such direct debit even when the conditions referred to in paragraph 1 of this Article are not satisfied. In such case, the payer's payment service provider may not reject the payer's request for refund of the payment transaction amount.

8   PAYMENT INSTRUMENT – CREDIT CARD

8.1 Payment Instrument – Credit Card

8.1.1   Upon the approval of credit application to the User, the Bank shall, upon his request, issue the User a Credit Card which shall be the payment instrument based on which the User shall dispose of the funds and/or initiate payment transactions up to the amount of the available balance under the loan.

8.1.2   Credit card shall be payment instrument through which approved loan shall be used up to the amount of the available balance of loan.

8.1.3   The Credit Card shall be made out to the User and it shall not be transferable. The Credit Card shall be the ownership of the Bank upon whose request it must be returned. The Credit Card User shall solely be responsible for the correct Credit Card Use.

8.1.4   For the issuance and use of the credit card, the Bank shall charge fees and costs, listed in the Price List. The Bank shall collect fees and other charges by debiting account the Card is tied to.
The Credit 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 Credit Card User.

8.1.5   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 of same or other payment Card brand, in which case, the Card used by the User will be changed without any additional costs and the functionalities corresponding to the functionalities of the replaced card will be ensured.

8.2 Card Issuance and Card Data Protection

8.2 Credit Card Newly issued Card and PIN (personal identification number) shall be delivered to the User at the Bank Branch and automatically activated when they are delivered to the User.

Reissued Credit Cards shall be delivered to the User by mail to the User's registered residential address, which must be recorded in the Bank's system.

The card sent to the User's registered residential address can also be activated via the George mobile / George web eBank application, and then by initiating the first transaction that requires PIN entry (Chip + PIN).

Reissued Credit Card shall retain the PIN of the previous card.

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

8.2.2   The Credit Card User must not disclose PIN to other persons (including, but without any limitation, members of family, merchant, bank officer). Otherwise, the User shall entirely be liable for any transactions executed due to the non-compliance with this obligation.

8.2.3   The User must not leave his Credit 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.

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

8.2.5   The Credit Card 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 any risks and consequences of identity theft and unauthorised use of data from card due to the provision of data on the Credit Card as mentioned above.

8.3   Credit Card Use

8.3.1   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 the 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) for payments at on-line points of sale that provide payment using 3DS technology by entering the OTP password that the User receives via SMS, and for users of the George mobile application, for payments at online points of sale that provide payment using 3DS technology via push notification and by entering a PIN or biometric data.

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 the User's account is confirmed.

From 30 June 2026, 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 the user's

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 hereof.

The Card user can give consent for the execution of the payment transaction through the payee and the payment initiation service provider.

The data on the card registered for payment on a certain site can be replaced by new card data after the reissuance of the card, if that process at the card company was initiated by the internet merchant.

8.3.2   Credit Card may be used at all points of sale and ATMs in Serbia/abroad where logo of the payment brand is displayed and for the payment of goods and services at EFT POS terminals and by the Internet. The Credit Card User may not make transfer from credit card to current account or make payments by transfer of funds from the credit card to other accounts, or withdraw funds from the card at the Bank teller desks.

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

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

8.3.5   The Acquirer shall issue the slip/bill copy to the User. The User shall keep the slip/bill copy for the purposes of complaint, if any.

8.3.6   The User shall not use the Credit 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 Credit Card User is in at the time of transaction. The User shall assume full liability in the event of an illegal purchase using the Card subject hereof.

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

8.3.8   The Credit 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.

8.3.9   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 EFTPOS terminals on a daily basis. Daily limit per issued credit card shall depend on the approved credit limit:

Limits for VISA Classic and Master Card credit cards					
	Amount of approved credit limit				
Transaction name	< 50,000	RSD 50,000–100,000	RSD 100,000–150,000	RSD 150,000–200,000	> 200,000
ATM/card use – max. number of transactions	7	10	10	20	20
ATM/MAX/cash withdrawal	RSD 50,000	RSD 100,000	RSD 150,000	RSD 200,000	RSD 400,000
POS/MAX/purchase	RSD 50,000	RSD 100,000	RSD 150,000	RSD 200,000	RSD 300,000
POS/MAX/cash withdrawal	RSD 30,000	RSD 30,000	RSD 50,000	RSD 50,000	RSD 80,000
POS / max. number of payment transactions	15	20	20	20	20

Limits for DINA Kredit credit cards					
	Amount of approved credit limit				
Transaction name	< 50,000	RSD 50,000–100,000	RSD 100,000–150,000	RSD 150,000–200,000	> 200,000
ATM/card use – max. number of transactions	7	10	10	20	20
ATM/MAX/cash withdrawal	RSD 50,000	RSD 100,000	RSD 150,000	RSD 200,000	RSD 200,000
POS/MAX/purchase	RSD 50,000	RSD 100,000	RSD 150,000	RSD 200,000	RSD 300,000
POS/MAX/cash withdrawal	RSD 30,000	RSD 30,000	RSD 50,000	RSD 50,000	RSD 80,000
POS/card use max. number of transactions	15	20	20	20	20

Limits for VISA Gold credit cards	
Transaction name	Amount of approved limit RSD 100,000–1,000,000
ATM/card use max. number of transactions	20
ATM/MAX/cash withdrawal	RSD 100,000
POS/MAX/purchase	up to the amount of approved limit
POS/MAX/cash withdrawal	RSD 100,000
POS / MAX / recovery of funds / On-line	up to the amount of approved limit
POS/card use max. number of transactions	40

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 or through eBank.

The Card User can, by using electronic banking, change the amount of daily limits for payments through POS terminals and on-line, as well as for cash withdrawals at ATMs, up to the maximum limit prescribed by the Bank. Considering that the internal consumption limit for on-line payments is included in the POS terminal spending limit, if the limit for on-line payments is increased via electronic banking in such a way that the new on-line payment limit exceeds the current POS payment limit, the Bank will automatically increase the POS payment limit to match the requested on-line payment limit so that the transaction can be completed. In situations where the Card User reduces the POS spending limit via electronic banking to an amount lower than the current limit for on-line transactions, the Bank will, in order to prevent potential misuses, also reduce the on-line transaction limit to the same new amount as the POS payment limit.

The Bank retains the right to, in accordance with the regulations and its internal acts, check and assess the request priori to limit change approval.

In the course of the contactless transaction execution using Credit Card, there is a possibility that a POS terminal does not request the PIN input or the User's signature up to certain transaction amount. 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, in the case of contactless transactions, the User may be required to execute the 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.

8.3.10   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.

8.3.11   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 Credit Card User is in compliance with the provisions of the Framework Agreement, upon the validity period expiry, he shall be automatically re-issued the Credit 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.

8.3.12 At the time of the initiation of any payment transaction with the Credit Card, the User must have funds on the card account in the amount of the transaction amount, and for transaction abroad in currency other than RSD which shall be additionally increased by 3% for the transactions abroad.   Based on the initiated payment transactions using the card, the Bank will make the provision of the funds on the account to which the card is tied. Funds provision will last for 15 days from the transaction execution date. Following the defined term, provision will be automatically cancelled in the system, whereby provision cancellation shall not release the User of the obligation to provide sufficient funds for the settlement of the executed transaction. Upon the receipt of the order for debit by the payee's service provider, the Bank will book i.e. debit the card account even following the cancellation of the respective provision, in which case the User shall provide sufficient funds on the card account for the transaction settlement. If the User finds that the debit has been booked, but the provisioned funds have not been released, the User must immediately contact the Bank to make any necessary checks.

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.

8.3.13   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.

8.4   Currency Exchange Rate

8.4.1   When exchanging the local currency into foreign currency, foreign currency into the local 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.

8.4.2   For the costs incurred using the card abroad, the Bank will convert the amount of 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.

8.4.3   MasterCard and Visa exchange rates shall be publicly available on Internet pages www.visaeurope.com and www.mastercard.com and they shall be variable during day, and the Bank exchange rate lists shall be available on the Bank Internet page and at all branches.

8.5   Complaints regarding Transactions Executed Using Credit Card

8.5.1   The Credit Card User shall keep slip/bill copy for the purposes of any complaint. The Credit Card User shall file complaints under concluded transactions in writing in the prescribed form to the closest point of sale of the Bank, immediately upon becoming aware thereof, but no later than 13 days upon the receipt of statement and/or date of debiting.

8.5.2   Date of the receipt of the Bank statement or notification on executed transaction through SMS means the date of becoming aware of executed transaction.

8.5.3   Complaints not filed within the prescribed deadline and form shall not be accepted by the Bank, and financial loss shall be borne by the Account Holder.

8.5.4   In the event of groundless complaint, actual costs shall be borne by the Credit Card User. The Bank shall charge user's account or collect costs in cash. Otherwise, the Credit Card User shall be released from such costs, and the account the Credit Card is tied to shall be credited in the amount of the transaction for which the complaint has been filed upon the procedure completion.

8.5.5   In the event the Credit Card User wants to get the complete transaction documentation, he must request it from the Bank no later than 13 (thirteen) months from date of debiting.

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

8.6   Lost/Stolen/Misused Credit Card

8.6.1 The User shall immediately report loss/theft/misuse of his Credit Card at the closest Bank branch, by telephone number **021/67 72 116**, or by sending e-mail from the User's address reported to the Bank, to the e-mail address sigurnost.kartice@erstebank.rs. The Credit Card User shall state the Credit Card number of his personal number in order for the Bank to, immediately upon the receipt, disable any the further use thereof, and, in the event of an unauthorised payment transaction or approved payment transaction which is the consequence of fraud or misuse, immediately take any reasonable actions for the purpose of funds recovery. The User shall, within 2 business days, confirm the report of the lost/stolen Card in writing.

The User can also block the Credit Card via online banking, in which case the card receives the status temporarily blocked.

The User shall, within 2 business days, report Card loss/theft in writing.

8.6.2   The Credit Card found after reporting loss must not be used, and cut card must be returned to the Bank in order to be destroyed.

8.6.3   The Credit Card User shall, without delay, report the Bank any damage and deficiency of the Credit Card in the manner provided for in the report of lost card.

8.6.4   In the event of any unauthorised use of the Credit Card and/or data from the Credit Card, resulting in the execution of unauthorised transactions, the User shall, immediately, upon becoming aware thereof, but no later than 13 months from the date of debiting, report the Bank on any transaction executed based on unauthorised use of the Credit Card and/or data from such Card.

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

8.6.6   The Bank shall provide the User with the evidence that the Bank has been notified by the User, in accordance with item 8.6.1, if the Payment Service User has filed application for the submission of such evidence within 18 months from the date of notification.

8.7   Liability for Damage

8.7.1   The Credit Card 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 meet the obligation of taking any reasonable and appropriate measures for the purpose of protecting personalised security elements of card due to his wilful intention or gross negligence.

8.7.2   The Credit Card User shall bear any losses relating to any transaction executed due to fraud committed by the User and the losses incurred due to failure to settle his liabilities which result from these General Terms.

8.7.3   The Credit Card User shall not bear any losses resulting from transactions executed upon reporting loss, theft, or unauthorised use of the Credit Card and/or data from the Credit Card unless he himself has made fraud or participated in fraud or acted with the intention of making fraud.
Regarding the Credit Card which may be used for making the Internet payment, unless the site on which payment is made supports 3-DS protection mechanism, the Credit Card User is, based on such payment, exposed to higher risk and the Bank will not be liable if any data from the Credit Card are misused.

8.7.4   If data from card are used by the Credit Card User with the aim of executing telephone, e-mail, or postal purchase, the User shall assume complete risk of possible Card data misuse.

8.7.5   The Credit Card 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 the lost, stolen, or misused Credit Card.

8.8   Protective and other Measures

8.8.1   The Credit Card User shall use the Credit Card in accordance with these General Terms governing the issuance and use of such an instrument.

Personalised card elements must not be made available to other person by the User (e.g. by forwarding the picture of the card, etc.). 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 made possible with 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 Postal Service of Serbia), act in such manner, because in the majority of cases, though they resemble 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 transactions and, without delay, 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 any notices on the Bank Internet address relating to warnings in connection with the possibilities of payment card misuse (phishing etc.) and act accordingly.

8.8.2   The Credit Card User shall, immediately upon the card receipt, take any reasonable and appropriate measures to protect personalised security elements of such a payment instrument – payment Card (PIN, card number, etc.).

8.8.3   The Credit Card User shall, immediately upon becoming aware of loss, theft, or fraud of his payment card, report the Bank thereof.

8.9   Credit Card Blocking

8.9.1   The Bank shall block any further use of the Credit Card, completely or partially (for certain types of transaction types based on certain parameters), if there are reasonable grounds relating to payment card security, if there is suspicion of unauthorised use of the Credit Card or the use thereof for the purpose of fraud, or as a consequence of fraud, or if there is an increased risk that the User will not be able to meet its payment obligation.

8.9.2   The Bank shall notify the User on its intention and reasons of the Credit Card blocking. Unless it is able to notify him thereof prior to the Credit Card blocking, the Bank shall do so immediately upon blocking. Notification on the intention of blocking i.e. the Credit Card blocking shall be submitted by the Bank to the Credit Card User in the manner set out in the Framework Agreement unless the provision of such notification is prohibited under regulations or if there are reasonable securities reasons not to do so.

8.9.3   The Bank will ensure re-use of the Credit Card or the Credit Card will be replaced with a new one – when reasons for blocking thereof cease.

9   PAYMENT INSTRUMENT – NETBANKING SERVICE

9.1   NetBanking

9.1.1   The User may arrange e-banking service with the Bank, which is the Bank application enabling the User to examine its account balance and turnover under account, agreement of banking services, and initiate payment transactions.

9.1.2   E-Bank service User may become any private individual holding current/payment account at the Bank (hereinafter: Applicant). The User shall arrange the E-Bank service NetBanking by signing the Application Form which is, at the same time, NetBanking Service Use Application or by flagging the relevant field in the Account Opening Application.

9.2   Service Type

9.2.1   Erste NetBanking shall cover the Internet Banking services and functionalities listed and described in the user manual.

9.2.2   Erste NetBanking services shall enable the following to the User:

– review of balance and turnover under all accounts

– payment transaction execution:

a. internal transfer of funds between own accounts and accounts for which the User is authorised

b. payment order through credit transfer, including instant credit transfers

c. foreign currency buying and selling

d. FX payment order

– arrangement of standing orders and Contractual Standing Orders

– overtaking statements in the application

– filing application for lending products

– card management – change in limit amount per card, administration of consumption channel (ATM and POS), temporary card blocking and unblocking

- two-way communication with the User within the application.

9.2.3 The Bank shall enable the User to use all services and functionalities offered within Erste NetBanking, and the User shall individually, at own discretion, determine which of the services and/or functionalities he wants to use. The Bank shall reserve the right to change the volume and content of the NetBanking services and functionalities on which the User shall be notified through the content of its web pages.

9.3   Erste NetBanking Service Use
9.3.1   Upon the approval of the application by the Bank, in the event the User arranges only NetBanking, the Bank shall provide the User, on his e-mail, with the user name and password (user identification), through an SMS to the reported number of the mobile telephone.

In the event that, at the same time, NetBanking and mBanking are arranged, the User will receive the user data for mBanking activation – identification code to his e-mail and activation code (user identification) through an SMS, after which mToken, for NetBanking login, will be individually generated through mBanking.

9.3.2 The User shall start using Erste NetBanking service after overtaking the user identification and change the password received in the SMS message. If the User logs in on Erste NetBanking using mToken, he shall, for every single log-in generate a new mToken. 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

9.3.3   Erste NetBanking service use shall be defined herein and in NetBanking Service Use Instructions.

9.3.4 All of the forms of using Erste NetBanking services which are electronically executed applying prescribed user identification shall be identical to signing.

9.3.5   The User shall fill in all orders and any necessary specifications in an orderly and accurate manner and authenticate them by way of the final transaction confirmation, 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.

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

9.3.7 The Bank shall not assume liability for the non-availability of Erste NetBanking service resulting as the consequence of technical problems on computer equipment, outage, or hindrances in telecommunication channels, electric power system outage, or as a consequence of force majeure.

9.4   Data Protection and Liability for Damage

9.4.1 The User shall keep the secrecy of the user identifications and accept full liability for any liabilities resulting from the attributes of his user identification.

9.4.2 The User shall immediately and inevitably ensure to notify the Bank on fraud, any unauthorised use of his user identification or other security device and on any other form of breaching security he becomes aware of in one of the following manners: initiating the NetBanking 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 NetBanking service to the e-mail address: <u>blokadaplatnoginstrumenta@erstebank.rs, in order for the bank to prevent the payment instrument use, and, in the case this is an unauthorised payment transaction or approved payment transaction which is the consequence of fraud or misuse, to immediately take any reasonable actions for the purpose of funds recovery.</u>

9.4.3 The Bank shall be entitled to block the use and disable any further use of the Erste NetBanking service if there are grounds relating to the security of this payment instrument, in the event of suspicion of unauthorised payment instrument use or fraud, as well as in other cases due to security reasons.

9.4.4   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.

9.4.5 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.

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

9.4.7 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.

9.4.8 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.

9.5   Protective and other Measures

9.5.1 The User shall use Erste NetBanking in accordance with the provisions hereof governing the issuance and use of such an instrument.

9.5.2 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.).

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

9.5.4 The User executing payment transactions through Erste NetBanking shall be in compliance with the following 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 user name 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 (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 if it is used for receiving SMS code (for transaction authorisation) for executing payment transactions through the E-bank application. 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.

9.5.5. The User shall follow the Bank web site on a regular basis, in particular, notices by the Bank in connection with the E-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.

9.6   Erste NetBanking Blocking

9.6.1 The Bank shall block any further use of Erste NetBanking if there are reasonable grounds relating to this payment instrument security, if there is suspicion of unauthorised use of payment instrument or the use thereof for the purpose 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.

9.6.2 The Bank shall notify the User on its intention of Erste NetBanking blocking and on the reasons of such blocking. Unless it is able to notify him thereof prior to blocking, the Bank shall do so immediately upon blocking. Notification on the intention of blocking i.e. Erste NetBanking blocking shall be submitted by the Bank to the User at the e-mail address known to the Bank unless the provision of such notification is prohibited under regulations or if there are reasonable securities reasons not to do so.

9.6.3 The Bank will ensure re-use of Erste NetBanking, or it will be replaced with a new one – when reasons for blocking thereof cease.

9.6.4. If the Bank, using special application, determines that the operating system used by the User for initiating payment transactions through the E-Bank/M-Bank is infected with a virus, trojans, etc., 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 the Erste NetBanking and M-Bank service.

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

9.7   Notification

9.7.1 The User shall be informed on payment and turnover transactions executed through Erste NetBanking through the Statement provided to the e-mail address reported to the Bank or in other agreed manner. The User can arrange with the bank the receipt of the notices on single payment transactions through SMS. The User accepts to receive additional notifications, of informative or other nature, through various Bank distribution channels.

9.7.2 The User may file complaint relating to a transaction set through Erste NetBanking immediately upon becoming aware of non-executed, incorrectly executed, or unapproved transaction, but no later than 13 months from the date of debiting.

9.7.3 The User shall report e-mail address change to the Bank, otherwise it shall be deemed that he has been duly notified in the Statement and through other notifications to the last reported e-mail address.

10   PAYMENT INSTRUMENT – mBANKING SERVICE

10.1   Introductory Provisions

10.1.1 Erste mBanking (hereinafter: mBanking) means the mobile banking service of Erste Bank a.d. Novi Sad (hereinafter: Bank), which shall enable the user to execute and view payment transactions and account balance. The excerpt hereof, including Application Form, Excerpt from the Price List, and Cut-off Times shall comprise a framework payment service agreement (hereinafter Framework Agreement).

10.2   mBanking Service Use Agreement

10.2.1 The mBanking service User may become any private individual holding current account at the Bank (hereinafter: User).

10.2.2 The User may arrange this service only if he has got an adequate mobile device, which may support the mBanking application.

10.2.3 The User shall arrange the mBanking service Use by signing the Application Form which is, at the same time, Application for mBanking Service Use or by flagging the relevant field in the Account Opening Application.

10.2.4 With his signature, the User shall acknowledge the accuracy of stated data.

10.3   Service Type

10.3.1 mBanking services shall cover the Internet Banking services and functionalities listed and described in the user manual.

10.3.2 The mBanking services shall enable the User to perform the following:

– view of balance and turnover under all accounts

– payment transaction execution:

a. internal transfer of funds between own accounts and accounts for which the User is authorised

b. payment order through credit transfer, including instant credit transfers

c. foreign currency buying and selling

d. FX payment order

– arrangement of standing orders and Contractual Standing Orders

– overtaking statements in the application

– filing application for lending products

– card management – change in limit amount per card, administration of consumption channel (ATM and POS), temporary card blocking and unblocking

- two-way communication with the User within the application.

10.3.3 The mBanking services shall cover the mobile banking services listed and described in instruction on mBanking service use. The Bank shall enable the User to use all of the services offered in the mBanking, and the User shall individually, at own discretion, determine which of the services he wants to use. The Bank shall reserve the right to change the volume and content of the mBanking services on which the User shall be notified through the content of its web pages. The User shall acknowledge and entirely accept such changes. The User shall not be entitled to request any indemnification in the event of the mBanking service change.

10.4   mBanking Service Use

10.4.1 Upon the approval of the application by the Bank, the Bank shall provide the User with the identification code to his e-mail and activation code through SMS to the reported mobile telephone number

In the event that NetBanking and mBanking are arranged at the same time, the User will receive the user data for mBanking activation – identification code to his e-mail and activation code through an SMS, after which mToken will be generated through mBanking with which he will login on the NetBanking.

10.4.2 The User shall start using the mBanking service upon overtaking his user identification and defining the four-digit PIN code.

Following mBanking activation, the User may opt for log-in using offered biometric data as well as grant consent for payment transactions in the same manner.

With mBanking, the User may choose the Prenesi service, based on which money can be paid through instant transfer instead of inputting payee's account number – by inputting the payee's mobile telephone number, and payments may be received in the same manner.

All of the forms of using mBanking services which are electronically executed applying prescribed user identification shall be identical to signing.

10.4.3 The Bank shall guarantee the mBanking service User free disposal of the funds on all demand accounts, opened based on the executed agreement with the Bank, up to the amount of the funds on the account, including overdraft on such accounts. In the event the client has already used the NetBanking service, the user identification already used for NetBanking will also be used for mBanking.

10.4.4 The User shall fill in all of payment orders in an orderly and accurate manner and authenticate them by way of the final transaction confirmation, 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.

10.4.5 The User shall be liable for the accuracy of all data of payment orders and bear the damage resulting from inputting incorrect data and fraud of the mBanking service in his own environment.

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

10.4.7 The Bank shall exclude its liability for any consequences which could occur due to the use of an inadequate mobile device.

10.4.8 The Bank shall not assume liability for the non-availability of the mBanking service resulting as the consequence of technical issues on computer equipment, outage or hindrances in telecommunication channels, electric power system outage, or as a consequence of force majeure.

10.5   Data Protection and Liability for Damage

10.5.1 The User shall keep the secrecy of the user identification of mBanking and accept full liability for any obligations resulting from the attributes of his user identification.

10.5.2 The User shall immediately and inevitably ensure to notify the Bank on fraud, any unauthorised use of his mBanking user identification or other security device and on any other form of breaching security he becomes aware of in one of the following manners: initiating the mBanking 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 the service of the mBanking to the e-mail address: blokadaplatnoginstrumenta@erstebank.rs, in order for the bank to prevent the payment instrument use, and, in the case this is an unauthorised payment transaction or approved payment transaction which is the consequence of fraud or misuse, to immediately take any reasonable actions for the purpose of funds recovery.

10.5.3 The Bank shall be entitled to block the use of the mBanking service and disable any further use thereof if there are grounds relating to the payment instrument security, in the event of suspicion of unauthorised payment instrument use or fraud, as well as in other cases due to security reasons.

10.5.4   The Bank will automatically block the mBanking 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.

10.5.5 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.

10.5.6 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.

10.5.7 The User shall not bear any losses resulting from mBanking 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.

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

10.6   Protective and other Measures

10.6.1 The User shall use mBanking in accordance with provisions hereof governing the issuance and use of such an instrument.

10.6.2 The User shall, immediately upon receiving the mBanking user identification, take any reasonable and appropriate measures to protect the personalised security elements of such an instrument (password, TAN table, token, etc.).

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

10.6.4. 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 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.

10.6.5 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.

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

10.6.7 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.

10.6.8. 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.

10.7 mBanking Blocking

10.7.1 The Bank can block or reject transaction execution and/or the Bank will block further use of mBanking if there are reasonable grounds relating to payment instrument security, if there is suspicion of unauthorised use of the mBanking or the use thereof for the purpose of fraud, or if there is an increased risk that the User will not be able to settle its payment liability when the use of such instrument is related to the approval of loan and/or overdraft to the User.

10.7.2 The Bank shall inform the User on its intention and reasons of the mBanking blocking. Unless it is able to notify him thereof prior to blocking, the Bank shall do so immediately upon blocking. Notification on the intention of blocking, i.e. the mBanking blocking, shall be submitted by the Bank to the User to the e-mail address reported to the Bank unless the provision of such notification is prohibited under regulations or if there are reasonable security reasons not to do so.

10.7.3 The Bank will ensure re-use of the mBanking or it will be replaced with a new one – when reasons for blocking thereof cease.

10.8   Notification

10.8.1 The User shall be informed on payment and turnover transactions executed through mBanking in the Statement provided at the e-mail address reported to the Bank. The User can arrange with the bank the receipt of the notices on single payment transactions through SMS. The User accepts to receive additional notifications, of informative or other nature, through various Bank distribution channels.

10.8.2 The User may file complaint relating to a transaction set through mBanking immediately upon becoming aware of non-executed, incorrectly executed, or unapproved transaction, but no later than 13 months from the date of debiting. Receiving of the statement on the balance and changes on the account submitted by the Bank shall be the date of informing the User.

10.8.3 The User shall report e-mail/postal address and mobile device change to the Bank, otherwise it shall be deemed that he has been duly notified by submitting Statement and other notifications to the last e-mail/postal address and/or number of mobile device reported to the Bank.

11   PAYMENT INSTRUMENT – GEORGE WEB APPLICATION SERVICE

11.1   George Web Application

11.1.1   The User may arrange George Web application – the eBank service with the Bank, which is the Bank's application enabling the User to examine its account balance and turnover under account, agreement of banking services, and initiate payment transactions.

11.1.2   The User shall arrange the use of the George web application by downloading the application on the App store and activating is as stated below. By activating the application it shall be deemed that the User consented to the use of the payment instrument – George web application.

11.2   Service Type

11.2.1 The George web application services allow the User to:
– view of balance and turnover under all accounts
– payment transaction execution:
a. internal transfer of funds between own accounts and accounts for which the User is authorised
b. payment order through credit transfer, including instant credit transfers
c. foreign currency buying and selling
d. FX payment order
– arrangement of standing orders and contractual standing orders
– overtaking statements in the application
– filing application for lending products

- card management – change in the limit amount per card, consumption channel change (ATM, POS, and Internet), temporary card blocking and unblocking, activation of debit cards sent to home address, PIN, card number, and CVV2 number view
 - contact data management – change in mobile number, e-mail address, and address for card delivery on home address
- consent management – granting/withdrawing consent (Consent and Legal agreements)
- two-way communication with the User within the application.

11.2.2 The Bank shall enable the User to use all services and functionalities offered within George web, and the User shall individually, at own discretion, determine which of the services and/or functionalities the User wants to use. The Bank shall reserve the right to change the volume and content of the George web application services and functionalities on which the User shall be notified through the content of its web pages and within the George web application.

11.3   George Web Application Use

11.3.1 The User shall start the George web application by inputting the User's personal identification number, after which, the Bank will send an activation and SMS code by SMS to the User's reported mobile telephone number.

11.3.2 The User shall begin using the George web application after receiving user identification and is required to create permanent credentials (username and password) to access the George web application. 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

11.3.3 It is necessary that the User has an active George mobile application, since each subsequent login to the George web application must be confirmed via George mobile application. A push notification will appear on the device where the George mobile application was last active.. A push notification will appear on the device where the George mobile application was last active, which the User must click on and confirm the login to the George web application by entering the User's PIN or using biometric data.

11.3.4 The George web application may not be used without a previously activated George mobile application.

11.3.5 The use of the George web application is defined by these General Terms and the Instructions for Using the George Web Application.

11.3.6 All forms of using the George web application conducted electronically with the prescribed user identification are considered equivalent to a handwritten signature.

11.3.7 The User undertakes to correctly and accurately complete all orders and any necessary specifications and to authenticate them with the final transaction confirmation, taking into account the available account balances at the Bank; otherwise, the User bears the risk of non-execution, incorrect execution, or refusal of execution of the payment order.

11.3.8 The execution deadline for a payment order is defined by the Bank's Schedule of Deadlines.

11.3.9 The Bank is not responsible for the unavailability of the George web application resulting from technical problems with the User's computer equipment, failures or interruptions in telecommunications channels, power system outages, or as a consequence of force majeure.

11.4 Data Protection and Liability for Damage

11.4.1 The User is obliged to keep the user identification confidential and accepts full responsibility for all obligations arising under the attributes of the user identification.

11.4.2 The User must immediately and without delay notify the Bank of any misuse, unauthorised use of the user identification, or any other security device, and of any other form of security breach they become aware of, by one

of the following methods: initiating the blocking of the George web application as provided in the application, in person at a Bank branch, by calling the contact center at 021/423-364 or 0800-201-201 on weekdays from 8:00 to 17:00 and Saturdays from 8:00 to 13:00, or by sending an email requesting the blocking of the George web application service to blokadaplatnoginstrumenta@erstebank.rs, so that the Bank can prevent the use of the payment instrument and, in the case of an unauthorised payment transaction or an authorized payment transaction resulting from fraud or misuse, immediately take all reasonable measures to recover the funds.

11.4.3 The Bank has the right to block the use of the George web application and prevent further use if there are justified reasons related to the security of this payment instrument, if there is suspicion of unauthorised use of the payment instrument or its use for fraud, as well as in other cases where security reasons require it.

11.4.4 The Bank will automatically block the User's access to the service if five incorrect login attempts are made. In this case, access will automatically be restored after 60 minutes. The User can also unblock the application in person at a Bank branch or by calling Customer Support.

11.4.5 The User bears all losses arising from the execution of unauthorised payment transactions if these transactions occurred due to the User's fraudulent actions or failure to take all reasonable and appropriate measures to protect the personalized security elements of the user identification, due to intent or gross negligence.

11.4.6 The User bears all losses related to any transaction executed through misuse that the User commits, as well as losses resulting from failure to fulfil obligations arising from these General Terms.

11.4.7 The User shall not bear losses arising from transactions executed after notifying the Bank of the loss, theft, or unauthorised use of the user identification, except if the User has committed misuse, participated in misuse, or acted with intent to defraud.

11.4.8 The User's liability is limited to 3,000 dinars if unauthorised payment transactions occur due to the use of lost or stolen user identification, or if the user identification was misused.

11.5 Protective and Other Measures

11.5.1 The User is obliged to use the George web application in accordance with the provisions of these General Terms and Conditions, which govern the issuance and use of this payment instrument.

11.5.2 The User is obliged, immediately upon receiving the user identification, to take all reasonable and appropriate measures to protect the personalised security elements of this instrument (user identification, PIN, etc.).

11.5.3 The User is obliged, immediately upon becoming aware of the loss, theft, or misuse of the payment instrument, to notify the Bank.

11.5.4 The User performing payment transactions via George web is obliged to comply with the following security requirements:

- The User shall, on the devices from which eBank 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;
- for accessing eBank 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 (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.
– The User must report to the Bank any loss or theft of a mobile device, as well as any change of the phone number used for receiving SMS codes (for transaction authorization) when performing payment transactions through the electronic banking application. Otherwise, the Bank shall not be liable for any cases of fraud.
- The User must not leave the eBank application turned on, and he shall be liable for the damage arising from the abuse by any persons from his environment.
- if the User notices any unusual operation or appearance of the eBank application, he shall immediately notify the Bank thereof.

11.5.5. The User shall follow the Bank web site on a regular basis, in particular, notices by the Bank in connection with the eBank services and adequately respond, in accordance with such notices.
The User is obliged, for the purpose of preventing potential misuse, to familiarise himself/herself with the security rules for using payment instruments on the website of the Association of Serbian Banks: www.ubs-asb.com/korisnici-finansijskih-usluga/bezbednost-bankarskih-klijenata.

11.6 Blocking the George Web Application

11.6.1 The Bank may refuse or delay the execution of a transaction and/or block further use of the George web application if there are justified reasons related to the security of this payment instrument, if there is suspicion of unauthorized use of the payment instrument or its use for fraudulent purposes, or if there is an increased risk that the User will be unable to fulfil payment obligation when the use of the payment instrument is linked to a credit approval or an authorised overdraft.

11.6.2 The Bank is obliged to notify the User of its intention to block the George web application and the reasons for such a block. Unless it is able to notify the User before blocking, the Bank shall do so immediately after the block. The notice of intention to block, or of the actual block of the George web application, shall be sent by the Bank to the User's email address known to the Bank, except where providing such notice is prohibited by regulations or where there are justified security reasons.

11.6.3 The Bank shall re-enable the use of the George web application once the reasons for its block no longer exist.

11.6.4 If the Bank, using a special application, determines that the operating system the User uses to initiate payment transactions via electronic or mobile banking is infected with a virus, malware, trojans, or similar software that allows unauthorized access to the security elements of the payment instrument and the User's unauthorised use, thereby compromising the security of the payment instrument, the Bank shall block further use of the George web application.

The Bank shall not be liable for any damage arisen from the execution of unauthorised transactions if they have been executed for the reasons referred in the above paragraph.

11.7   Notification

11.7.1 The User is informed about payment transactions executed via the George web application through statements sent to the email address registered with the Bank, or by another agreed method. The User may arrange with the Bank to receive notifications about individual payment transactions via SMS messages. The User also agrees to receive additional notifications, of an informative or other nature, through various Bank distribution channels.

11.7.2 The User may file a complaint regarding a transaction initiated through the George web application immediately upon becoming aware of an unexecuted, incorrectly executed, or unauthorised transaction, but no later than 13 months from the date of debit.

11.7.3 The User undertakes to notify the Bank of any change in the User's email address; otherwise, it shall be assumed that the User has been properly informed by the delivery of statements and other notifications to the last registered email address.

12. PAYMENT INSTRUMENT – George Mobile Application Service

12.1 Contracting the Use of the George Mobile Application

12.1.1 The User may contract with the Bank to use the George mobile application as a mobile banking service of Erste Bank a.d. Novi Sad (hereinafter: the Bank).

12.1.2 The User may contract this service only if they have an adequate mobile device capable of supporting the George mobile application.

12.1.3 The User contracts the use of the George mobile application by downloading the application from the App Store and activating it as described below. By activating the application, the User is deemed to have given consent for the use of the payment instrument – the George mobile application.

12.3 Service Type

12.3.1 The George mobile application includes the internet banking services and functionalities listed and described in the user guides.

12.3.2 The George mobile application services enable the User to:
– view of balance and turnover under all accounts
– payment transaction execution:
a. internal transfer of funds between own accounts and accounts for which the User is authorised
b. payment order through credit transfer, including instant credit transfers
c. foreign currency buying and selling
d. FX payment order
e. registration and payment through the Prenesi service
– arranging standing orders and contractual standing orders
– overtaking statements in the application
– filing application for lending products
– Card management – changing card limits, managing spending channels (ATM, POS, and Internet), temporarily blocking and unblocking cards, activating cards sent to the home address, displaying the PIN, card number, and CVV2;
– Contact information management – updating mobile phone number, email address, and card delivery address;
– Consent management – granting or withdrawing consents (Consent and Legal Agreements);
– Push notification management – enabling/disabling notifications, setting payment limits, receiving notifications of incoming, outgoing, and card transactions via Push notifications;
– Two-way communication with the User within the application.

12.3.3 The George mobile application includes the mobile banking services listed and described in the George mobile application user guides. The Bank provides the User with access to all services offered through the George mobile application, and the User independently chooses which services to use. The Bank reserves the right to modify the scope and content of the George mobile application and will notify the User of such changes via its website and within the application itself. The User shall acknowledge and entirely accept such changes. The User has no right to claim compensation for damages in the event of changes to the content of the George mobile application.

12.4 George Mobile Application Use

12.4.1 The User begins activation of the George mobile application by entering unique personal ID number into the application, after which an activation code will be sent to the User via email and an SMS code via SMS to the registered phone number.

12.4.2 The User shall start using the George mobile application after receiving user identification and setting PIN code consisting of 4 to 8 digits.

After activating the George mobile application, the User may choose to log in using the offered biometric data and may also provide consent for payment transactions in the same manner.

Within the George mobile application, the User may opt for the "Prenesi" service, which allows sending money via instant transfer using the recipient's mobile phone number instead of entering the account number, as well as receiving payments in the same way.

All forms of using the George mobile application electronically, with the prescribed user identification, are considered equivalent to signing with a handwritten signature.

12.4.3 The Bank guarantees the User of the George mobile application free disposal of funds in all demand accounts opened under the agreement with the Bank, up to the amount of available funds in the account, including any authorised overdraft.

12.4.4 The User undertakes to fill out payment orders correctly and accurately and to authenticate them with final transaction confirmation, taking into account the available funds in the User's Bank accounts; otherwise, the User bears the risk of non-execution, incorrect execution, or rejection of the payment order.

12.4.5 The User is responsible for the accuracy of all payment order data and bears any loss resulting from entering incorrect data or misuse of the George mobile application in the User's own environment.

12.4.6 The execution time of the payment order is defined by the Bank's Schedule of Terms.

12.4.7 The Bank shall exclude its liability for any consequences that may occur due to the use of an inadequate mobile device.

12.4.8 The Bank is not responsible for the unavailability of the George mobile application resulting from technical problems on the User's equipment, failures or disruptions in telecommunications channels, power outages, or as a result of force majeure.

12.5   Data Protection and Liability for Damage

12.5.1 The User is obliged to keep the George mobile application user identification confidential and accepts full responsibility for all obligations arising under the attributes of the user identification.

12.5.2 The User must immediately and without delay notify the Bank of any misuse, unauthorised use of the George user identification, or other security breaches they become aware of, by one of the following methods: initiating a block of the George mobile application usage as provided in the application, in person at a Bank branch, by calling the contact center at 021/423-364 or 0800-201-201 on weekdays from 8:00–17:00 and Saturdays from 8:00–13:00, or by sending an email requesting the blocking of the George mobile application service to: blokadaplatnoginstrumenta@erstebank.rs. This allows the Bank to prevent further use of the payment instrument and, in the case of an unauthorized payment transaction or a payment transaction resulting from fraud or misuse, to immediately take all reasonable measures to recover the funds.

12.5.3 The Bank has the right to block the use of the George mobile application service if there are justified reasons related to the security of the payment instrument, suspicion of unauthorised use, use for fraud, or in other cases where security reasons require it.

12.5.4 The Bank will automatically block the User's access to the George mobile application service if incorrect user credentials are entered three times during login. In such a case, the User may unblock access in person at a Bank branch or by calling User Support.

12.5.5 The User bears all losses arising from unauthorised payment transactions if such transactions occur due to fraudulent actions by the User or failure to take all reasonable and appropriate measures to protect the personalized security elements of the user identification due to intent or gross negligence.

12.5.6 The User bears all losses related to any transaction resulting from misuse committed by the User and also bears losses arising from failing to fulfil the User's obligations under these General Terms.

12.5.7 The User does not bear losses arising from the use of the George mobile application, i.e., transactions executed after reporting to the Bank the loss, theft, or unauthorized use of user identification, except if the User has committed misuse, participated in misuse, or acted with fraudulent intent.

12.5.8 The User's liability is limited to 3,000 RSD if unauthorized payment transactions are executed via the George mobile application due to the use of lost or stolen user identification, or if the George mobile application user identification was misused.

12.6 Protective and other Actions

12.6.1 The User is obliged to use the George mobile application in accordance with the provisions of these General Terms and Conditions, which govern the issuance and use of this payment instrument.

12.6.2 The User is obliged, immediately upon receiving the George mobile application user identification, to take all reasonable and appropriate measures to protect the personalised security elements of this instrument (password, TAN table, PIN, etc.).

12.6.3 The User is obliged, immediately upon becoming aware of the loss, theft, or misuse of the George mobile application, to notify the Bank.

12.6.4 The User performing payment transactions via the George mobile application is obliged to comply with the following security requirements:

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

Recommendations for the safe use of the George mobile application:
- The User should activate the security features offered by the User's mobile device (for example, screen lock after a 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 the User's 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 a mobile device to a power port, under certain conditions and without the User's knowledge, access to the data and applications on the device may be possible.
- on the devices from which mBank 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 abuse by the persons from his environment.

12.6.5 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.

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

12.6.7 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.

12.6.8 The User is obliged to regularly monitor the Bank's website, particularly the Bank's notices regarding electronic and mobile banking services, and to respond appropriately in accordance with such notices. The User is also obliged, for the purpose of preventing potential misuse, to familiarise himself/herself with the security rules for using payment instruments on the website of the Association of Serbian Banks: www.ubs-asb.com/korisnici-finansijskih-usluga/bezbednost-bankarskih-klijenata

12.7 George Mobile Application Blocking

12.7.1 The Bank may refuse or delay the execution of a transaction and/or block further use of the George mobile application if there are justified reasons related to the security of this payment instrument, if there is suspicion of unauthorized use of the George mobile application or its use for fraud or as a result of fraud, or if there is an increased risk that the User will be unable to fulfil the User's payment obligation when the use of the payment instrument is linked to credit approval or an authorised overdraft for the User.

12.7.2 The Bank is obliged to notify the User of its intention to block the George mobile application and the reasons for such a block. Unless it is able to notify the User thereof prior to blocking, the Bank shall do so immediately upon blocking. The notice of intent to block, or of the actual block of the George mobile application, is sent by the Bank to the User's email address registered with the Bank, unless providing such notice is prohibited by regulations or justified security reasons exist.

12.7.3 The Bank will re-enable the use of the George mobile application once the reasons for its block no longer exist.

12.8 Notification

12.8.1 The User is informed about payment transactions executed via the George mobile application through statements sent to the email address registered with the Bank. The User may arrange with the Bank to receive notifications about individual payment transactions via SMS messages or Push notifications. The User accepts to receive additional notifications, of informative or other nature, through various Bank distribution channels.

12.8.2 The User may file a complaint regarding a transaction initiated through the George mobile application immediately upon becoming aware of an unexecuted, incorrectly executed, or unauthorised transaction, but no later than 13 months from the date of debit. The date on which the Bank delivers the statement of account balance and changes shall be considered the date on which the User is informed.

12.8.3 The User undertakes to notify the Bank of any change in the User's email address, postal address, or mobile phone number; otherwise, it shall be considered that the User has been duly informed by the delivery of statements and other notifications to the last email address, postal address, or mobile phone number registered with the Bank.

12.9 Payment Limits in mBank and eBank Applications

12.9.1. For security reasons, the Bank applies daily limits in terms of payment transaction limits executed through eBank and mBank.

The daily limit for the execution of dinar payment transactions amounts to RSD 1,000,000 (one million).

Daily limit for the execution of foreign currency payment transactions amounts to EUR 10,000 (ten thousand), i.e. 10,000 (ten thousand) in other foreign currencies.

The Bank retains the right to, in accordance with the regulations and its internal acts, check and assess the justification of the request priori to limit change approval.

12.A   SPECIAL SECURITY ACTIONS TAKEN BY THE BANK

12.A.1   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.

12.A.2   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.

12.A.3   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.

13.   PAYMENT SERVICE PROVISION

13.1   Consent for Payment Transaction

13.1.1 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.

13.1.2 The manner of granting consent to payment transactions shall depend on a payment instrument (payment card, eBank, and order receipt channel (by direct provision at the Bank branch, electronically, by presenting and reading QR code at the merchant's site in the event of initiating instant transfer of credit, etc.).

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

- at the Bank branches – by signing payment order,

- Via the George web application – by confirming the transaction using strong customer authentication via a push notification in the George mobile application (with PIN entry or the use of biometric data). During the transaction confirmation process, the transaction amount and the payment recipient are clearly displayed to the user, ensuring compliance with security standards and protection against unauthorised actions.
- Via the George mobile application – by confirming the transaction using strong customer authentication, which includes entering a PIN code or using biometric data (fingerprint or facial recognition). During the transaction confirmation process, the transaction amount and the payment recipient are clearly displayed to the user, ensuring compliance with security standards and protection against unauthorised actions.

- through the NetBanking and mBanking using one-off SMS code, token, (biometric data (fingerprint or facial recognition), or other security designation, and final transaction verification in the manner defined in the application for such service,

- 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 on 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. For users of the George mobile application, additional authentication for card payments at online points of sale that support 3D Secure is performed via a push notification in the George mobile app and by entering a PIN or biometric data, thereby giving consent for the payment transaction.

- granting consent through the payee and payment initiation service provider

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

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

- if he has agreed and signed standing order or direct debit with the Bank or payee for the execution of single and/or a series of payment transactions (standing order and direct debit)

- using the deep link technology via mBanking.

13.2   Payment Order Types

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

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

13.2.3 Payment order shall include the following basic elements: 1) name of payer, 2) name of payee, 3) number of payee's current/payment account, 4) currency designation, 5) amount, 6) payment purpose, 7) payment code, 8) model reference number relating to crediting number, 9) reference number of crediting, 10) place and date of receipt, 11) execution date, 12) payer's signature and/or consent 13) method of order execution – urgent.

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

13.2.5 Outgoing payment order shall include the following basic elements: 1) name of payer, 2) name of payee, 3) number of current/payment account, 4) currency designation, 5) amount, 6) payment purpose, 7) payment code, 8) model reference number relating to debiting number, 9) reference number of debiting, 10) place and date of receipt, 11) execution date, 12) payer's signature and/or consent.

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

13.2.7 Electronic payment orders shall include the same elements as payment order forms in hard copy.

13.2.8 Transfer order shall include the following basic elements: 1) order execution method – urgent, 2) name of payer, 3) name of payee, 4) number of payer's current/payment account, 5) number of payee's current/payment account, 6) currency designation, 7) amount, 8) payment purpose, 9) payment code, 10) model reference number relating to crediting number, 13) reference number of crediting, 14) place and date of receipt, 15) execution date, 16) signature and/or consent by payee/payer.

13.2.9 The Bank may individually, for the purpose of payment transaction execution, also determine additional payment order elements – bar code, optical character recognition – OCR, etc.

13.2.10 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 Operations, 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.

13.3   Payment Order Receiving

13.3.1 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/mBanking/payment card issuance, etc.) provided by the Bank relating to such accounts.

13.3.2 The Bank may receive a payment order:

- -by personal submission at the Bank branch, in writing;
- electronically through Netbanking/Mbanking; or by scanning or presenting the QR code and through deep link technology
- Indirectly through the payee (using the payment card or by direct debit), or through service provider od payment initiation

13.4   Bank Procedure upon Order Receiving

13.4.1 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.

13.4.2 Any orders in the amount exceeding the amount set out in the Law on the Prevention of Money Laundering and Terrorism Finance or orders for which particular documentation is prescribed 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.

13.4.3 The Bank shall be entitled to request 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.

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

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

13.4.6 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.

13.5   Order Receipt Time

13.5.1 The time for payment order receipt shall be the moment when the Bank directly receives payment order.

13.5.2. The payment orders in writing, in the amount up to RSD 300,000, indicated by the User when the order is filled in as an instant payment (urgent) will be, in the event such order is received during business day, executed by the Bank instantly or almost instantly.

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

13.5.4   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 a business day of payment service provider, it shall be deemed that order is received on the next business day of such provider.

13.5.5   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.

13.5.6   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. The payment orders in the amount up to RSD 300,000, initiated electronically through the eBank, for which client, when the order is filled in, selects the instant payment (urgent) option, will be, in the event such orders are issued, executed by the Bank instantly or almost instantly at any time of the day during every day in year.

13.5.7   User's payment account may be debited prior to the payment order receipt.

13.6   Payment Order Execution

13.6.1 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 account for the payment of total amount from order and accrued fee for payment service, or if the user executing incoming payment to its current account provides the Bank with the cash in the amount necessary for order execution,

- if consent is granted for payment order as per agreement.

13.6.2 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.

13.7   Payment Order Rejection

13.7.1 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.

13.7.2 The Bank shall be entitled to reject an 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, regulations in the area of sanctions, or internal acts of the Bank passed based on such regulations.

13.7.3 In the event of an instant transfer order, the Bank shall be entitled to reject such an order if it receives a notification from the IPS system operator on the rejection of the execution of such order, because, the conditions set out in the rules of such system have not been met for the execution of such transfer. 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.

13.7.4 If a payment order is rejected by the Bank, it shall be deemed that the payment order has not been received.

13.7.5 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.

13.8   Payment Order Recall

13.8.1 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 ensuring to initiate such recall prior to the execution of the instructions contained in such order provided that the Bank has not executed such payment order.

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

13.8.3 If transaction is initiated by the payee using direct debit, the payer may recall such order no later than at the end of the business day preceding the date set out for debiting payer's account.

13.8.4 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 payment transactions initiated by payment card, the payer may not recall payment order upon transaction authorisation and/or upon inputting PIN and approving transaction.

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

13.8.6 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.).

13.8.7 Recall of 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 Retail and Registered Farm Service Price List.

13.8.8 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.

13.9   Payment Transaction Execution Deadline for Payer's Payment Service Provider

13.9.1 Payment orders shall be executed in accordance with the time of receipt and execution date, in accordance with the Cut-off Times.

13.9.2 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.

13.9.3 For payment transactions not covered in the above paragraph, deadlines for payment transactions set out in the law and/or relevant by-laws shall apply.

13.9.4 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 the 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.

13.10 Execution of Payment Transaction to the Payee

13.10.1 The Bank shall, as the payee's payment service provider, without undue delay, credit the payment account of the User – payee or, where the User does not have a payment account of the Bank, make the funds available to the User:
> 1) if the amount of the payment transaction for the User-payee has been credited to the Bank account or if the Bank has otherwise received such amount;
> 2) if the Bank has received all information necessary for crediting the payee's payment account or making funds available to the payee.

The Bank shall enable the User–payee to dispose of the funds immediately upon crediting such funds on the payment account of this 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.

13.10.2 If the payment service user 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 on the next business day, at the latest.

13.10.3 If funds have been credited to the account of the Bank on the day which is not a business day, it shall be deemed that the Bank has received such funds for the payee on the next business day.

13.11   **Debit Value Date and Credit Value Date**

13.11.1 The payer's payment service provider shall ensure that the value date of debiting the payer'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.

13.11.2 The payee's payment service provider shall ensure that the value date of crediting the payment account of the payee, in connection with payment transaction execution, is no later than the business date when the payment transaction funds are credited on the account of such provider.

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

13.12.1 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 item 13.10.2.

13a   Confirmation on the availability of funds

13a.1 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. on payment Services

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.

13b   Rules on access to payment account in the case of payment initiation services

Where the payer's payment account is accessible online, 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 this 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 this 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.

13c   Rules on access to and use of payment account information in the case of account information services

Where a payment account is accessible online, 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.

13.d   Limits of the access to payment accounts by payment service providers

13.d.1 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.

13e   Payment transactions where the transaction amount is not known in advance

13.e.1 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.

14. INFORMATION AND COMMUNICATION METHOD BETWEEN THE BANK AND THE USER

14.1 Information in Pre-agreement Stage

14.1.1 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.

14.1.2 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.

14.1.3 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 framework agreement shall be valid for five days from the date of delivery to the User.

14.2 Information of Payer prior to and upon Payment Transaction Execution

14.2.1 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.

14.2.2 Data on the execution terms, fees, and costs shall be communicated to the payer at the site of payment transaction execution.

14.2.3 The Bank will, without delay, after any executed individual payment transaction, provide the payer with the information on such transaction, in the manner and volume as stipulated in the Law on Payment Transactions or in higher volume as agreed.

14.2.4 The Bank shall periodically provide the information referred to in the above paragraph on a monthly basis, in the agreed manner, in hard copy or other permanent data carrier.

14.2.5 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 on a monthly basis.

14.2.6 The Bank shall, minimum on an annual basis, free of charge, provide the User with the report on all charged fees for the services connected to the payment account (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.

14.3 Information to Payee upon the Execution of Individual Payment Transaction

14.3.1 The Bank shall, immediately upon transaction execution, provide the User – payee with data in the manner and volume as stipulated in the Law or in higher volume as agreed.

14.3.2 The Bank shall periodically provide the information referred to in the above paragraph on a monthly basis, in the agreed manner, in hard copy or other permanent data carrier.

14.3.3 The Bank shall provide the payer, upon his request, free of charge, with the information referred to in paragraph 1 of this item on individual executed payment transactions on a monthly basis.

14.4 Communication Method

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

14.4.2 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.

14.4.3 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.

14.4.4 The User shall notify the Bank in writing on any changes of personal data, address, e-mail address, 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.

14.4.5 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.

15   FEES AND INTEREST RATES

15.1   Fees

15.1.1 For payment service execution, the Bank shall charge fees in accordance with the Retail and Registered Farm Product and Service Price List.

15.1.2 The User accepts that the Bank shall collect fees and other costs arisen in accordance with this Agreement by debiting his account. Regarding fees for FX account maintenance, the Bank shall collect fees by debiting the User's account at the middle exchange rate of the NBS applicable on the date of collection.

RSD account maintenance fee shall be charged if the User has had minimum one transaction on a monthly basis, save for Premium Current Account, 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.).

15.1.3 The User accepts and authorises the Bank to, in the event he does not have funds on his current account on fee collection day, the Bank is to reserve funds and, upon the inflow thereof, make collection from his account. In the event that there are insufficient funds on the User's account, the User accepts and authorises the Bank to also make partial collection from the User's account up to the complete liability settlement.

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.

15.1.4 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.

15.1.5 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.

15.1.6 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.

15.2 Interest Rates

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

15.2.2 On the amount of due and unpaid obligations to the bank, the Bank calculates and charges default interest in the amount and in the manner prescribed in the Law on the Protection of Financial
On the overrun amount the Bank calculates and charges interest According to Framework agreement and the Law on the Protection of Users of Financial Services.

16 LIABILITY FOR PAYMENT TRANSACTION EXECUTION

16.1 Liability for Non-approved Payment Transaction

16.1.1 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.

16.1.2 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.

16.2 Payer's Liability for Unauthorised Transaction

16.2.1 By way of derogation from the above item hereof, 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) use of the payment instrument that has been misused

16.2.2 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.

16.2.3 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.

16.2.4 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.

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

16.3.1 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.

16.3.2 If the payer's payment service provider is liable for non-executed or incorrectly executed payment transaction, it shall, immediately upon becoming 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.

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

The payee's payment service provider shall ensure, 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.

16.3.3a Where a payment transaction is executed after the time set out in item 11.10-11.12 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 pursuant to item 11.10-11.12 herein.

16.3.4 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.

16.3.5 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.

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

16.4.1 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.

16.4.2 If payment order has not 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 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.

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

16.4.4 If the payee's payment service provider provides the payee, and, as necessary, the payer's payment service provider, with the evidence that it is not liable to the 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.

16.4.5 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.

16.5 Rights and Obligations of Payment Service Providers in Case of Incorrectly Executed Payment Transaction

16.5.1 Rights and obligations of payment service providers in case of incorrectly executed domestic payment transactions are 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 the case referred to in the above paragraph, item 1) and 3), the Bank may debit the User's account for the amount of incorrectly or groundlessly received funds.

14.5.2 The refund of the funds referred to in paragraph 1 items 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.

16.6a Rights and obligations of payment service providers in cases of fraudulent or misused transactions

16.6.1a 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.

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

16.6.1 The payment service provider shall be liable to the payment service user for a non-executed or incorrectly executed payment transaction in dinars even if the liability is attributable to an intermediary participating in the execution of that payment transaction among payment service providers.

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

16.7.1 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 of payment transaction with a view to refunding

the amounts of payment transaction and notify the user about the outcome of measures taken without undue delay.

16.8   Liability for Using Unique Identifier

16.8.1 If 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 determination irrespective of other data the payment service provider has been provided with.

16.8.2 If unique identifier submitted by the payment service user to payment service provider is incorrect, the payment service provider shall not be liable for non-executed or incorrectly executed payment transaction.

16.8.3 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.

16.8.4 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.

16.8.5 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.

16.9   Liability Exclusion due to Force Majeure or Law

16.9.1 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.

16.9.2   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.

16.9a   Exclusion of Liability for the Actions of Intermediary Bank

16.9a.1 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 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.

16.9b Liability for losses stemming from unauthorised, non-executed, defective or late payment transactions

16.9b.1 Provisions of Articles 16.2-16.4 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.

16.9.c Burden of proving the execution of payment transactions

14.9.c.1 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.

16.9d Execution of international payment transactions and payment transactions in currencies of third countries

16.9d.1 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).

16.9e SEPA Credit Transfer (SCT)

16.9e.1 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;
• 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);

16.9e.2 When issuing a payment order for the SCT execution, the Bank must obtain the following data from the User:

1) payer's name and surname;
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.

16.9e.3 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 name of payer;
2) data on payment transaction amount;
3) payment transaction description.

16.9e.4 Time of SEPA SCT order receipt and execution is set out in the Bank's Cut-off Time.

16.9e.5 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.

16.9e.6 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.

16.10   User's Complaints

16.10.1 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.

16.10.2 The User shall immediately notify the Bank on any unauthorised, non-executed, or incorrectly executed payment transactions, and/or if he requires correct payment transaction execution, upon becoming aware of such payment transaction, but no later than 13 months from the date of account debiting. The date of the receipt of the statement on the balance and changes on the account from the Bank will be deemed to be the date of informing the User.

16.10.3 Complaint, i.e. notice on a non-authorised, incorrectly executed, or non-executed transaction may be filed at the Bank's point of sale, by sending 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 data subject to the complaint.

16.10.4 Upon the expiry of the period referred to in the sub-item 16.10.2, 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.

16.11   Corrections on Account

16.11.1 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.

16.11.2 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.

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

17   PAYMENT ACCOUNT DEBITING WITHOUT PAYMENT ORDER

17.1 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 the case referred to in item 16.6a.1,

5)   in other cases prescribed in the law.

17.2 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.

18   PROTECTION OF THE RIGHTS AND INTERESTS OF PAYMENT SERVICE USER

18.1   Introductory Provisions

18.1.1 If the Bank fails to be in compliance with provisions of this 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 shall be entitled to the protection of his rights and interests.

18.1.2 The procedure of protecting rights and interests of payment service users shall subject to provisions of the law governing the protection of financial services consumers which relates to exercising the protection of rights and interests of financial services consumers.

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

18.2   Right to Complaint

18.2.1 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.

18.2.2 The User shall be entitled to complaint within 15 days after the User became aware of the disputable event, but, in every case, three years from the date when his right or legal interest has been breached.

18.2.3 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.

18.2.4 The Bank shall, in its business premises in which services are rendered to users, by mail, e-mail, within the eBanking/mBanking application, and on its web page, 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.

18.3   The Right to Filing Claim to the National Bank of Serbia

18.3.1 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.

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

18.3.3 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.

18.4   Extra Judicial Settlement of Disputable Relation

18.4.1 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.

18.4.2 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.

18.4.3 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.

18.4.4 The mediation procedure shall be confidential and urgent.

18.4.5 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.

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

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

19.   CLOSING PROVISIONS

19.1   General

19.1.1 Excerpt from the 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.

19.1.2 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.

19.2   Agreement Amendments

19.2.1 The Bank shall notify the User on any General Terms/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 electronically provide amendments if e-mail address is available to the Bank, otherwise the delivery will be made by mail.

19.2.2 It will be deemed that the User has acknowledged proposed amendments if the Client has not notified the Bank on its disagreement therewith, until the date of the beginning of the application thereof.

19.2.3 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.

19.2.4 The User may request 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.

19.3   Payment Service Termination

19.3.1 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.

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

19.3.3 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.

19.3.4 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.

19.3.5 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.

19.3.6 The Bank shall be entitled to terminate the Agreement, excluding notice period, in the following cases:

• if it is found that any statement of the client, as well as provided documents and data by the client are not complete, true or updated;

• if there are reasonable grounds of suspicion that the client uses the current account for non-permitted services, fraud, or with the aim of any other misuse of the law;

• in accordance with the Law on the Prevention of Money Laundering and Terrorism Finance and sanction regulations

The Bank may also unilaterally terminate the Framework Agreement in other cases set out in the Framework Agreement, General Terms of Business, the law governing contracts and torts, or in other law.

19.4   Regulations Application

19.4.1 Applicable regulations and the Bank General Terms of Business, legislation, and other acts of the Bank governing operation with 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.

19.4.2 The User acknowledges that he is aware of and fully accepts the Bank General Terms of Business.

19.4.3 Executing the agreement, application form, or other form of the Bank arranging the use of the payment services, the User acknowledges that he is informed and that he 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.

19.5   Dispute Resolution

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

19.6   Application of the General Terms

19.6.1 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.

19.6.2 The General Terms shall come into force on 20 May 2026, except for the SEPA credit transfer provisions which shall come into force on 04 May 2026.