ERSTE BANK A.D. NOVI SAD
BOARD OF DIRECTORS
Number: 1436/2023-503/8
Date: 30.01.2023.

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 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;
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 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;
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.

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, 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;

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 where the payment service provider enables the payee the execution of payment transactions initiated by the payer by using a specific payment instrument;

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;

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.

The users who, until the effective date of the General Terms, held a multi-currency FX account, on which they had a balance, or who did not have any balance, but had turnover on the account in a foreign currency in the period from 01 December 2020 to the beginning of the GTB application, new FX accounts, for every currency, they had on balance, or in which they had turnover on the account, will be opened by the Bank.

The existing FX account of the users who opened the FX account after 01 June 2021, excluding any balance and turnover on the account, will be tied to the EUR currency.

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

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;

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 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. In the event of the application of the consumer who has legal residence in the Republic of Serbia to open RSD payment account with basic services, such application may be rejected by the Bank even in the case the consumer has already held payment account with other bank referred in Article 73p of the Law on Payment Services unless the consumer provides the statement in writing and submits the notice of the other bank that the payment account will be closed.

4.1.8 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.

4.1.9 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.

4.1.10 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 on the Bank web page www.erstebank.rs and in the Bank business premises in which operations with clients are executed.

4.1.11. The Bank shall enable the payment service user opening of the payment account with a new payment service provider to change the payment account in the same currency, solely based on the authorisation by the payment service user submitted in writing to the new service provider, provided that the payment service user has no overdues under such account and that other conditions prescribed in the Law on Payment Services are fulfilled.

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.

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 (Visa, MasterCard, etc.).

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.

5.2 Card Issuance and Card Data Protection

5.2.1 The User shall be provided with the Card and PIN (personal identification number). The Bank shall guarantee the Card User PIN issuance secrecy until the provision 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 to keep 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.

5.2.2 The User must not disclose PIN to other persons (including, without limitation, family members, merchant, bank officer). 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 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 The Debit Card User shall give his consent for the execution of specific payment transaction, i.e. when using the Card on ATM, he shall type his PIN, and if Card is used on EFTPOS terminal, he shall sign slip or input PIN. In case of the Card that may be used for payment through the Internet, the User shall, when making payment on the Internet, input full number of card (PAN) and CVV2 value (three-digit number embossed on the back of the card). If the web site through which an Internet payment is executed supports 3D Secure protection mechanism, inputting the OTP password received by SMS, the User confirms the consent to execute the payment to be debited on his account.

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 EFT POS terminals and by the Internet.

5.3.3 The Bank shall not be liable if merchant does not want to accept the Card though VISA/ MAESTRO/MASTER CARD logo 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 The User shall, when paying for goods and services, also sign appropriate slip at acquiring point. Acquirer shall issue slip/account copy to the User.

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 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 for issued debit card shall amount to RSD 350,000.00, for executing transactions through EFTPOS terminal and RSD 50,000.00 for cash withdrawal on ATM. Limit of the number of daily transactions executed using card through EFTPOS shall be 15 transactions. The Card User shall be entitled to request the change in daily limit level, by providing application for limit change, without the obligation of executing Annex to the Framework Agreement.

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 Debit Card User shall be entitled to, within 30 days prior to card validity, state unless he wants to be re-issued card..

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

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 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/Abused Card

5.6.1. The User shall immediately report Debit Card loss/theft/abuse 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. 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.

5.7 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 or failure 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 to notify the Bank, without delay, on loss, theft, and abuse of payment card.

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 abuse.

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 abused Card if the User has failed to protect his personalised security elements.

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 abuse 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 abuse 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 abuse of the data from the card, and the User shall make prior check whether this is the web site referred 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 abuse (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 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, 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.

7 DIRECT DEBIT

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 in paragraph 1 of this Article. The payer may not refer to the condition

referred 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 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.

7.2.5 If he rejects the request referred 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 The payer and its payment service provider may agree by provisions of the framework agreement regulating direct debits that the payer may request a refund of the amount of the authorised payment transaction executed through direct debit even when the conditions under paragraph 1 of this Article have not been met. 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.

8.2 Card Issuance and Card Data Protection

8.2.1 The User shall be provided with the Credit Card and PIN (personal identification number). 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 abuse 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 The Credit Card User shall give his consent for the execution of specific payment transaction, i.e. when using the card on ATM, he shall type his PIN, and if Card is used on EFTPOS terminal, he shall sign slip or input PIN. In case of the Card that may be used for payment through the Internet, the User shall, when making payment on the Internet, input full number of card (PAN) and CVV2 value (number embossed on the back of the card). If the web site through which an Internet payment is executed supports 3D Secure protection mechanism, inputting the OTP password received by SMS, the User confirms the consent for the payment to be debited on his account.

8.3.2 Credit Card may be used at all points of sale and ATMs in Serbia/abroad where logo of card company 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 VISA/ MAESTRO/MASTER CARD/DINA CARD logo 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 Credit Card User shall, when paying for goods and services, also sign appropriate slip at acquiring point. Acquirer shall issue slip/account copy to the User.

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. 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.

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.

8.4 Currency Exchange Rate

8.4.1 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.

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

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 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/Abused Card

8.6.1 The User shall immediately report loss/theft/abuse 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 disable any the further use thereof. The User shall, within 2 business days, confirm the report of the lost/stolen Card 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.

8.7 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, as well as if the User fails to notify the Bank, without delay, on loss, theft, and abuse of Credit Card.

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-D Secure protection mechanism, any risk relating to such payment will be assumed by the Credit Card User, and the Bank will not be liable if any data from the Credit Card are abused.

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 abuse.

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 if the User has failed to protect its personalised security elements.

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 abuse 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 abuse 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 abuse of the data from the card, and the User shall make prior check whether this is the web site referred 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 abuse (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 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 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.

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 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: blokadaplatnoginstrumenta@erstebank.r

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 and notify the Bank, without delay, on loss, theft, and abuse of the payment instrument and/or user identification.

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 abused, because the User has failed to protect his personalised security elements.

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 abuse 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 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 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. 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. 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 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.

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, to notify the Bank, without delay, on loss, theft, and abuse of the payment instrument and/or user identification.

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 abused, because the User has failed to protect his personalised security elements.

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 abuse 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 shall 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 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 SERVICE PROVISION

11.1 Consent for Payment Transaction

11.1.1 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.

11.1.2 The manner of granting consent to payment transactions shall depend on a payment instrument (payment card, NetBanking, mBanking, 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.).

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

- at the Bank branches – by signing payment order,

- through the E-Bank and E-Bank using one-off SMS code, token, smart card, or other security designation, and final transaction verification in the manner defined in the application for such service,

- using payment transaction, handing card to the merchant and inputting PIN in the POS device or by signing the slip generated from the POS device, placing the card close to the contactless device, inserting the card in the ATM and inserting PIN in the ATM, inserting data on payment card – validity period, card number (PAN), CVV2 value (the number embossed on the back of the card) during i-commerce, and one-off (OTP) password received through SMS if the web site through which i-commerce is made supports 3D Secure mechanism of protection, inserting or placing the card close to the self-service device, or by using the card in the manner in which the self-service device requires the authorisation,

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

- 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 (when the technical conditions for this functionality are fulfilled).

11.2 Payment Order Types

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

11.2.2 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).

11.2.3 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.

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

11.2.5 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.

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

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

11.2.8 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.

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

11.2.10 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.

11.3 Payment Order Receiving

11.3.1 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.

11.3.2 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).

11.4 Bank Procedure upon Order Receiving

11.4.1 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.

11.4.2 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.

11.4.3 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.

11.4.4 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.

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

11.4.6 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.

11.5 Order Receipt Time

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

11.5.2. 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.

11.5.3 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.

11.5.4 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.

11.5.5 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.

11.5.6 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 Netbanking/mBanking, 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.

11.6 Payment Order Execution

11.6.1 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.

11.6.2 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 in the order are sufficient for the execution thereof.

11.7 Payment Order Rejection

11.7.1 The Bank may reject order execution unless all of the conditions for order execution prescribed herein are fulfilled.

11.7.2 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.

11.7.3 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.

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

11.8 Payment Order Recall

11.8.1 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.

11.8.2 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.

11.8.3 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.

11.8.4 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.

11.8.5 If user recalls an order upon the expiry of the deadlines referred 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.

11.8.6 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.).

11.8.7 Recall of order upon the expiry of the deadlines referred in paragraph 1–3 of this Article may be charged by the Bank, in accordance with the Retail and Registered Farm Service Price List.

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

11.9 Payment Transaction Execution Deadline

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

11.9.2 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.

11.9.3 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.

11.9.4 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.

11.10 Execution of Payment Transaction to the Payee

11.10.1 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.

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.

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.

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

12.1 Information in Pre-agreement Stage

12.1.1 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.

12.1.2 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.

12.1.3 The Bank may provide the User with the information referred 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.

12.2 Information of Payer prior to and upon Payment Transaction Execution

12.2.1 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.

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

12.2.3 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.

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

12.2.5 The Bank shall provide the payer, upon his request, free of charge, with the information referred in paragraph 2 of this Article on individual executed payment transactions on a monthly basis.

12.2.6 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.

12.3 Information to Payee upon the Execution of Individual Payment Transaction

12.3.1 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.

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

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

12.4 Communication Method

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

12.4.2 The Bank and the User shall perform the communication as agreed: by exchanging notices and other letters by mail or e-mail, and, upon the explicit request by the User, by direct overtaking of a letter at Bank branch.

12.4.3 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.

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

13 FEES AND INTEREST RATES

13.1 Fees

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

13.1.2 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.). 13.1.3 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.

13.1.4 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.

13.1.5 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.

13.1.6 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.

13.2 Interest Rates

13.2.1 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.

13.2.2 Legal default interest in the amount and in the manner prescribed in the Law on Default Interest shall be accrued and charged by the Bank to the funds exceeding the account limit (negative balance) and to any overdue funds.

14 LIABILITY FOR PAYMENT TRANSACTION EXECUTION

14.1 Liability for Non-approved Payment Transaction

14.1.1 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.

14.1.2 If the Payment Service User denies that he has given consent for the executed payment transaction or claims that payment transaction has not been duly or timely executed, and the Bank fails to prove that payment transaction authentication has been implemented and that payment transaction has been incorrectly recorded and posted, the Bank will refund the amount of such transaction to the payer i.e. it will restore the payer's payment account to the balance in which it would have been unless non-approved payment transaction has been executed, and refund the amount of all fees charged to the payer, i.e. pay the amount of any fees the payer would be entitled to unless non-approved payment transaction has been executed.

14.2 Payer's Liability for Unauthorised Transaction

14.2.1 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) misappropriation of a payment instrument if the payer has failed to protect its personalised security features.

14.2.2 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.

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

14.2.4 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.

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

14.3.1 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.

14.3.2 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.

14.3.3 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.

14.3.4 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.

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

14.4.1 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.

14.4.2 If payment order has not been submitted or payment order has not been correctly submitted in the case referred 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.

14.4.3 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.

14.4.4 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.

14.4.5 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.

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

14.5.1 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 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 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.

14.6 Liability of an Intermediary for Non-executed or Incorrectly Executed Payment Transactions

14.6.1 The payment service provider shall be liable to the 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.

14.7 Obligation to Trace Funds in Case of Non-executed or Incorrectly Executed Payment Transactions

14.7.1 In case of a 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.

14.8 Liability for Using Unique Identifier

14.8.1 If payment order is executed in accordance with the payee's unique identifier referred 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.

14.8.2 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.

14.8.3 In the case referred in paragraph 2 of this Article, the payment service user shall be entitled to require its payment service provider to take any reasonable measures i.e. to provide it with information on payment transaction monetary funds flow (e.g. on payee's payment service provider and/or payee) with a view to refunding the payment transaction amount.

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

14.8.5 In the event of non-executed payment transaction due to an incorrect unique identifier referred 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.

14.9 Liability Exclusion due to Force Majeure or Law

14.9.1 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.

14.9.2 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 in the Cut-off Times, shall be excluded.

14.9a Exclusion of Liability for the Actions of Intermediary Bank

14.9a.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.

14.10 User's Complaints

14.10.1 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.

14.10.2 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.

14.10.3 Complaint request 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 request 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 regarding which the complaint is filed.

14.10.4 Upon the expiry of the period referred in the sub-item 15.10.2, 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.

14.11 Corrections on Account

14.11.1 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.

14.11.2 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.

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

15 PAYMENT ACCOUNT DEBITING WITHOUT PAYMENT ORDER

15.1 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 in item 14.5.1,

5) in other cases prescribed in the law.

15.2 The executed payment transaction referred 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.

16 PROTECTION OF THE RIGHTS AND INTERESTS OF PAYMENT SERVICE USER

16.1 Introductory Provisions

16.1.1 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.

16.1.2 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.

16.1.3 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.

16.2 Right to Complaint

16.2.1 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.

16.2.2 The User shall be entitled to complaint within three years from the date when his right or legal interest has been breached.

16.2.3 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.

16.2.4 The Bank shall, in its business premises in which services are rendered to users, by mail, e-mail, 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.

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

16.3.1 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.

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

16.3.3 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.

16.4 Extra Judicial Settlement of Disputable Relation

16.4.1 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.

16.4.2 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.

16.4.3 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.

16.4.4 The mediation procedure shall be confidential and urgent.

16.4.5 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.

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

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

17. CLOSING PROVISIONS

17.1 General

17.1.1 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.

17.1.2 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.

17.2 Agreement Amendments

17.2.1 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.

The Bank will electronically provide amendments if e-mail address is available to the Bank, otherwise the delivery will be made by mail.

17.2.2 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.

17.2.3 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.

17.2.4 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.

17.3 Payment Service Termination

17.3.1 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.

17.3.2 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.

17.3.3 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.

17.3.4 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.

17.3.5 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.

17.3.6 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 abuse 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

17.4 Regulations Application

17.4.1 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.

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

17.4.3 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.

17.5 Dispute Resolution

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

17.6 Application of the General Terms

17.6.1 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.

17.6.2 The General Terms shall apply from 03.05.2023.