SPECIAL CONDITIONS FOR CREDIT CARDS TO COMPANIES UNICREDIT BANK SERBIA JSC BELGRADE

Belgrade, 20th October 2025

TABLE OF CONTENTS

Introductory provisions:
UniCredit Bank Serbia JSC Belgrade (hereinafter referred to as the Bank) by these Special Conditions for Credit Cards for Companies (hereinafter referred to as: the SC for Credit Cards) shall regulates mutual rights and obligations of the Bank and the Cardholders related to the conditions for credit card issuance and use.

I. MEANING OF CERTAIN TERMS

Cardholder - refers to the legal entity that is the holder of the primary and additional credit card, as defined in these Terms of Use for credit card operations.**Card Issuance Application -** means the Bank form filled out by potential cardholder for the issuance of a credit card.
Payment Card - in terms of these SC for Credit Cards is a credit card in physical and digital form, which represents a payment instrument, which allows the Cardholder to pay for goods or services either through/ payment/a point of sale or remotely and/or to withdraw and/or deposit cash and/or use of other services at an ATM or another device and which all represent debit and credit transaction.
Main Card - means a card issued to the Cardholder, the account owner.
Additional Card - means a card linked to the main card account, which usage results in debits/credits the main card account.
PIN - a numeric code known only to the User, which serves as an authentication element for the cardholder or for the transaction initiated by the cardholder and/or for the authorization of payment transactions. As such, it is strictly confidential.
Acceptance point – the point of sale of the payee's goods and/or services where there is a device through which card transactions can be initiated (ATM, POS terminal, online point of sale).
Online point of sale - a point of sale of the payee's goods and/or services on the Internet that accepts a card as a non-cash means of payment.
Acceptor - a legal person designated as the recipient of funds that are the subject of a payment transaction.
ATM - means an electronic device which, depending on its features, may serve for cash withdrawal or deposit, statement enquiry, PIN change, etc.
POS (Point of Sale) terminal- is an electronic or mobile device authorising transactions and electronic acceptance of payment cards at an acceptor's points of sale. It constitutes an integral part of an electronic system for payment card transaction acceptance and processing.
Digital wallet - in a term of this SC for Credit cards is a mobile payment application solution of a digital wallet service provider, which allows the Cardholder to register data related to one or more payment cards within the application and thus digitize the cards for the purpose of initiating payment transactions. On the Bank's website, the cardholder can find out in which digital wallets one or more debit cards issued by the Bank can be registered as a digitized card.
Digitized card - refers to a debit card registered in the Digital Wallet and/or the Bank's electronic and mobile banking applications, which enables the User to initiate payment transactions without using a physical card at points of sale, ATMs that support contactless transactions, and online merchants that allow such payment methods.
The User can find information on the Bank's website regarding which debit cards can be digitalized.
Mobile Device - in a term of this SC for Credit cards means the device on which the Digital Wallet or POS terminal is installed.
SMS Card Alarm - is a service available to the Cardholders allowing them to receive text messages via their mobile phone in respect of each approved card transaction. The division of the transaction is possible write upon receipt of an SMS message with the details of the transaction, but not later than the last day of the month when the transaction is completed.
CVV2 code - means a three-digit number on the back of the card used for the card verification in online payments.
Daily Limit - means a daily allowed amount of funds and number of transactions for withdrawing cash and paying for goods and services.
Credit Limit - is a contractually agreed amount of funds made available by the Bank to the Credit Cardholder.
Credit Card Statement/transaction report - means an overview of information on individual payment transactions executed for a certain period and submitted to the card holder.
3D Secure environment - An online payment environment at internet merchants that requires additional user authentication at the moment of giving consent for the execution of a payment transaction initiated by payment cards from the respective card scheme. This applies only to specific internet merchants that are supported by certain card schemes.
Contactless payment- is carried out by tapping the payment instrument on devices (POS/ATM) where the merchant has enabled contactless payment. In certain cases, PIN entry may be required. When initiating contactless transactions at ATMs, it is necessary to enter a PIN.
OTP code – a security element in the form of a one-time numeric password sent to the User during the initiation of a payment at 3D Secure internet merchants, to the mobile phone number registered in the Bank's system, for the purpose of cardholder authentication.**Payment transaction** means the payment, transfer or payment of funds initiated by the payer or on his behalf or by the payee, and it is performed regardless of the legal relationship
between the payer and the payee.
Payment transaction initiation means the taking of actions which are a precondition for starting the execution of a payment transaction, including payment order issuance and
Authentication.
Remote payment transaction means a payment transaction initiated via internet or through a device that can be used for distance communication.

Authentication means a procedure which allows the payment service provider to verify the identity of a payment service user or the validity of the use of a specific payment instrument,
including the use of the user's personalised security credentials.
Strong customer authentication means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something
only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others and is designed in such a way as to protect the confidentiality of the authentication data.
Personalised security credentials mean personalised data and features provided by the payment service provider to a payment service user for the purposes of authentication (eg PIN code or OTP code for 3D Secure authentication).
Sensitive payment data means data, including personalised security credentials which can be used to carry out fraud, for the activities of payment initiation service providers and
account information service providers, the name of the account owner and the account number do not constitute sensitive payment data.
A payment initiation service provider is a payment service provider that performs a service where, at the request of a payment service user, a payment order is issued to the credit of the payer's payment account maintained with another payment service provider.

II. GENERAL CONDITIONS

1. The rights and obligations of Credit Cardholders shall be governed by Contract on Issuance and Usage of Credit Cards, the SC for Credit Cards, as well as the Tariff for general banking services for Corporative clients, i.e. Tariff for general banking services for SME clients (hereinafter referred to as: the Fee Tariffs).
2. The credit cards are the property of Unicredit Bank Serbia JSC and they are issued under the name of the person in question, who may not give it for use to any third parties.
3. The credit cards issued by the Bank, and which may be used for paying for goods and services/the receipt of funds through POS terminals and online, for withdrawing cash locally and internationally are: Mastercard Business Charge and Mastercard Business Revolving.
4. The Credit Cardholder/the person whose name is on the card is obliged to provide a sufficient cover on the date when liabilities fall due in the RSD current account or Card Repayment Account.
5. The main Cardholder is liable for usage his/her own and additional cards in accordance with these SC for Credit Cards.
6. The Cardholder is liable for the accuracy of all information provided to the Bank and obliged to notify any change in the information from the Application in written form to the Bank.

III. INTEREST, FEES AND COSTS

1. The Bank shall agree, calculate and charge the interest on credit cards in accordance with the Contract and these SC for Credit Cards.
2. The interest rate may be stated on annual, monthly or daily basis. The calculation of the nominal interest is done by applying the straight-line method. When calculating the interest, the Bank applies the actual number of days in the month against a 360-day year. The nominal interest rate applied by the Bank may be fixed or variable and for each type of credit cards is described in details in the Contract on Issuance and Usage of Credit Card.

3. The fees and costs charged by the Bank may be fixed or variable. The amount of costs and fees, the method and dates of payment are stipulated in the Fee Tariffs and Contract on Issuance and Usage of Credit Card.

IV. CREDIT CARD ISSUANCE

1. The Bank shall issue a credit card on a basis of a prior Credit Card Issuance Application filed in written form by the Cardholder (hereinafter referred to as: the Application) and the concluded Contract on Issuance and Usage of Credit Card.
2. When Client applying for Credit card, the Bank will open Transaction account (Card repayment) in RSD, which is the account for cover liabilities proceeds by using of credit card and this is the only purpose of that account.
3. The Bank shall replace credit cards without a signed request from the User only in cases of card malfunction, product migration to new technological solutions, product discontinuation, when the previous card has been deactivated for security reasons due to misuse or suspected misuse, as well as in cases of enhancing the protection level of the product or the User.
4.
5. The person whose name is on the card shall be delivered the card and personal identification number (hereinafter referred to as: the PIN), i.e. the person authorised by the Credit Cardholder to take over the credit card. The card can be used upon its activation in one of the described way:
   - upon collection at a Bank branch;
   - If the card is sent to the company's address (provided this option is offered by the Bank), the identification of the cardholder and activation will be carried out after the User (or authorized person) submits confirmation of receipt of the card and PIN code

at the specified address. Once the documentation is verified, the Bank will activate the card and notify the User via the email address registered in the Bank's system.

6. The person named on the card is obliged to sign the card upon receipt. A card that is not signed shall not be valid and financial consequences, which may arise as a consequence of the fact that the plastic is not signed, in the event of fraud involving an unsigned card shall be borne by the Cardholder. The person named on the card is obliged to keep the assigned PIN confidential, and to take all reasonable and appropriate measures for the protection thereof, in order to protect the card from fraud, in particular in view of the prohibition to accept third party assistance in entering the PIN at an ATM or POS. In addition, it is most important that the PIN is not written on the card or any other document carried with the card. The cardholder has the possibility to change the PIN within the Bank's ATM network in the territory of the Republic of Serbia. If the Cardholder determines this possibility and makes a change of the PIN code, which is handed over to him by the Bank, he is obliged to establish the newly defined PIN in a way that it meets the minimum-security standards in terms of the adequacy of the numeric code. In such situations, where the User changes the PIN code initially, he also assumes responsibility for all possible financial consequences that may occur if he improves the PIN code by third parties by inadequate selection of the numerical combination and in this way enables abuse of the debit card. The Cardholder shall incur all financial consequences of debit card fraud in the event of undue debit card safeguarding or using by the person named on the card.
7. When producing the credit card, the validity term shall be determined as embossed on the face of the card in the format MM/YY. The card shall expire on the last day of the month embossed on the card at 24:00 h.
8. If the Cardholder fails to cancel the card no later than 60 days prior to expiry and uses it in accordance with these SC for Credit Cards, the plastic is automatically produced with a new validity term. If the Cardholder fails to meet the conditions in accordance with the applicable laws and the Bank's internal rules, the card will not be automatically renewed and/or delivered.

V. CREDIT CARD USAGE

1. Mastercard credit card may be used to make a payments at points of sale, pay via the Internet, and Cash withdrawal within the acceptance network where its logo, Mastercard, is displayed.
2. An expired credit card may not be used any longer.
3. The Cardholder/person whose name is on the card is not entitled to post the credit card as pledge or collateral for payments.
4. If the Cardholder/person whose name is on the card is deprived by the Bank of the right to use the credit card, he/she is obliged, as requested by a seller of goods and/or services (Acceptor) or paying bank, to surrender his/her credit card.
5. The person whose name is on the card is obliged, when paying for goods and/or services at an acceptor's point equipped with a POS terminal, to enter his/her PIN personally with all possible discretion, if requested to do so by the Acceptor. The person whose name is on the card shall not disclose his/her PIN to the Acceptor or any other person.
6. When using the card at POS terminals that support contactless technology, the User may choose to complete the transaction via contactless payment or request the merchant to process the transaction using the standard method, which involves authorization by entering the PIN code. If the User opts for contactless payment, transactions are carried out by tapping the card on the POS terminal. In certain cases, additional authentication by entering the PIN code may be requiredThe
7. For a transaction made, the point of sale shall issue a copy of the slip/receipt and the person whose name is on the card is obliged to sign the copy of the slip/receipt for the Acceptor, in the same way, as he/she has signed the credit card.
8. In addition credit card (based on payment and cash withdrawals) can be debited, but credit card can also be initiated a credit transaction approval, which imply the inflow of the funds on the account linked to the credit card. Posting the authorization transaction does not settle the due obligation of the Cardholder, but rather increases the available credit card balance.
9. By his/her signature, the person whose name is on the card shall guarantee that the amount is correct and that he/she will reconcile it in accordance with the SC for Credit Cards. A copy of the slip (receipt) shall be retained by the person whose name is on the card in the case of complaint. The use of PIN shall be deemed to constitute the signature of the Cardholder/ person named on the card.
10. The person whose name is on the card may withdraw cash at the bank or post office tellers, as well as at ATMs by entering his/her PIN. The person whose name is on the card may change the PIN within the Bank's ATM network in the territory of the Republic of Serbia. Order to increase security, the Bank shall define a daily, weekly or other limit (in respect of the amount and number of transactions) for withdrawing cash or payments for goods and services from the card account according to the related Fee Tariff. The Cardholder may request a change of limit and/or number of transactions by signing the Application or by sending it via e-banking. The User acknowledges that any increase in the limit at their request increases the potential financial damage in the event of card misuse, for which the User is solely responsible beyond the daily limits defined in the Fee Schedule. The Bank reserves the right to decline the requested limit increase if it assesses that there is an elevated risk of misuse or potential material damage resulting from such misuse. The Bank shall independently adopt a Decision on Changing the Set Limit and shall be under no obligation to explain its Decision.
11. The person whose name is on the card may check the card balance, i.e. available funds by ATM enquiry, accordance with the related Fee Tariff.
12. ATM and POS electronic records shall constitute proof of a transaction made.
13. The credit cards of UniCredit Bank may not be used for transactions on foreign websites registered for gambling.
14. The Bank shall reserve the right to limit credit card usage (blockade) in accordance with the General Conditions for providing payment services to companies, as well as in the following instances:
    i. if there are justifiable reasons pertaining to credit card security
    ii. if there is suspicion of unauthorised credit card usage or its usage for the

purpose of fraud. In the case of suspicious transactions, the Bank shall block the card until the person whose name is on the card confirms the transaction authentication as his/her own, by calling the phone number which is located on the back of the card.

iii. In the case when a card is used for making transactions at POSs, Internet merchants or ATMs, with prior compromising activities recorded (skimmer set-up, data abuse, etc.), the Bank shall permanently block the card, adopt a decision reissuing the card in the case of which the Cardholder/person named on the card shall automatically receive the reissued the card, free of charge.

iv. following three consecutive unsuccessful PIN entries, the User may unblock the credit card by contacting the Bank's Contact Center

14. Depending on the circumstances above, the Bank may temporarily or permanently block the card.

15. The Bank is obliged to notify the person whose name is on the card about the intention to block the credit card and the reasons for doing so by email or phone, or by sending a text message to the phone number provided by the person whose name is on the card to the Bank as the contact-number, and if incapable of notifying him/her thereof prior blockade of the credit card, the Bank will do it immediately afterwards. Cardholders of SMS Card Alarm service shall be automatically send a text message in respect of the card blocking.

16. The Bank shall not notify the person whose named on the card about the (intended) blockade of the credit card if such notice is prohibited by law, or if there are justifiable security reasons therefor.

17. The Bank will make a credit card available for re-use or it will replace it with a new one once the reasons for the blockade thereof have ceased.

18. In order to protect the Cardholder in case of online payments, the Bank will perform additional validation of the Cardholder's identity for online payments in 3D Secure environment..

- Credit cards from Mastercard program provide payment on the Internet in a 3D Secure environment with one-time password, which is sent to the Cardholder via SMS, or through e-banking and m-banking using biometrics. The precondition for one-time password sending is an active SMS card alarm service. Cardholders registered for SMS Card Alarm, a one-time password will be delivered to the phone number that the Cardholder reported to the Bank for that service. The cardholder is responsible for updating the contact information in terms of the mobile phone number that the was reported to the Bank for the use of the SMS Card Alarm service and is aware of the fact that this service is necessary if Cardholders plans to pay with credit card on the Internet on sites that support the 3D Secure environment.
- If the customer does not receive a one-time SMS message when paying online on sites that supports 3D secure environment, it is necessary to contact the Bank in order to check and update the mobile phone number.
- The Bank can approve payment by card on online sites without additional verification of the Cardholder's identity through a one-time password in case of assessment that the transaction in question is of low risk (the Cardholder pays at a point of sale that he often uses, through a device that he often uses, etc.), or in situations where the Online point of sale does not require authentication of the Cardholder.
- The cardholder is responsible for keeping the password and performing all activities by using the received password. The cardholder is not allowed to transfer or allow access to the same to a third party. In case of lost or stolen card, any unauthorized use of a password or other data for verification, or in case of any other security breach, the cardholder is obliged to notify the Bank immediately. The Bank shall not be liable for any loss or damage arising from the Cardholder's failure to comply with the terms and conditions for the provision of this service.
- In a case of using the card for transactions where the card is not physically present, the Cardholder is obliged to take basic precautions:
  - i. to use only trusted online stores
  - ii. to never send sensitive payment data via e-mail, SMS, or phone
  - iii. to check whether the name of the point of sale specified in the SMS message corresponds to the point of sale where the User initiates the transaction, before giving consent for the execution of the transaction
  - iv. to initiate payments with merchants who have provided a secure environment to ensure user authentication. Authentication is performed by entering security elements – an OTP code and a static password assigned to the User by the Bank upon card issuance, which is known exclusively to the User. The OTP code is sent to the phone number registered with the Bank, and the User is solely responsible for the accuracy of this information. The User is responsible for safeguarding the OTP code and for all activities carried out using the received OTP code. The cardholder is not permitted to transfer or allow access to the OTP code to any third party. In the event of a lost or stolen card, any unauthorized use of the OTP code or other verification data, or any other breach of security, the User is obliged to immediately notify the Bank. The Bank shall not be held liable for any loss or damage resulting from the User's failure to properly safeguard the data as described above.

VI. CONSENT (AUTHORISATION) FOR THE EXECUTION OF PAYMENT TRANSACTION AND CARDHOLDER'S PAYMENT OBLIGATION

13. Cardholder gives his consent for the execution of the payment transaction before the execution of the payment transaction, and in one of the following ways:

i. By using the card at the POS terminal by reading the chip or by contactless reading the chip and entering the PIN code in case the same is required for authentication, or by signing the slip when reading the magnetic strip if a signature is required for authorization

ii. By contactless reading of the chip from the card without entering the PIN code in accordance with the limits for contactless payments defined by card associations
iii. By tapping a mobile device with an installed digital wallet on a POS terminal or ATM that supports contactless transactions
iv. By entering the PIN code when initiating a payment transaction at the ATM (by inserting the card into the reader or by contactless reading)
v. By entering the security elements required by the Acceptor when initiating a payment transaction at online points of sale (card number, CVV2 ode and/or one-time password (OTP) or OTP and static password))
vi. By using the card within the digital wallet in the manner described in these Terms of Business with debit cards

1. The card user can give consent for the execution of a payment transaction both through the payee and through the provider of the payment initiation service.
2. After giving consent for the execution of a payment transaction, the consent cannot be revoked except in the case of an agreement between the Card User and/or the Bank and/or the Acceptance Point.
3. The time of receipt of the payment order means the moment when the Bank received the electronic data on the payment transaction from the Bank of the payee. Within one day from the date of the interbank settlement, the transactions arrive at the Bank for processing and are recorded with the currency date when the settlement between the banks was completed. Upon receiving the debit order from the payee's payment service provider, the Bank will book the transaction, i.e. debit the account/accounts linked to the payment card and cancel the reservationThe settlement value of the Bank for debit/credit transactions for international transactions is EUR, i.e. RSD for national transactions. All the debit/credit transactions that the person named on the card makes abroad, by using an internationally valid payment card outside the Eurozone, shall be subject to conversion from the local currency into the EUR at the exchange rate applied by the Mastercard Association. The Bank performs the conversion on the day of posting the debit transaction at the Bank's selling rate, that is, at the Bank's buying rate on the day of processing for authorization transactions. Transactions originating outside the Eurozone are subject to conversion from the local currency to EUR according to the exchange rate applied by the card schemes.
4. In cases where to the Cardloder is given the option of selecting the debit/authorization currency during the execution of the transaction, and in which the Cardholder decides for conversion of transaction and to perform payment in RSD currency, the debit/authorization transaction on the Cardholder's account will be performed in the selected RSD currency, whereby the Bank has no insight into the conversion rate and the fees applied by the receiving place registered abroad. The information that is presented to the Cardholder on the screen of the device or on the slip is not binding for the Bank as the issuer of the card.
5. All credit card liabilities for transactions made locally or internationally shall be accounted in RSD only, at the Bank’s offer rate on the day of processing the transaction.
6. The time of receipt of the payment order means the moment when the Bank received the electronic data on the payment transaction from the Bank of the payee. Within a period of one day from the date of the interbank clearing, transaction arrive at the bank for the processing and are credited with the value date when the settlement between the banks is done.
7. If, even 60 days following the transaction, by using a credit card, a change has not been registered in the card account, i.e. a change has not been registered in the Statement of Liabilities Due for the credit card, the Cardholder is obliged, without delay, to notify the Bank thereof. If the Cardholder fails to act in accordance with the foregoing it shall be deemed that he/she misused the credit card. The Bank is obliged to ensure reimbursement of an amount or proper completion of a payment transaction to the Cardholder if the Cardholder notifies it of an unapproved, incomplete or improperly completed transaction, i.e. if he/she requests its proper completion promptly upon learning of such transaction, provided that the Cardholder furnishes such notification, i.e. request to the Bank within 13 months of the debit date.
8. The Cardholder agrees and authorises the Bank to collect the outstanding liabilities arising from credit cards business, from any other accounts held by the Cardholder at the Bank.
9. The Bank shall not be liable for any damage caused by circumstances beyond its control (blackouts, ATM breakdowns, omissions and/or failures to act by other banks, payment institutions or merchants, etc.).
10. The Cardholder is conversant with and accepts that the usage of a credit card for electronic payment (online, catalogue and telemarketing, etc.) bears a fraud risk, arising from transmitting the card number and personal information through a public network and in relation therewith all financial consequences occurring due to fraud shall be incurred by the Cardholder.
11. The Cardholder/person named on the card is obliged prior to completion of a transaction online to check, whether the merchant through which he/she is performing the online transaction, has been registered its POS locally or internationally, and accordingly check if the transaction at hand will be delivered to the Bank as a local or international transaction. The Bank shall not incur any costs, foreign exchange differentials or be liable for any transactions made online, at POS terminals located outside Serbia, for which the Cardholder/person named on the card has failed to obtain all the required information prior performing a transaction, resulting in a mismatch between the amount displayed while performing the transaction and the booked amount thereof.
12. The
13. When initiating a payment transaction with a payment card, the Bank authorizes the transaction and for authorized transactions conducts simultaneous reservation of funds in the account/accounts linked to the payment card, in accordance with the rules defined by these Special Conditions.
14. Bank system will release the reservation, after the expiration of deadline set by the international standards for Card operations as the deadline for delivery of debits on performed transactions by payment service providers of the payee or merchants. The stated deadlines depend on the place where the transaction was concluded, so for ATM transactions it is 5 working days, for POS terminal it is 7 working days, but

they can also depend on the type of merchant, so in the case of Rent a car Agency, it is 30 days. Authorization has been systematically released after a predefined deadline, and cardholder is obliged to monitor debit of his/her account and to provide sufficient funds in order to enable settlement of the card payment transaction, in case that the reservation is released without prior charge for the specific payment transaction. If cardholder recognizes that reservation has been released without debit the account due to the transaction made or the debit was posted without releasing the reserved funds, it is necessary to contact Bank immediately in order that bank execute necessary checks and availability of funds at cardholder account and aligned it with actual status. When performing payment transactions by card, cardholder should also bear in mind that, the date of debit of account may differ from the date when the payment transaction was concluded.

VII. REPAYMENT MODELS AND ORDER OF CLOSING THE OBLIGATIONS

1. The Credit Cardholder is obliged to regularly settle his/her liabilities towards the Bank, respectively on a monthly basis, unless otherwise is stipulated in the Contract.
2. The Bank shall deliver to the Credit Cardholder once per month the Statement of New Liabilities notifying the Cardholder of all the transactions and fees arising by using the basic and/or additional card locally or internationally for the preceding month, in the current debit amount for the accounting period, minimum payment amount, and the due date of the monthly liabilities.
3. In the case when Cardholder does not receive the excerpt of the card until the 15th day in a month, and in the previous month he/she has been using the card or has the assets for usage from the previous period, he/she is obliged to immediately inform the Bank.
4. Credit card repayment models:
   i. Revolving model for Companies:
      - "Minimum payment amount" – the required portion of payment. If the Cardholder in his/her card repayment account provides the minimum payment amount, i.e. an amount higher than the minimum payment amount, but less than the current debit for the period, the outstanding amount of debt is subject to the agreed interest as of the day of processing the transaction until the day of making the payment, including the interest on the outstanding amount of debt until the last day of the accounting period. Each day of delay in payment of due liabilities shall be subject to the default interest
      - "Current Debit" - if the "Current Debit" amount is settled by the due date as indicated in the statement, the interest shall not be accounted.

   ii. Charge model for companies:
      - "Current Debit" on the card is equal to the total debt in the accounting period which falls due in the full amount. Each day of delay in payment of due liabilities shall be subject to the agreed penalty interest.
5. The Credit Cardholder, at the time of signing the Contract on Issuance and Usage of Credit Cards, shall opt for a type of delivery of the monthly Statement, by mail or e-mail at the address stated in the Application. If the Cardholder opts for mail delivery at the address, then the Bank charges a print-out fee for the Statement as determined in the current Fee Tariffs. The Credit Cardholder may at any time prepay the debt on the credit card, free of charge.

VIII. TERMS OF USE OF A DIGITISED PAYMENT CARD

1. To register a debit card in the Digital Wallet, it is necessary for the Cardholder to have a valid mobile phone number registered with the Bank, to use a Mobile Device with NFC technology and an appropriate operating system according to the requirements of the Digital Wallet service provider, as well as to set the lock on the Mobile Device used.
2. The cardholder can register his debit card in the Digital Wallet through the Digital Wallet or through the Bank's mobile banking application, if the Bank allows it. By registering a debit card in the Digital Wallet, a Digitized Card is created for which all the conditions apply to a debit card whose Digitized Card is a digital representation, and in accordance with these Special Terms and Conditions. The cardholder can register more than one card in the Digital Wallet, whereby the first one registered becomes the default card for payments. The cardholder can set the default card in the Digital Wallet.
3. A Digitized card transaction is initiated by bringing the Mobile Device to the POS terminal or ATM, i.e. by selecting the Digital Wallet payment option at the online point of sale and confirming the transaction itself on the Digital Wallet. The Bank will debit the Cardholder's payment account to which the registered debit card is linked for the amount of the payment transaction thus executed.
4. If, for any reason, the Bank replaces the debit card registered by the Cardholder in the Digital Wallet with a new debit card (for example, if it is reported as lost, stolen, replaced with a new one after the expiration date), re-registration of the Digitized Card through the Digital Wallet is not required. If for any reason the Cardholder abandons the use of the debit card or the Bank denies the Cardholder the right to use the debit card, the right to use the Digitized Card also ceases at the same time. The blocking of the debit card results in the blocking of the Digitized card, while the blocking of the Digitized card does not imply the blocking of the debit card.
5. The Cardholder can delete the Digitized Card from the Digital Wallet at any time, which does not affect the ability to use his debit card, nor the Digitized Cards on other Mobile Devices on which he digitized the same card.
6. In the case of a change of Mobile Device, it is necessary for the Cardholder to delete the Digitized Cards from the Digital Wallet on that device, in order to prevent their further use, and if he wants to continue using the Digital Wallet on a new Mobile Device, he needs to repeat the card registration process.

7. By registering a debit card in the Digital Wallet on a certain Mobile Device, the Cardholder assumes the obligation to handle the Mobile Device with due care, and to take all reasonable measures to protect it from unauthorized use, loss and theft, as well as to notify the Bank without delay of loss, theft, unauthorized access or use of the Mobile Device, in which case the Bank blocks the Digitized Cards on that device.
8. The Bank is not responsible for the functioning of the Digital Wallet in situations caused by technical defects or settings of the Mobile Device itself and the Digital Wallet over which the Bank has no control.

IX. CARDHOLDER'S RIGHT TO CHECK TRANSACTIONS AND COMPLAINT

1. User has the right to submit a complaint, including a dispute regarding a payment transaction, within six (6) months from the date they became aware of the violation of their rights. In any case, the right to submit a complaint expires three (3) years from the date the violation occurred. Regardless of whether the complaint concerns a primary or supplementary debit card, the service User, i.e., the account holder, must be the one submitting the complaint to the Bank, except in cases specifically described in Section 6 of this chapter. If the primary cardholder submits a complaint after the expiration of the prescribed period, the Bank will inform them that the complaint was submitted after the deadline and that it is not obliged to consider it.

2. If the User submits a dispute regarding a payment transaction executed with a payment card, they must do so in the form of a Transaction Verification Request (hereinafter: the Request). The Request informs the Bank of an unauthorized, unexecuted, or improperly executed payment transaction and requests proper execution of the transaction. The Request may be submitted to the Bank no later than thirteen (13) months from the date the transaction occurred on the debit card. The User must also submit the Request in cases where a payment initiation service provider was involved in the execution of the transaction.

3. Any complaints regarding the quality of goods and/or services paid by a credit card shall be addressed by the Cardholder/person named on the card only to the seller of the goods and/or services - Acceptor. If a merchant refunds the assets to the Cardholder, on the basis of founded complaint regarding the quality of goods and/or services or for other reasons, the Bank shall not incur the costs of foreign exchange differentials, if any, if the initial transaction was made in a foreign currency and/or booked by debiting the Cardholder's account in a currency other than the refund currency.

4. The Cardholder may submit a complaint in one of the following ways:
i. In the business premises of the Bank using the Contact form which is available at all branches of the Bank,
ii. By submitting a complaint by post to the following address:
UniCredit Bank Serbia JSC.
Customer experience and complaint management
Rajićeva 27-29
11000 Belgrade
iii. By e-mail at: josbolje@unicreditgroup.rs
iv. Through the Bank's website
v. By using digital channels (e.g. electronic banking) if the client uses these services, it is possible to submit a complaint based on a specific contractual relationship.

5. A complaint must contain information about the complainant based on which it will be possible to identify the complainant i.e. determine the business relationship with the Bank to which the complaint relates, as well as reasons for submission of complaint. If the complaint constitutes a Request for Verification, it must include details of the transaction for which the user's account was charged and which the user disputes as unauthorized or improperly executed, as well as the circumstances under which the transaction was carried out, to the extent known to the user. Based on such a submitted Request for Verification, the Bank will determine whether there is a basis for initiating a dispute resolution process through the card association, with the aim of obtaining additional information and data related to the transaction, or securing a refund of the transaction amount from the merchant, provided that the conditions for such a process are met in accordance with the rules governing this type of dispute resolution.

6. When a complaint is submitted through an authorized representative, a specific power of attorney must also be provided, authorizing the representative to submit the complaint to the Bank on behalf of the User/legal representative of the User and to undertake actions in the complaint procedure. The power of attorney must also include the User's consent for the representative to access information considered banking secrecy under the law governing banks, or business secrecy under the law governing payment services.

7. For written complaints submitted to the Bank in electronic form, via the Bank's website, or through electronic or mobile banking applications, the Bank will confirm receipt of the complaint via email or through the respective application on the same business day the complaint is received. Complaints received outside the Bank's established business hours will be considered received on that day, and the complainant will be informed of this in the confirmation of receipt.

8. The Bank shall provide the complainant with a clear and comprehensible written response to the complaint no later than 15 days from the date of receipt. If, due to circumstances beyond the Bank's control, it is unable to respond within the specified timeframe, the deadline may be extended by a maximum of 15 additional days. In such cases, the Bank shall inform the complainant in writing within 15 days from the date of receipt of the complaint. This notification shall clearly and understandably state the reasons for the delay and indicate the final deadline by which the response will be provided.

9. The complaint resolution procedure is free of charge.

10. Exceptionally, in cases where the Bank compensates the User prior to the conclusion of the previously initiated dispute resolution process defined in Item 5 of this section, the Bank reserves the right to request reimbursement of the compensation amount from the User if, through subsequent checks and obtained information, it is determined that the disputed transaction was authorized by the User, or that it does not constitute an unauthorized payment transaction. The Bank

shall first notify the User in writing, providing the evidence confirming the authorization of the transaction.

11. If the User is not satisfied with the response to the complaint, or if the response is not provided within the prescribed 15-day period, the User may submit a grievance to the National Bank of Serbia within 6 months from the date of receipt of the response. The grievance may be submitted by mail to the following address: National Bank of Serbia, Nemanjina 17, 11000 Belgrade, or via the website: https://www.nbs.rs/sr_RS/formulari/prituzba/.
12. The dispute between the Cardholder and the Bank may also be resolved through an out-of-court procedure – mediation before the National Bank of Serbia, initiated at the proposal of one party to the dispute and accepted by the other party. The mediation procedure is conducted by the National Bank of Serbia and is free of charge for both parties. A proposal for mediation may be submitted to the National Bank of Serbia in written form, by mail or via the internet presentation: https://nbs.rs/sr/ciljevi-i-funkcije/zastitakorisnika/medijacija/index.html
The proposal submitted by the Cardholder must include a deadline for acceptance, which cannot be shorter than 5 days or longer than 15 days from the date of submission.

X. STOLEN OR LOST CARD LIABILITY OF THE BANK AND THE USER FOR THE EXECUTION OF A PAYMENT TRANSACTION

1. The Cardholder/person on whose name is the card, is obliged, without delay upon finding out about the credit card loss or theft, to report it to the Bank and request that the Bank block its further use.
2. The Cardholder/person named on the card shall report the card loss/theft to the Bank by telephone to the Customer Service on +381 11 3777 888, therefore, it is advised that the Cardholder always keeps the number of the Bank's Contact Center with him. Following the report of the card lost/stolen, the Cardholder shall confirm such report by filling in the appropriate form in the nearest Bank branch.
3. If the case if lost or stolen credit card is returned to the Cardholder/person named on the card or the Cardholder/person named on the card finds it, he/she must notify the Bank.
4. If the credit card is destroyed/damaged, the Cardholder/person named on the card is obliged to notify the Bank thereof in written form by filling in a relevant form at the Bank's branch where the card has been issued.
5. If the credit card is destroyed/damaged, the Cardholder will get a new PIN code with the new card.
6. In the case of unauthorised usage of the credit card or the credit card information – the cardholder is obliged, upon learning thereof, but no later than 13 months of the debit date, to report to the Bank the transaction made by unauthorised usage of the credit card, i.e. the credit card information.
7. The Cardholder shall incur all losses in relation to any transaction made by fraud committed by the persons named on the cards, and bears the losses arisen due to non-performance of his/her obligation to report to the Bank the credit card loss, theft or fraud, his/her obligation to properly safeguard the card and the PIN code, as well as other obligations arising from these SC for Credit Cards.
8. The cardholder shall not incur any losses arisen from transactions made after reporting to the Bank the loss, theft or unauthorised use of the credit card, i.e. credit card information, unless the persons named on the cards committed or participated in fraud or acted with an intention to defraud.
9. If the Bank is responsible for an unapproved payment transaction, it is obliged, at the Card User's request, to refund the amount of that transaction to the Cardholder without delay, i.e. to return the card account to the state in which it would have been if the unapproved payment transaction had not been carried out, as well as to perform refund of all fees charged to the Cardholder, except in case of suspicion of fraud or abuse on the part of the Cardholder, in which case within 10 days from the day of learning about the unauthorized payment transaction, justify the refusal of the refund and report the fraud/abuse to the competent authority or make a refund to the User, if he concludes that he did not commit fraud or abuse.
10. The Bank shall not be held liable for any damage incurred by the User resulting from an unexecuted or improperly executed payment order, where the User is responsible in accordance with these Terms of Use for debit card operations, and where it is proven that the payment service provider of the payee received the amount of the payment transaction in accordance with the User's order. The Bank shall also not be liable in cases caused by force majeure, such as war, natural or ecological disasters, epidemics, power outages, and interruptions in telecommunications, as well as other similar causes not resulting from the Bank's actions. Furthermore, the Bank shall not be liable where it was required to comply with other regulations, or in the event of unforeseen circumstances beyond its control, the consequences of which could not have been avoided despite exercising due diligence.
11. Gross negligence shall be deemed to include, but not be limited to: writing down the PIN on the card or in a manner that makes it accessible to third parties; keeping the card and PIN together; sharing a one-time password with a third party for any purpose other than confirming an online payment; sharing an activation code (for activating a digital wallet) with a third party; using an unsigned card; leaving the card in a parked vehicle or another location accessible to third parties; losing sight of the card at a point of sale; accepting assistance from a third party when entering the PIN at an ATM or merchant's point of sale; and other similar actions by the User that enable misuse of the card or card data, unauthorized use, or execution of an unauthorized payment transaction.

XI. CARD CANCELLATION

1. As requested by the Cardholder in written form, the Bank is obliged to cancel the credit card.
2. If the Cardholder fails to perform the obligations provided under the Contract and these SC for Credit Cards, i.e. discontinues fulfilling the required conditions for credit card approval, the Bank may deprive the right to use the card to such Cardholder.

3. The Bank shall reserve the right for produced card, which the Cardholder fails to take over within 6 months of production, to terminate without any explicit written request by the Cardholder.
4. All transactions made by the card return date, including all related costs, shall be incurred by the Cardholder.

XII. FINAL PROVISIONS

1. By signing the Contract, the Cardholder agrees and authorises the Bank to charge its RSD current account or foreign currency account for all transactions and fees arising from usage of the card and in accordance with the relevant Fee Tariffs.
2. By signing the Contract, the Cardholder acknowledges that he/she is familiar with and concordant to all the provisions of the SC for Credit Cards and the relevant Fee Tariffs.
3. The Bank shall reserve the right to amend these SC for Credit Cards, upon giving a prior notice to the Cardholder.
4. Anything not provided by these SC for Credit Cards, shall be governed by the Bank's General Conditions for providing payment services to companies, General Business Conditions for Companies – General part.
5. In case of any dispute, Court in accordance with the law will be competent.
6. These SC for Credit Cards have been drafted in accordance with the Payment Services Act and the regulations of the Republic of Serbia and are available on the Bank's webpage www.unicreditbank.rs , as well as at all Bank's branches.
7. These SC for Credit Cards have been drafted in Serbian and English. In the case of any inconsistencies between the Serbian and English versions, the Serbian version will prevail.
8. The provisions of these SC for Credit Cards shall come into force on the date of their adoption by the Bank's Supervisory Board and shall apply as of 01 st of January 2026.

Supervisory Board of UniCredit Bank Serbia JSC Belgrade