

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

Belgrade, 20th October 2025

TABLE OF CONTENTS**INTRODUCTORY PROVISIONS**

I.	MEANING OF CERTAIN TERMS	3
II.	GENERAL CONDITIONS.....	3
III.	DEBIT CARD ISSUANCE.....	4
IV.	CARD USAGE.....	4
V.	TERMS OF USE OF A DIFITISED PAYMENT CARD.....	6
VI.	AUTHORISATION AND POSTING OF TRANSACTION	7
VII.	CARDHOLDER'S RIGHT TO CHECK TRANSACTIONS AND COMPLAINT	8
VIII.	DAMAGED, STOLEN OR LOST CARD	9
IX.	CARD CANCELLATION	10
X.	FINAL PROVISIONS.....	10

Recital:

UniCredit Bank Serbia JSC, Belgrade, as the debit service provider (hereinafter referred to as: the Bank) by way of these Special Conditions for Debit cards to Companies (hereinafter referred to as: the SC for Debit cards) shall govern mutual rights and obligations of the Bank and the Cardholders regarding the conditions for debit card issuance and use.

I. MEANING OF CERTAIN TERMS

Cardholder - Refers to the legal entity that is the holder of the primary and additional card, as defined in these Special Terms and Conditions.

Card Issuance Application - means the Bank form filled out by potential user for the issuance of a debit card.

Debit Card - in terms of these SC for Debit cards is debit card in physical and digital form, which represents a debit instrument, which allows the Cardholder to pay for goods or services either through/ debit/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 in the name of 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 – Personal Identification Number, a numeric code known only to the Cardholder, which serves as a means of authenticating the Cardholder or the transaction initiated by the Cardholder and/or authorizing 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.

Payee - 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 code change, etc.

POS (Point of Sale) terminal - is an electronic or mobile device authorising transactions and electronic acceptance of debit cards at an acceptor's points of sale.

Digital wallet - is a mobile payment application solution of a digital wallet service provider, which allows the User 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 user 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 In a digital wallet and/or the Bank's electronic and mobile banking applications, enabling 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 about which debit cards can be digitized.

Mobile Device – refers to a device on which a 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.

CVV2code - means a three-digit number on the back of the card used for the card verification in online payments.

3D Secure environment - an environment for making payments at online merchants that require additional authentication of the Cardholder at the moment of giving consent for the execution of a payment transaction initiated with payment cards from the relevant card scheme.

OTP code – represents a security element in the form of a one-time numeric password delivered to the User when initiating a payment at 3D Secure online merchants, to the mobile phone number registered in the Bank.

Daily Limit - means a daily allowed amount of funds and number of transactions for withdrawing cash and paying for goods and services.

Daily limit – the maximum allowed daily amount of funds and number of transactions for cash withdrawals, cash deposits, and payments for goods and services.

Contactless payment – executed by tapping the payment instrument on devices (POS/ATM) where the merchant has enabled contactless payments. In certain situations, entering a PIN code may be required. When initiating contactless transactions at ATMs, PIN code entry is mandatory.

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 debit 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.
 2. The Bank issues debit cards to legal entities for which the processing, clearing, and settlement of domestic payment transfer orders are carried out within the payment system of the Republic of Serbia (DinaCard cards).
In addition to the card mentioned above, the Bank may, upon the User's specific request, issue another card from its offering, for which the processing, clearing, and settlement of domestic payment transactions are carried out outside the Republic of Serbia (internationally valid cards). DinaCard debit card can be used for the payment of goods and services/receipt of funds via POS terminals and the internet, as well as for cash withdrawals within the ATM network in the territory of the Republic of Serbia. Internationally valid cards can be used for the payment of goods and services/receipt of funds via POS terminals and the internet, as well as for cash withdrawals within the ATM network both in the Republic of Serbia and abroad.
-
3. The primary cardholder is required to ensure sufficient funds are available in the RSD and/or foreign currency (current) account linked to the international debit card

at the time of performing a transaction. In the case of domestic payment transactions initiated with a DinaCard, the cardholder must ensure that sufficient available funds are present in the RSD account to which the card is linked.

4. The Cardholder is liable for using all cards issued by the Bank in accordance with these SC for Debit cards.
5. 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 to the Bank in accordance with General Conditions for providing payment services to Companies.
6. Any consequences and costs arisen due to failure to report changes shall be incurred by the Cardholder.

III. CARD ISSUANCE

1. If the current account holder submits a Request for the issuance of a debit card that can be used to initiate payment transactions from the current account, the Bank is obligated to first issue to that User, free of charge, a debit card for which the processing, clearing, and settlement of domestic payment transfer orders initiated through its use are carried out within the payment system of the Republic of Serbia (hereinafter referred to as the DinaCard).
2. In accordance with the above, the issuance of a debit card for which the processing, clearing, and settlement of domestic payment transfer orders initiated through its use are carried out within the payment system of the Republic of Serbia. In accordance with the above mentioned, the issuance of a debit card where in the domestic debit transaction processing, clearing and settlement are performed in the Republic of Serbia is a prerequisite for applying for any other type of debit card that the Bank has in its offer.
3. The debit card issuance process shall involve the following: filing of the Application, production and serving of a debit card. The Bank delivers the card to the User in a branch or by delivering the card to the User's valid address in the Bank's system (if the specified option is available).
4. For SME clients The Bank issues the debit card on the basis of previously submitted Application for the issuance of the debit card by the Cardholder within Account package (hereinafter referred to as: Application), for corporate clients Bank issues the debit card on the basis of previously submitted Application.
5. After the card is produced, the Bank delivers/hands over the card and the PIN code (Personal Identification Number) to the User. The card can be used after activation, through one of the following methods, subject to prior identity verification of the User:
 - when collected at a Bank branch,

- upon the first transaction with correct PIN entry (e.g., cash withdrawal, balance inquiry at an ATM, or payment at a point of sale), in cases where a digital version of the card was previously issued,
 - when the card is sent to the company's address (if this option is offered by the Bank), the identification of the Cardholder and activation will be performed after the User (authorized person) submits confirmation of receipt of the card and PIN code at the company's address.
Upon verifying the documentation, the Bank will activate the card and notify the User via the email address registered in the Bank's system.
6. The Bank will replace debit cards without a signed request from the Cardholder only in the following cases: malfunction of the debit card, product migration to new technological solutions, product discontinuation, deactivation of the previous card due to security reasons (misuse or suspected misuse), or in cases of enhanced product or user protection—provided that a DinaCard debit card has already been issued to the User for the respective account.
 7. In the event that the physical debit card is damaged or destroyed, the User is required to notify the Bank by completing the appropriate form. When replacing a damaged card, a new PIN code will also be generated for the User.
 8. 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 code is not written on the card or any other document carried with the card. The cardholder has the possibility to change the PIN code 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 code 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.
 9. When producing the debit card, the validity 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.
 10. In the month in which the validity of a debit card expires—where the processing, clearing, and settlement of domestic payment transfer orders initiated through its

use are not carried out within the payment system of the Republic of Serbia—such a card may be reissued only upon the specific request of the payment service user, and only if a DinaCard debit card has already been issued to that user for initiating payment transactions from the same current account.

IV. CARD USAGE

1. The debit card can be used to make payments at points of sale, pay via the Internet, and Cash withdrawal within the acceptance network of the card association to which the card belongs (DinaCard, Mastercard, Visa). The debit card issued in physical form can be used for cash payments at certain Bank ATMs marked for that purpose.
2. An expired debit card may not be used any longer.
3. The Cardholder/person named on the card is not entitled to post the debit card as pledge or collateral for debits.
4. If the Cardholder/person named on the card is deprived by the Bank of the right to use the debit card, he/she is obliged, as requested by a seller of goods and/or services (Acceptor) or paying bank, to surrender his/her debit card.
5. The person named on the card is obliged, when paying for goods and/or services at an acceptor's point equipped with a POS terminal, if the card is based on CHIP technology personally enter his PIN with all possible discretion, or his signature if the card is based on magnetic stripe technology.
6. It is considered that the User, as a business entity having a business relationship with the Bank for providing payment services, authorized all the persons for which he requested the issuance of a debit card, to dispose with the funds from the account for which the particular card is linked, only by using a specific debit card, without the need for a special authorization. For concluded transaction, the merchant may issue a copy of the slip/receipt and asked the person named on the card to sign the copy of the slip/receipt for the Acceptor, as he/she has signed the debit card. By his/her signature, the person named on the card shall guarantee that the amount is correct and that the Cardholder will service it in accordance with the SC for Debit cards. A copy of the slip (receipt) shall be retained by the person named on the card for complaint purposes. The use of PIN shall be deemed to constitute the signature of the person named on the card.
7. In addition debit card (based on debit and cash withdrawals) can be debited, but debit card can also be initiated a credit transaction approval, which imply the inflow of the funds on the account linked to the debit card. Client can dispose with approved funds resulting from the usage of debits card, only after Bank receives them, ie. after the funds are posted on his account.
8. The person in whose name the card is issued may withdraw cash at bank counters, post offices, and ATMs using their PIN code. This person also has the option to change the PIN code within the Bank's ATM network in the territory of the Republic of Serbia. To enhance security, the Bank defines daily, weekly, or other

limits (in terms of transaction amounts and number of transactions) for cash withdrawals or payments for goods and services from the card account, in accordance with the applicable Fee Schedule for General Banking Services for Corporate Clients, Fee Schedule for General Banking Services for Small Enterprises, and the Fee Schedule for Debit and Credit Cards for Entrepreneurs. The User may request a change to the transaction limit or number of transactions by submitting a request at a Bank branch. The request may also be submitted via electronic banking or through the m-banking application, provided that such functionality has been previously enabled by the Bank. The User acknowledges that any increase in the limit, upon their request, increases the potential financial damage in the event of card misuse. The User is solely responsible for any such damage exceeding the daily limits defined in the Fee Schedule. The Bank independently decides on changes to the agreed limits and is not obligated to justify its decision. The Bank reserves the right to reject a requested limit increase if it assesses an increased risk of misuse or potential financial loss due to misuse.

9. When using the card at POS terminals that support contactless technology, the User has the option to choose between executing the transaction via contactless technology or requesting the merchant to process the transaction in the standard way using the debit card, which involves authorizing the transaction by entering the PIN code.

If the User opts for contactless payment when using the card at POS terminals that support contactless technology, the User has the option to choose between executing the transaction via contactless technology or requesting the merchant to process the transaction in the standard way using the debit card, which involves authorizing the transaction by entering the PIN code.

If the User opts for contactless payment, the transaction is executed by tapping the card on the POS terminal. In certain situations, additional authentication by entering the PIN code will be required.

10. The person named on the debit card may check the account balance, i.e. available funds in the card account by ATM enquiry, charged according to the related debit card Fee Tariff.
11. ATM and POS electronic records shall constitute proof of a transaction made.
12. The debit cards of UniCredit Bank may not be used for transactions on foreign websites registered for gambling.
13. The Bank shall reserve the right to limit debit card use (block it) in accordance with the General Conditions for providing payment services to companies, as well as in the following instances:
- if there are justifiable reasons pertaining to debit card security
 - if there is suspicion of unauthorised debit card use or its use for the purpose of fraud, or as a result of fraud. In the event of suspicious transactions, the Bank shall block the card until the person named on the card confirms the transaction authentication as his/her own, by calling the phone number on the back of the card.
 - In the event when a card is used for making transactions at POS and on

line 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 be automatically reissued the card, free of charge.

- iv. following three consecutive unsuccessful PIN entries.

14. Subject to the circumstances above, the Bank may temporarily or permanently block the card.
15. The Bank is obliged to notify the Client who will transfer information to all authorized persons for which he requested the issuance of a debit card, about intention to block the debit 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 named on the card to the Bank as the contact-number, and if incapable of notifying him/her thereof prior to blocking the debit card, the Bank will do it immediately afterwards. Users 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 Client of the (intended) blocking of the debit card if such notice is prohibited by law, or if there are justifiable security reasons therefor.
17. The Bank will make the debit card available for re-use or replace it with a new one once the reasons for the blocking 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 in 3D Secure environment
- Debit cards from Visa and 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. Users registered for SMS Card Alarm, a one-time password will be delivered to the phone number that the User reported to the Bank for that service. The user 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 online on sites without additional verification of the User'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 the situations where 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 cases where the card is used for transactions in which the card is not physically present,

The User is obligated to take basic precautionary measures:

- i. to use only trusted online merchants,
- ii. to never send sensitive payment information via email, SMS, or phone,
- iii. to verify that the merchant name shown in the SMS notification matches the merchant where the User initiated the transaction,
- iv. to initiate payments only with merchants that provide a secure environment to ensure User authentication.

User authentication is performed by entering security elements – an OTP code and a static password assigned by the Bank when the card is issued, which is known only to the User. The OTP code is sent to the mobile phone number registered with the Bank, and the User is solely responsible for the accuracy of this information. The User is also responsible for safeguarding the OTP code and for all actions performed using the received OTP code. The Cardholder is not permitted to share or allow access to the OTP code with 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 security breach, the User is obligated to immediately notify the Bank. The Bank shall not be held liable for any loss or damage resulting from the User's failure to follow the above-described data protection measures.

V. CONSENT AUTHORISATION FOR EXECUTION AND POSTING OF PAYMENT TRANSACTIONS

The Cardholder gives consent for the execution of a payment transaction prior to its execution, in one of the following ways:

- I. By using the card at a POS terminal through chip reading or contactless chip reading and entering the PIN code, if required for authentication, or by signing the receipt when the magnetic stripe is read and a signature is required for authorization;
- II. By contactless chip reading without entering the PIN code, in accordance with contactless payment limits defined by card schemes;
- III. By tapping a mobile device with an installed Google Pay or Apple Pay digital wallet on a POS terminal or ATM that supports contactless transactions;
- IV. By entering the PIN code when initiating a payment transaction at an ATM (either by inserting the card into the reader or via contactless reading);
- V. By entering security elements required by the payee when initiating a payment transaction at online merchants (card number, CVV2 code, and/or entering OTP and PIN or OTP and static password);
- VI. By using the card within a digital wallet in the manner described in these Terms of Use for debit card services.

The Cardholder may also give consent for the execution of a payment transaction through the payee or through a Payment Initiation Service Provider.

Once consent for the execution of a payment transaction has been given, it cannot be revoked, except in cases of agreement between the Cardholder and/or the Bank and/or the Merchant.

The time of receipt of the payment order is considered the moment when the Bank receives the electronic data related to the payment transaction from the payee's bank.

Within one business day from the date of interbank settlement, the transactions are received by the Bank for processing and are posted with the value date corresponding to the date on which the interbank settlement was completed.

Upon receiving the debit order from the payee's payment service provider, the Bank will post the transaction, i.e., debit the account(s) linked to the payment card and cancel the corresponding reservation.

1. All authorizations resulting from the use of debit cards are processed in the local currency, i.e., Serbian dinars (RSD). Accordingly, the amount of reserved funds for debit/credit transactions in other currencies may differ from the original amount until the transaction is posted.
2. **Transaction concluded on devices (ATM/POS) registered in the country** – calculated currency is RSD. After the transaction is submitted to the Bank, the RSD current account is going to be debited / approved first. If the User has no RSD current account linked to the card, or there are insufficient funds on that account, other current accounts are going to be debited / approved in the order in which they are linked to the card. The conversion is going to be made by Bank's bid rate on the day of processing, if it is debit transaction, or by Bank's offer rate, if it is credit transaction.
3. **Transaction concluded on devices (ATM/POS) registered abroad** – calculated currency is EUR. Transaction concluded outside EUR zone are going to be converted to EUR currency, according to the exchange rate applied by Visa/Mastercard association. If the original currency of transaction made by Visa card is different from calculated currency, the original transaction amount will be increased by 2% during conversion. Once the transaction is submitted to the Bank for posting, the EUR current account is going to be debited / approved first. If the User does not have a EUR current account linked to the card or there are insufficient funds on that account, other current accounts are going to be debited / approved in the order in which they are linked to the card. The conversion is going to be made by the Bank's offer rate on the day of processing in case if it is debit transaction, or by the Bank's bid rate, in case if it is credit transaction. In cases where the Cardholder is given the option of selecting the debit/authorization currency during the transaction, and in which the User decides for payment in RSD currency, the debit/authorization transaction on the User'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. The information presented to the User on the screen of the device or on the slip is not binding for the Bank as the issuer of the card.

4. Exceptionally the preceding paragraph, for debit of goods and services on the merchant web sites that are tied in the Republic of Serbia and where they provide option of selecting the debt currency of the transaction, the Bank will debit Client in accordance with the information provided to the Bank by the point of sale, which depends on the business relationship of the User and the trader.
5. 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 Acceptor. Within one day from the date of interbank settlement, transaction came to the Bank for processing and they are posting with same value date when settlement between banks was done.
6. The debit Cardholder shall have access to his liabilities, i.e., all transactions and fees incurred by the use of main and/or additional card in the country and abroad for the previous month, by means of a Statement from the dinar and foreign currency account.
7. When initiating a payment transaction using a payment card, the Bank performs transaction authorization and, for authorized transactions, simultaneously reserves funds on the account(s) linked to the payment card, in accordance with the rules defined in these Terms of Use for debit card services. 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 reservation.
8. 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. If the transaction is booked after the reservation has been released, the card user is obliged to provide funds on the card account to cover the transaction in question. 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.

9. If, after the expiry of 60 days from the date of the transaction made by using the debit card, no change is recorded in the current account of the Cardholder, or the change is not recorded in the Statement, the Cardholder shall, without delay, notify the Bank.
10. The Bank shall ensure the refund of the amount or a correct execution of the debit transaction if the Cardholder has notified the Bank about the unauthorised, failed, or incorrect execution of the debit transaction and/or has requested the correct execution of the debit transaction, immediately after becoming aware of such debit transaction, provided that he has delivered such notification and/or request within 13 months after the debit date.
11. The Cardholder agrees and authorises the Bank to collect the outstanding liabilities incurred by operations with debit cards also from other accounts that the Cardholder has opened at the Bank, which do not have to be linked to the card.
12. The Bank shall not be liable for damage caused by circumstances that it cannot influence (power failure, failure of ATMs, omissions and/or inaction by other banks, debit institutions and retailers, etc.).
13. The Cardholder is aware and accepts that the use of debit cards for debit by electronic means (Internet, MO/TO (mail order and telephone order) transactions, etc.) carries the risk of abuse that exists when communicating the card number and other personal data through the public network and all financial consequences caused by such abuse shall be borne by the Cardholder.
14. Before the execution of a transaction on the Internet the Cardholder must become aware whether the merchant through which he makes an online transaction has registered POS in the country or abroad and based on such knowledge to become aware whether the underlying transaction will be delivered to the Bank as an international or domestic transaction. The Bank will not bear any expenses, exchange loses, nor have any liability for transactions executed on the Internet, on POS terminals that are located of outside Serbia, for which the Cardholder has not obtained all the necessary information before the execution of the transaction which caused disagreement of amounts presented to the Cardholder at the execution of the transaction and the posted transaction amount. The Cardholder shall authorise the Bank to charge the account for the "Card not present" type of transaction, failing to result in the standard receipt/slip. Also the cardholder shall authorise the Bank to debit his account for transactions executed with a debit card based on the authorization made in the so-called offline regime.

VI. TERMS OF USE OF A DIGITALISED PAYMENT CARD

1. To register a debit card in a Digital Wallet, the User must have a valid mobile phone number registered with the Bank, use a mobile device with NFC technology and an appropriate operating system as required by the Digital Wallet service provider, and enable screen lock on the mobile device.
In certain cases, the digital wallet service provider (e.g., Google Pay, Apple Pay)

may disable the use of a digitized card within its mobile wallet, over which the Bank has no control and no insight into the reasons for such action.

2. The user 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 user can register more than one card in the Digital Wallet, whereby the first one registered becomes the default card for payments. The user 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 User'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 User 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 User abandons the use of the debit card or the Bank denies the User 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 User 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 User 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 User 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.

VII. CARDHOLDER'S RIGHT TO CHECK TRANSACTIONS AND COMPLAINT

1. Cardholder 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 Cardholder 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 debit 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
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. It is necessary that the complaint contains data of the complainant, on the basis of which his identification can be carried out, that is, the determination of the business relationship that the complainant has with the Bank, to which the complaint refers, as well as the reasons for submitting it. 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 Cardholder and to undertake actions in the complaint procedure. The power of attorney must also include the Cardholder'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 Cardholder 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 Cardholder if, through subsequent checks and obtained information, it is determined that the disputed transaction was authorized by the Cardholder, or that it does not constitute an unauthorized payment transaction. The Bank shall first notify the Cardholder in writing, providing the evidence confirming the authorization of the transaction.
11. If the Cardholder is not satisfied with the response to the complaint, or if the response is not provided within the prescribed 15-day period, the Cardholder 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/prituza.
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.

VIII. DAMAGED, STOLEN OR LOST CARD

1. The Cardholder/person named on the card is obliged, without delay upon learning about the debit card lost or stolen, 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 lost/stolen by telephone to the Contact centre 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 or using e-banking and m-banking application.
3. When debit card that was blocked previously by the client (lost/stolen) need to be reissued, it is necessary to fulfill the preconditions that was set through this SC for Debit card in the sense that the DinaCard debit card has already been issued to the cardholder.
4. If the lost or stolen debit card is returned to the Cardholder/person named on the card or the Cardholder/person named on the card finds it, he/she undertakes to notify the Bank thereof. If the debit card is blocked based on the reported debit card lost or stolen, the Cardholder/person named of the card may not request that it be activated or used further.
5. If the debit card is destroyed/damaged, the Cardholder/person named on the card is obliged to notify the Bank thereof in writing by filling in a relevant form of the Bank. If the debit card is destroyed/damaged, the Cardholder will be issued a new PIN code with the new card.
6. In case of unauthorised use of the debit card or the debit 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 through unauthorised use of the debit card, i.e. the debit 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 the losses arisen due to non-performance of his/her obligation to report to the Bank the debit card lost, stolen or fraud, his/her obligation to properly safeguard the card and the PIN code, as well as other obligations arising from these SC for Debit cards, which determine the rights and obligations of the User arising from the concrete business relationship with the Bank, as well as the conditions under which the debit card is issued to the User, or

the rules of its use

8. The Cardholder shall not incur any losses arisen from transactions made after reporting to the Bank the lost, stolen or unauthorised use of the debit card, i.e. debit 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.

IX. CARD CANCELLATION

1. As requested by the Cardholder in writing, the Bank is obliged to cancel the debit card.
2. If the Cardholder fails to perform the obligations provided under the Contract and these SC for Debit cards, the Bank may deprive such Cardholder of the right to use the card.
3. The Bank shall reserve the right to the produced card which the Cardholder fails to take over within 6 months of production, and terminate it without any explicit written request by the Cardholder.
4. All the transactions made by the card return date/submission a request for closing the current account for which the card is, including related costs, if any, shall be incurred by the Cardholder.

X.FINAL PROVISIONS

1. By signing the Application, the Cardholder agrees and authorises the Bank to charge its RSD current account or foreign currency account for all transactions and fees arising from using the card, in accordance with the relevant debit card Fee Tariffs.
2. By signing the Application Cardholder acknowledges that he/she is conversant with and agrees to all the provisions of these SC for Debit cards, which in conjunction with the Application, the Tariff for general banking services for corporate client, Cut-off time plan for debit accounts for Companies and Tariff for general banking services for SME clients Cut-off time plan for debit for SME clients constitute the Debit card Issuance and Use Contract, which have been handed to him/her on filing the Application.

The Bank shall reserve the right to amend these SC for Debit cards upon giving a prior notice to the Cardholder, if the changes relate to the contractual relationship of the User and the Bank

3. Anything not provided herein shall be governed by the General Business Conditions for Companies – General part and framework contract which user has concluded with the Bank, which regulates the rights and obligations related to the provision of payment services to the User
4. In case of any dispute, Court in accordance with the law will be competent.
5. These SC for Debit 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 sub-branches.
6. These SC for Debit cards have been drafted in Serbian and English. In the event of any inconsistencies between the Serbian and English versions, the Serbian version will prevail.
7. The provisions of these SC for Debit cards shall enter into force on the day of their adoption by the Bank's Supervisory Board and shall apply as of 01st of January 2026.

Supervisory Board of UniCredit Bank Serbia JSC Belgrade