# SPECIAL CONDITIONS FOR DEBIT CARDS FOR INDIVIDUALS, ENTREPRENEURS AND AGRICULTURISTS UNICREDIT BANK SERBIA JSC BELGRADE

**Belgrade, 20th July 2026**

**TABLE OF CONTENTS**

**Introductory provisions:**

**UniCredit Bank Serbia JSC Belgrade, as payment service provider (hereinafter referred to as: the Bank), these Special Conditions for operation for Debit cards for Individuals, Entrepreneurs and Farmers (hereinafter referred to as: SC for Debit cards) regulate mutual rights and obligations of the Bank and Users in respect of terms of issue and use of payment card.**

## I MEANING OF CERTAIN TERMS

**Payment Card** - in terms of these SC for Debit cards is debit card issued in physical form (plastic) or digital form (card data available within mobile application), which represents a payment instrument, which allows the Cardholder to perforem debit and credit pyment transactions, in accordance with and in a way described by this SC for Debit cards.
**Request for issuing a card** - the Bank's form that is filled out by the User of the basic card in the Bank, for the purpose of issuing a debit card, which represents essential part of the Request for use/modification of the account package.
**Main Card -** card issued in the name of the Cardholder, the owner of one or more bank accounts that are debited/approved using a debit card.
**Additional Card -** card issued in the name of the person for whom the Cardholder of the basic card submitted a request, and with the use of which the accounts of the User of the basic card are debited/approved.
**Cardholder** - refers to private individuual, sole proprietor, or agricultural entrepreneur who is the the user of the main and additional cards in the following text of these Special Conditions.
**PIN** - Personal Identification Number, a numeric code known only to the User, which serves as an authentication element for the User or the transaction initiated by the cardholder and/or authorization of payment transactions. 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 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.
**Digital wallet** – in a term of this SC for Debit cards 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** means the debit card registered in a Digital Wallet and/or electronic and mobile banking applications, which enables the User to initiate contactless payment transactions without using the physical card at points of sale, at ATMs that support contactless transactions and at the Online points of sale that allow this type of payment. The user can find out which debit cards can be digitized on the Bank's website.
**Mobile Device** - in a term of this SC for Debit cards means the device on which the Digital Wallet or POS terminal is installed.
**CARD ALARM** - is a service available to the the Card Users who are individuals or agriculturists to receive information about each successfully authorized card transaction immediately after it is executed, via a 'push' notification within the mobile banking (mbanking) application or SMS message, which simultaneously serves as a means of preventing misuse or card forgery by other persons. For entrepreneurs, notification of successfully executed card transactions is done via the SMS Card Alarm service, in accordance with the Special Conditions for using the SMS Card Alarm service. CARD ALARM does not affect the card user's right to receive information about completed payment transactions in other ways provided for by the contract, these Special Terms and applicable regulations.
**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.
**Service "Podigni dinare"** – cash withdrawal with purchase is a service offered by certain merchant, which allows consumers to raise cash with their debit card when buying goods. The amount of cash that can be raised on that occasion is defined by the merchant that provides this service.
**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
**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.
**Push notification** - a direct communication channel between the mobile application and the User, through which the User receives real-time notifications on their device without having previously requested the information.
**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.
**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.
**Biometric Data** – personal data unique to each User, such as fingerprint, facial contour, and similar identifiers. For the purposes of these Terms of Use for credit card operations under special conditions, it refers to a method of User authentication during online payments or payments made via the Digital Wallet.
**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.
**Digital content** means goods or services which are produced and supplied in digital form, the use or consumption of which is restricted to a technical device, and which do not include in
any way the use or consumption of physical goods or services.
**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 payment cards are ownership ofthe Bank, issued to the name of the Cardholder who may not give it away for use to third parties.
2. The Bank issues to the Cardholder payment card where the domestic payment transactions processing, clearing and settlement is done in the payment system in the Republic of Serbia (DinaCard cards). Besides the card from previous paragraph, at special request of the Cardholder the Bank can issue another type of the card from its offer range, for which the domestic payment transactions processing, clearing and settlement is done in the payment system outside of the Republic of Serbia ( internationally accepted cards). DinaCard payment cards can be used to pay for goods and services, via POS terminals and online, the receipt of funds, withdraw cash within the ATM network in the territory of the Republic of Serbia. Visa and Mastercard cards can be used to pay for goods and services, via POS terminals and online, the receipt of funds, withdraw cash within the ATM network (hereinafter referred to as: ATM) in the territory of the Republic of Serbia and abroad.
3. The Cardholder of the internationally accepted main card is required to ensure coverage on the dinar and/or foreignaccount at the time of payment card transactions. In a case payment transaction initiation with national payment card (DinaCard) the User must have sufficient available funds on the dinar account linked to the card.
4. The Cardholder of the main card is responsible for the use of his card as well as for the use of additional cards in accordance with the SC for Debit cards.
5. The Cardholder of the main card is responsible for the accuracy of the information provided to the Bank and is obliged to notify the Bank of any change in the information in accordance with General Conditions for providing payment services to Private Individuals Entrepreneurs and Agriculturists.

## III DEBIT CARD ISSUANCE

1. If the owner of current account applies for payment card that is linked to the account, the Bank is obliged first to issue a DinaCard payment card. In accordance with the above mentioned, the issuance of a payment card where in the domestic payment transaction processing, clearing and settlement are performed in the Republic of Serbia is a prerequisite for applying for any other type of payment card that the Bank has in its offer.
2. The process of issuing a debit card includes: submission of the Request (As part of the Request for Package Usage/Modification), creation and delivery of the 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) in the manner and in accordance with the Tariff of fees for debit and credit cards for private for individuals and agriculturists
3. When submitting a Request for the use/modification of a package, the User has the option of submitting a request for issuing a debit card in digital form (a prerequisite is that the user utilizes the Bank's mBanking service). In that case, the card details (card number, expiration date, and CVV/CVC code) are available in the mBanking application, under the section "Card Details." The PIN code is available under the section titled "Options," in "PIN Code Creation and Display," upon authentication using the selected method (mBanking PIN or biometrics)., with authentication by the selected method (mbanking PIN, biometrics). If the User requested the issuance of a card only in digital form, he can at any time request the issuance of a card in physical

form (plastic) through the mobile application or in the nearest branch of the Bank, in which case plastic with the same number, validity period and CVV/CVC number will be issued. In the case of a DinaCard debit card, in addition to issuing a card in digital form, the Bank automatically issues a plastic card to the User, which for security reasons is issued with a new card number as well as a CVV number and which must be activated during collection/handover. By issuing the plastic card, the client still has the possibility of viewing the card data within the mobile application through the appropriate option to display the card data.

**4.** The Bank issues the payment card on the basis of previously submitted Application by the User for the issuance of the payment card/usage of Package account that include payment (hereinafter referred to as: **Application**), which with these SC for Debit cards, General Condition for providing payment services to private individuals, enterprenuers and agriculturists, Cut-off time plan for payment accounts for private individuals, enterprenuers and agriculturists and corresponding Tariff for payment cards of the Bank shall be the contract on Issuance and Usage of payment cards.

**5.** The Bank will replace debit cards without a signed request from the User only in case of problems in the functioning of the debit card, migration of products to new technological solutions, cancellation of products or changes in the content of the Product Catalog, in situations where the previous card was deactivated for security reasons due to misuse or suspected misuse, as well as in cases of increasing the level of protection of the product or the card user, where authorized the person for taking over the card from the User gives the User's consent by signing the confirmation of taking over the card and PIN, only if that User has already been issued a DinaCard debit card.

**6.** In case plastic of the payment card is destroyed/damaged, the User is obliged to inform the Bank in writing form in the Bank branch or using e-banking and m-banking application. When replacing the damaged plastic, the new PIN code will be generated to the user.

**7.** The Bank may, at the request of the User of the main card, issue additional cards, in the manner and under the conditions defined by the Bank's current offer. and that, subject to the condition of fulfillment of the prerequisites indicated in point 1, the costs incurred through the use of additional cards are charged to the account of the user of the main card, in accordance with the Tariff of Fees. The user of the basic card or the person in whose name the user of the additional card was issued can pick up the additional card at the Bank's branch. In case of sending an additional card to the address, it is delivered to the address of the User of the main

**8.** When creating a card, the Bank generates a PIN for the Cardholder, which is known only to the cardholder , which is used to withdraw cash from ATMs or using „Podigni dinare“ service, as well as perform transactions at POS terminals. The Bank bears the risk in connection with the delivery of the card and PIN to the Cardholder. The Bank enables the User to view the PIN and card data (card number, expiry date, CVV/CVS) through the mbanking application immediately after activating the card and they are available to the User at all times for all cards issued at his request.

**9.** The physical card can be used after activation, which is performed in one of the following ways, subject to prior user authentication:

- Upon collection of the card at a Bank branch, in which case a Bank employee performs user identification;
- During the first transaction with a correctly entered PIN code (e.g., cash withdrawal, balance inquiry at an ATM, or payment at a point of sale), in cases where the card was previously issued in digital form, and the PIN entry confirms user authenticity;
- By calling the Bank’s Contact Center, where the Contact Center agent verifies the user’s identity.

**10.** The Cardholder must sign the plastic immediately upon receipt/delivery. An unsigned card is invalid, and any financial consequences, which may arise as a consequence of the fact that the plastic is not signed, in the event of misuse of an unsigned card shall be borne by the Cardholder. The Cardholder is obliged to keep the assigned PIN secret and to take all reasonable and appropriate measures to protect it, in order to protect the card against abuse, which in particular means sharing of PIN information through verbal or written communication, as well as the prohibition of accepting assistance from third parties when typing the PIN at an ATM or at a point of sale. Also, it is especially important not to write PIN on the card or on any other document that is kept 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, and within the mobile banking aplication. 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 payment card. Sharing the PIN, as a security credential, with third parties; storing it together with the payment card; or selecting a numerical PIN code that does not meet minimum security standards when changing it, shall be considered gross negligence on the part of the Cardholder. Consequently, the Cardholder shall bear full financial responsibility for any consequences arising from misuse of the debit card due to such actions, or in cases of careless storage and use of the debit card..

**11.** During production, the period of validity indicated in the format MM/YY on the face of the plastic, i.e. in a digital form of the card in mobile application, shall be decided on. The period of validity of the card expires on the last day of the month indicated on the card at 24:00 hours.

**12.** After the expiry of the validity period of a debit card in which, in domestic payment transactions, the processing, netting and settlement of transfer orders issued on the basis of its use are carried out in the payment system in the Republic of Serbia, such card is automatically issued for a new period of validity. After the expiry of the validity period of a debit card for which, in domestic payment transactions, the processing, netting and settlement of transfer orders issued on the basis of its use are not carried out in the payment system in the Republic of Serbia, such a card is automatically issued for a new period of validity, and only if that User has already been issued a debit card for initiating payment transactions from the same current account, with which, in domestic payment transactions, the processing, netting and settlement of transfer orders issued on the basis of its use are carried out in the payment system in the Republic of Serbia, and with the condition that the User is had transactions with that debit card in the previous 6 months

## IV USAGE OF THE CARD

1. The debit card issued in physical form (plastic) can be used to make payments at points of sale, pay via the Internet, and withdraw cash within the acceptance network of the card association to which the card belongs. The debit card issued in physical form can be used for cash payments at certain Bank ATMs marked for that purpose.
2. Debit cards issued in digital form are enabled for payments via the Internet with 3D Secure authentication (Mastercard, Visa, Dina cards. Debit cards issued in digital form can be registered in a digital wallet (Mastercard and Visa cards), which enables the performance of all transactions with a digital wallet, in the manner and in accordance with Chapter VI of these Special Conditions.
3. The payment card whose term of validity expired must not be used further.
4. The Cardholder is not entitled to give the payment card as collateral or security instrument for the payment.
5. If the Cardholder has been denied by the Bank the right to use the payment card, he shall at the request of the seller of goods and/or services (Acceptor) or the paying bank, hand over the payment card.
6. The Cardholder shall, when purchasing goods and/or services at the point of acceptance that is equipped with a POS terminal, if the card is based on CHIP tehnology personally enter his PIN with all possible discretion, or his signature if the card is based on magnetic stripe tehnology. The Cardholder must not tell his PIN to the Acceptor or to any other person.
7. The point of sale issues a copy of the slip/receipt for executed payment and the Cardholder is required to sign the copy the slip/receipt in the way he signed the payment card and the slip/receipt remains with the Acceptor. The use of PIN shall be considered the Cardholder’s signature, by which the User approves the payment transaction.
8. When using a card at POS terminals that support contactless technology, the User can decide if he whant to make the transaction through a contactless technology or to require a merchant to make a standard payment transaction method, which entails the authorization of the transaction by entering the PIN code. If the user opts to use the contactless payment option, transactions are carried out by tapping the card on the POS terminal. In certain situations, additional authentication by entering the PIN code may be required if the amount or number of transactions exceeds certain limits for card use, all in order to prevent potential misuse.
9. In addition debit card (based on payment 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. With inflow authorization funds the User may dispose only after posting of the transaction to the corresponding current account of the beneficiary.
10. With his signature/PIN autentification, the Cardholder guarantees that the amount is correct and that he will settle it in accordance with the SC for Debit cards. A copy of the slip (receipt) is retained with the Cardholder, in case of complaint.
11. The Cardholder may withdraw cash at bank counters, post offices, ATMs and using service “Podigni dinare” using a PIN. The Cardholder has the possibility to change the PIN, within the Bank’s network of ATMs in the territory of the Republic of Serbia. In order to increase safety, the Bank defines daily, weekly or other limits (in terms of amount and number of transactions) for withdrawal of cash or payment for goods and services from the card account according to the applicable Tariff of fees for payment cards of the Bank. The Cardholder may request a change of daily limits and/or the number of transactions, by signing the Request at the branch. Request for change of daily limits and/or the number of transactions Cardholder may also initiate by sending a Request via e-banking or trough mBanking functionality. The User acknowledges that any increase in the card limit, upon their request, raises the potential financial risk in case of card misuse. The User shall bear full financial responsibility for any damage exceeding the daily limits defined in the Bank’s Fee Tariff. The Bank reserves the right to decline the requested limit increase if it assesses a heightened risk of misuse or financial loss resulting from such misuse. The user can make a cash payment in local currency RSD (on dinar account linked to the card) and foreign EUR currency (on foreign account linked to the card) at certain ATMs of the Bank, with the use of a PIN, and in accordance with the limits defined by the Bank's Tariff.
12. The Cardholder of the payment card can check the account balance on dinar account linked to the card or the balance of available funds by means of a query on an ATM, with payment of fees in accordance with Tariff of fees for payment cards. The User can check the available balance on the accounts linked to the debit card via the Bank’s mBanking/eBanking application.
13. Electronic records from ATM and POS terminals (logs) are proof of the transaction.
14. The Bank through the CARD ALARM service notifies the cardholders who are individuals or agriculturits of a successfully completed card transaction immediately after the transaction is executed, i.e., authorized. The CARD ALARM service is automatically activated upon issuance and delivery of the card. CARD ALARM notifications are received via push notifications in the mBanking application if the client has activated the mBanking application and enabled the receipt of push notifications. In the event of not activating mobile banking application or disabling push notifications in the mBanking application, notifications on completed transactions are delivered via SMS to the phone number of the user registered in the Bank’s system. The CARD ALARM notification provides the User with information on successfully completed payment card transactions (payment for goods/services as well as cash withdrawals). Notifications regarding the use of an additional card/cards are sent to the primary cardholder via push or SMS message. The Card Alarm notification regarding a successfully completed transaction contains information about the transaction amount in the currency in which it occurred, the place and time when the transaction took place, as well as the remaining amount of available funds in the accounts to which the card used for the transaction is linked. The condition for receiving a push notification is connecting the mobile phone to the internet.

The user is obliged to immediately block the payment card via the mobile banking application or by calling the Bank's Contact Center if they receive a Card Alarm notification for a transaction they did not initiate, in order to prevent misuse. The Bank shall not be responsible if the information provided through the CARD ALARM service becomes accessible to third parties due to the loss/theft of a mobile phone, until the sending of such information is stopped based on the User's notification, and/or the User's negligence which results in the accessibility of this information to third parties. The Bank shall not be responsible for any potential misuse of data provided through the CARD ALARM service that may occur due to the use of mobile operator networks.After the reception of push notifications in the mobile application has been disabled, the User may request that the Bank cease sending SMS notifications by submitting a Request at the nearest Bank branch. The card user is aware that after the termination of receiving SMS notifications, he will not receive CARD ALARM notifications about completed transactions, that is, he will not be notified in real time about completed card transactions, and that he thus assumes the risk of untimely knowledge of disputed transactions and the consequences that may arise due to delays in taking protective measures and reporting them to the Bank.

The payment cards issued by the Bank may not execute transactions in foreign sites registered for gambling.

**15.** The Bank retains the right to limit the use of payment card (blockade) in accordance with the General Conditions for providing payment services to Individuals, Entrepreneurs and Farmers, as well as in the following cases:

i. if there are legitimate reasons concerning security of the payment card.
ii. if there is a doubt with regard to unauthorised or fraudulent use of the payment card, or as a result of fraud. In the case of suspicious transactions, the Bank blocks the card until the Cardholder authenticates the transaction as his transaction by calling the phone number placed on the back of the card.
iii. in the case when transactions on POS terminals, Online point of sale and ATMs are made by the card, which compromising activity was previously recorded (placing the skimmer, misuse of data, etc.), the Bank permanently blocks the card, makes a decision on re-issuance of the card in which case it shall automatically re-issue the card to the Cardholder, free of charge, if the conditions of this SC for Debit cards are fulfill.
iv. if there is a higher risk that the Cardholder will not be able to meet his payment obligations, when the use of payment card is associated with the approval of the User’s account overdraft.
v. after three consecutive incorrect PIN entries, the card can be used again only after contacting the Bank’s Contact Center.

**16.** Depending on the circumstances mentioned in the preceding paragraph, the Bank may temporarily or permanently block the card.

**17.** The Bank shall notify the Cardholder of its intention to block the payment card and the reasons for the blockade by email or by calling or sending an SMS to the phone number that the Cardholder submitted to the Bank as a contact, and if it is unable to notify the Cardholder before the blockade of the payment card, it is obliged to do so immediately after the blockade.

**18.** The Bank shall not notify the Cardholder about an intention of blockade or of payment card blocking if giving such notifications is prohibited by law or if there are justifiable security related reasons.

**19.** The Bank will again enable the use of the payment card or will replace it with a new one - once the reasons for its blocking cease to exist.

- In a case of using the card for transactions where the card is not physically present, the User is obliged to take basic precautions:
  i. to never send sensitive payment data via e-mail, SMS, or phone
  ii. 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
  iii. To initiate a payment at merchants that provide a secure environment (Visa Secure, Mastercard ID Check, DinaCard Secure), in order to ensure reliable user authentication. Reliable user authentication is performed as follows:
  a) By logging into the mobile application after receiving a push notification for each individual transaction. This is the primary method of authentication and depends on the activation of the mobile banking service as well as the notification settings within the application.
  b) 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 keeping this information up to date.

The Bank reserves the right not to approve a transaction initiated at Internet sales points that provide payment using the 3D service if the Card User authentication has not been performed.

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 share or grant 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 comply with the above-described data protection measures.

The Bank may apply exceptions to reliable User authentication in accordance with positive regulations (recurring transactions with the same amount and the same payment recipient within certain time intervals, low-value transactions, transactions assessed as low-risk, etc.). In the case of recurring transactions, the User at the online point of sale gives consent for all subsequent transactions until the consent is withdrawn.

In the mobile application, under the Card options, the User has the ability to view the online points of sale where consent has been given for executing recurring transactions, as well as any other online points of sale where card data is stored for future payments without entering card data (card-on-file). In the mobile application, the User can temporarily disable charging from the card account based on subscriptions and card-on-file payments, while a complete termination of charging from the card account is carried out by terminating the contractual relationship between the User and the online merchant. In order to facilitate faster and more secure payments at online retail locations that support this service, the User may register their card on the Click to Pay platform and make payments without manually entering card information at merchants that support this payment method.

## V AUTHORISATION AND POSTING OF TRANSACTIONS

1. 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. 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. 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. Tapping a mobile device with an installed Digital Wallet on a POS terminal or ATM that supports contactless transactions (deposit/withdrawal of RSD and EUR transactions for ATM transactions).
   iv. Entering the PIN code when initiating a payment transaction at the ATM (by inserting the card into the reader or by contactless reading)
   v. Entering security elements required by the payee when initiating a payment transaction at online merchants (card number, CVV2/CVC2 code and/or one-time password), including authentication elements such as biometrics or login PIN for the mobile application, OTP code, and static password assigned by the Bank and known exclusively to the User.
   vi. Using the card within the digital wallet in the manner described in these Terms of Business with credit cards
2. 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.
3. 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.
4. 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 reservation.
   All debits/credits authorisations resulting from the use of payment cards are made in the local currency, i.e., in dinars, and so the amount of reserved funds for debits/credits transactions in other currencies, until the posting of the transaction, may differ from the original amount.
5. **Transaction concluded on devices (ATM/POS/Internet) registered in the country** – calculated curency is RSD. After the transaction is submitted to the Bank, the RSD current account is going to be debited / approved first. If the User of the main card 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.
6. **Transaction concluded on devices (ATM/POS/Internet) registered a broad** – 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 Bank's settlement 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 of the main card 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 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.
7. Exceptionally the preceding paragraph, for payment 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 debt 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.
8. The Client can dispose with approved funds resulting from the usage of payments card, only after Bank receives them, ie. after the funds are posted on the account of the main card user.
9. 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 SC for debit cards.
Banksystem 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.
The user of the main cardshall 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
If, after the expiry of 60 days from the date of the transaction made by using the payment 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. The Bank shall ensure the refund of the amount or a correct execution of the payment transaction if the Cardholder has notified the Bank about the unauthorised, or incorrect execution of the payment transaction and/or has requested the correct execution of the payment transaction, immediately after becoming aware of such payment transaction, provided that he has delivered such notification and/or request within 13 months after the debit date.

**10.** The Cardholder agrees and authorises the Bank to collect the outstanding liabilities incurred by operations with payment cards also from other accounts that the Cardholder has opened at the Bank, which do not have to be linked to the card.

**11.** 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, payment institutions and retailers, etc.).

**12.** The Cardholder is aware and accepts that the use of payment cards for payment 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.

**13.** 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 outside of 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.

## VI CONDITIONS OF USE OF THE DIGITIZED CARD

**1.** To register a debit card in the Digital Wallet (such as for example Apple Pay,Google Pay), it is necessary for the User 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. In certain cases, the service provider may disable the use of the Digitized Card in their mobile wallet, which the Bank cannot influence or have insight into the reasons for this.

**2.** By signing the Request for issuing a card/Request for opening/changing a package account and issuing a debit card, the Bank makes it possible for the User to register the debit card in the mobile wallet, subject to the fulfillment of the conditions specified in the previous paragraph. The Bank will consider each request for card registration in the Digital Wallet when the phone number submitted to the Bank in the card tokenization request is identical to the User's phone number in the Bank's system as an authorized User request.

**3.** 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 through the mobile banking application, the User authorizes the Bank to provide the Service Provider with the User's identification data and the registered debit card information, all for the purpose of using the service of the Provider. The Bank does not influence and is not responsible for the manner in which the Service Provider collects and processes the data.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.

**4.** 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.

5. 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.
6. 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.
7. 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.
8. The user is obliged to keep his card data, as well as all the data he receives from the Bank for the purpose of authentication during the card registration process, exclusively for himself, as well as to never share them with other people or enter them outside of the mobile wallet. After successfully completing the registration of the debit card in the mobile wallet, the Bank sends an SMS notification to the User. If the User has not personally initiated the debit card registration process, it is necessary to immediately take all measures in order to block the card as quickly as possible and prevent possible misuse..
9. The Bank may, in case of suspicion of misuse of debit card data for the purpose of its registration in the Digital Wallet of a third party other than the User or of other User data relevant to the process, request additional authentication by referring to the Bank's Contact Center or mobile application, as well as perform a temporary blocking debit cards. The Bank informs the User about the temporary blocking, in accordance with Article IV of these Special Conditions
10. By registering a debit card in the Digital Wallet on a certain Mobile Device, the User undertakes 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 Digitized Cards on that device.
11. 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 TRANSACTION 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 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 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 of the main card 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. through an electronic or mobile banking application, if the complaint refers to services that the Bank provides or has provided through those services.
5. The complaint must include the complainant's personal information necessary for identification and for determining the business relationship with the Bank to which the complaint refers, as well as the reasons for submitting the complaint. If the complaint represents a Request for Verification, it must contain details of the transaction for which the user's current account was debited, and which the User disputes as unauthorized or improperly executed, along with any known circumstances under which the transaction occurred. Based on such a submitted Request for Verification, the Bank will determine whether there are grounds to initiate 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 from the merchant, provided that the conditions for such action are met in accordance with the rules of this type of dispute resolution procedure
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 Cardholder 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 User 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 User must include a deadline for acceptance, which cannot be shorter than 5 days or longer than 15 days from the date of submission.

## VIII STOLEN OR LOST CARD/ LIABILITY OF THE BANK AND THE USER FOR THE EXECUTION OF A PAYMENT TRANSACTION

**1.** The Cardholder must, without delay urgently upon learning of the lost or stolen of the payment card block the card via the mobile application, and request from the Bank to block the card's further use.

**2.** The customer reports the lost/stolen card by telephone to the number of Contact Centre +381 11 3777 888, therefore, it is advised that the Cardholder always keeps the number of the Bank's Contact Center with him. After blocking the card through the mobile application or report the lost/stolen a debit card , 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.** In the case that a lost or stolen payment card is returned to the Cardholder or the Cardholder has found it, he must notify the Bank thereof. If there is a blockade of the payment card, based on the previously reported stolen or loss of the card, the Cardholder can request its activation and continued use.

**4.** In case of loss/theft of a mobile phone in which the Bank's mobile application is installed, through which the User is enabled to view the card data, it is necessary for the client to report the theft/loss to the Bank without delay by calling the Contact Center number +381 11 3777 888, in in which case the Bank will block the card.

**5.** When payment card that was blocked previously by the client (lost/stolen) need to be reissued, it is necessary to fulfill the preconditions that was set trough this SC for Debit card in the sense that the DinaCard payment card has already been issued to the cardholder. On that occasion, the User can also submit a request for the issuance of a card in digital form. After reporting the loss/theft of a mobile phone in which the Bank's mobile application is installed with the possibility of viewing the debit card data, the User is obliged to confirm the report to the Bank by filling in the appropriate form in the nearest branch of the bank, as well as to request the reissuance of the card.In the event that the payment card is destroyed/damaged, the Cardholder is obliged to notify the Bank in writing thereof by filling out the appropriate form in the branch of the Bank where the card is issued.

**6.** In the event that there has been an unauthorised use of the payment card or of the data from the payment card - the Cardholder shall, immediately after finding this out, and not later than within 13 days from the date of debiting, report to the Bank the transaction executed by unauthorised use of the card or of the data on the card, in which case he/she may bear the loses as a result from the unauthorised use up to a maximum of RSD 3,000.

**7.** The Cardholder shall bear all loses in connection with any transaction executed by means of abuse which he/she does himself/herself, and shall bear the loses made as a result of failing to fulfil his/her obligation to immediately inform the Bank of the lost, stolen and misuse of the payment card, the obligation to adequately keep his/her card and the PIN code, as well as other obligations under 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 payment card is issued to the User, or the rules of its use.

**8.** 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.

**9.** The Cardholder shall bear no loses for an unauthorised payment transaction arising from transactions executed after reporting to the Bank the lost, stolen or unauthorised use of the payment card or payment card data:

i. if the loss, theft or misuse of the card was not detected by the User before the execution of the unapproved payment transaction, unless the User did not fulfill his obligations arising from these PU operations with debit cards

ii. If the unapproved payment transaction is the result of the Bank's action or omission,

iii. if the Bank does not provide at all times appropriate means of notification of a lost, stolen or misappropriated payment instrument,

iv. on the basis of transactions carried out after reporting to the Bank the loss, theft or unauthorized use of the debit card, i.e. the data from the debit card, unless Cardholder committed abuse or participated in abuse or acted with the intent to defraud

v. If the Bank does not require and does not apply reliable authentication of the Card User in cases where it is legally obliged to do so, unless the loss is due to the fraudulent actions of the Cardholder.

**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

## IX CARD CANCELLATION

**1.** At the written request of the Cardholder, the Bank shall cancel the use of the payment card free of charge. Request for closing the payment card where in the domestic payment transactions processing, clearing and settlement use are performed in the payment system in the Republic of Serbia, it implies automatic shutdown of all payment cards issued to the User by the Bank.

**2.** If the Cardholder does not comply with the obligations of the contract and these SC for Debit cards, the Bank may deny the right to card use.

**3.** The Bank reserves the right to cancel the produced card which Cardholder does not collect within 6 months of production without a specific written request of the Cardholder.

**4.** All transactions concluded until the day of return of the card/submission a request for closing the current account for which the card is linked as well as any expenses shall be borne by the Cardholder.

**5.** The Cardholder is entitled to have his payment card closed free of charge.

## X FINAL PROVISIONS

**1.** By signing the Request, the Cardholder agrees and authorises the Bank to debit his current dinar or foreign currency account for all transactions and fees incurred by using the card in accordance with the Tariff of fees for payment cards.

**2.** By signing the Request, the user of the basic card confirms that he is familiar with and agrees with all the provisions of these PU operations with debit cards, as well as to familiarize the Users of additional cards with them.

**3.** The user of the basic card agrees that the Bank has the right to change and supplement these PU operations with debit cards, the Tariff of fees and the Term Plan without the express consent of the User of the basic card. The Bank undertakes to submit in writing, in accordance with the General Terms and Conditions of Payment Services to Individuals, Entrepreneurs and Agriculturists, proposals for changes and additions to the User, if they relate to the User's contractual relationship with the Bank, no later than two months before the proposed date of commencement of application of those changes. . The user can agree that the proposed changes and additions produce a legal effect even before the proposed day of the start of their application. It will be considered that the User has agreed with the proposal of amendments and additions, if he has not informed the Bank that he does not agree with the proposal before the day of their application. If the User does not agree with the proposed amendments, he has the right to cancel the debit card without paying fees and other costs before the date of implementation of the proposed amendments.

**4.** For everything that is not provided for in this PU of business with debit cards, the General Terms and Conditions of Business with Individuals, Entrepreneurs and Agriculturists apply - General part and framework agreement that the user of the basic card has concluded with the Bank, which regulates the rights and obligations in relation to with the provision of payment services to the User.

**5.** In the event of a possible dispute, the local and actual competent court in the Republic of Serbia is competent.

**6.** These PUs for business with debit cards were drawn up in accordance with the Law on Payment Services and regulations of the Republic of Serbia and are available on the Bank's website www.unicreditbank.rs, as well as in all branches of the Bank

**7.** These SC for Debit cards are prepared in Serbian and English. In the event of discrepancies between the Serbian and English versions, the Serbian version shall prevail. The Bank will act in good faith when executing Cardholder's orders and will do everything in its power to protect the interests of the Cardholder in each individual case.

**8.** The provisions of the SC for Debit cards shall enter into force upon their adoption by the Board of Directors and shall apply from 12th October 2026.

**Management Board of UniCredit Bank Serbia JSC Belgrade**