General Conditions of Use

(GCU)

Current account and attached products

– Individuals –

SUMMARY

I. GENERAL PROVISIONS

CHAPTER 1. INTRODUCTION

1.1 Scope. a) These General Conditions of Use ("GCU") govern the relationship between the Bank, on the one hand, and the Client, Proxy, User, any person representing the Client, on the other hand, with regard to the execution, performance and termination of the agreement for Current Account and the other products/services in the scope of the GGUs. Each required product/service is applicable with: **(i)** General Provisions (Chapters 1-4) together with the Final Provisions (Chapters 12-13) and **(ii)** Related Special Provisions, respectively Chapters 5-12. The Special Provisions shall prevail where there is a discrepancy between them and any of the General Provisions and Final Provisions. The GCU provisions are binding on the parties.

b) From the moment of their signing/ communication on a Durable medium, these GCUs replace any previous form thereof, and any contrary provisions existing in the contents of any prior forms/ contracts related to the products/ services subject to these GCUs and, where appropriate, these GCUs supplement them. An exception from the above are the costs, as in their regard the previous provisions shall remain valid, as they can be amended only according to the law and the Agreement, as well as the provisions of art. 9.1, para. (8).

c) The provision of a product/service is conditioned by the opening and maintenance of a Current Account with the Bank. Any reference to a particular product /service is applicable in the relationship between the parties only if it had been contracted. If the Client fail to provide the documents/information requested by the Bank or provide false data/documents or with regard to which there are solid indications that they are false/incomplete or in other circumstances in observance of legal conditions, the Bank is entitled to deny the Client's request to provide a product/service and/or performance of payment operations and/or opening of the relationship, at its sole discretion, in observance of legal provisions related to the know-your-customer legal provisions, in order to prevent money laundering and funding terrorism.

1.2 The Bank provides to the Client the possibility to contract/amend/supplement particular products/services without the physical presence of the Client, by the use of remote communication techniques. The Client will answer any questions and provide any information required for their identification, in order to prevent unauthorised access to confidential data; otherwise, the Bank will deny the application. Prior to contracting/amending/supplementing, the Client will be notified with regard to the product/service according to the applicable legislation in force. Immediately after this moment, the Bank will notify the Client, with regard to the complete terms and conditions of the agreement, in writing, on paper support or on another Durable medium.

1.3 Terms used (arranged alphabetically): **Strict authentication** - authentication based on the use of two or more elements assimilated in the category of specific knowledge (something that only the user knows - e.g., PIN), possession (something only the user possesses, e.g., Token device - Digipass, Mobile Token, card, Mobile B@nking) and inhesion (something that represents the user, e.g., facial scanning, fingerprint) which are independent and the compromise of one item does not lead to the compromise of reliability of the other elements and which are designed to protect the confidentiality of authentication data. **Bank** - UniCredit Bank S.A., a company administered in a two-tier system, having its registered seat in Bucharest, Bld. Expoziției nr. 1F, sector 1, registered with Trade Register under no. J40/7706/1991, European Unique Identifier (EUID): ROONRC.J40/7706/1991, in the Bank Register under no. RB-PJR-40-011/18.02.1999, sole registration code RO361536, registered capital subscribed and paid-in of RON 455,219,478.30, web page www.unicredit.ro. **UCFin** - UniCredit Consumer Financing IFN, a company administered in a two-tier system, having its registered seat in Bucureşti, Bd. Expoziției 1F, et 6, sector 1, registered in NBR General Registry under no RG-PJR-41-110247/24.10.2008 and Special Registry under no RS-PJR-41-110065/09.02.2010, registered in Payment Institutions Registry under no IP-RO-0009/02.03.2015, sole registration code RO 24332910, registered capital subscribed and paid-in of RON 103.269.200 Lei, web page www.ucfin.ro **ATM** - an unassisted terminal which can provide cash withdrawal services via Payment Instruments (physical debit / credit card), the garnishment bar code and MCash code, invoice payments, notifications regarding the balance of Accounts and the history of the last 10 trasactions made by debit card. **Beneficial owner** – any natural person who ultimately holds or controls the client and/or the natural person on whose behalf a transaction, operation, or activity is performed according to the provisions of Law no. 129/2019 on the prevention and countering of money laundering and funding terrorism, as well as for the amendment and supplementation of legislative acts ("Law no. 129/2019"). **NBR** – the National Bank of Romania. **Client** – natural person coming into legal relationships with the Bank by signing the Agreement and acting for purposes outside their professional activity. **The MCash code** - represents the numeric code or its equivalent transposed in QR graphic format (matrix barcode containing information that can be read by a scanner and transposed into text information), generated from Mobile B@nking for cash withdrawals in RON from the current account, from the ATM / BNA terminals of UniCredit Bank. **Current account/Payment account/Payment account with basic services** - bank account used for the performance of Payment Operations. In the Agreement, any reference to the Current Account/Payment Account also includes the payment account with basic services and any reference to the Payment account with basic services will be

understood as being performed strictly related thereto. **Payment account accessible on-line** – payment account which can be accessed by the Client by means of an on-line interface (e.g., Mobile B@nking, Online B@nking). **Agreement** – the **„**Application**"** (representing the application in the standard format of the Bank, regardless of name, with which the Client requested the provision of any product/service in the scope of the GCU, except for the term deposit which does not require the filing of an Application), together with the present General Terms of Use ("GCU") and the "Annex" (representing the Annex with Fees and Commissions, regardless of name, which includes the costs related to bank products/services contracted by the Client, owed by the Client), as well as any other written document which is specified to be an integral part of the Agreement. The Agreement is executed in the number of original counterparts corresponding to the number of signatories. **Foreign currency date** – the reference date used by the Bank to calculate the interest related to the funds debited or credited from/into the Client's account. **Unauthorised overdraft** – excess of the amount available in the accounts of any type of the Client by the value of fees, interests, any amounts owed to the Bank as a result of the use of any product/service made available by the Bank. **Security elements** – customised characteristics provided by the Bank to the Client/User, consisting of information and devices (including, without being limited to codes/passwords/PIN code/Username/Security code/Token device-Digipass) which allow the authentication of the Client/User in order to access/use the products and services in the scope of Agreement and which are not transmissible to other persons. **Agreed utility provider's/Utility providers** – the utility suppliers that entered in an agreement with the Bank, for which the payment of utilities can be ordered and for which interbank direct debit mandates can be concluded, according to the information made available in/on Online B@nking/ Mobile B@nking/ BNA screen/ webpage. The Bank may amend this list at any time. **Group/UniCredit Group** - UniCredit SpA (Italy) and companies controlled directly/indirectly, including the Romanian companies of the Group (UniCredit Bank SA, UniCredit Leasing Corporation IFN S.A., Debo Leasing IFN SA, UniCredit Leasing Fleet Management SRL, UniCredit Insurance Broker SA, UniCredit Consumer Financing IFN SA, UCTAM RO SRL etc.) and the legal successors of these entities. **IBAN** – an array of characters which identify uniquely and on international level a client's account with a credit institution. **Imprinter** – a mechanical device which allows the collection of a print of items embossed on the card, on the surface of a paper document to certify the execution of the transaction (receipt). **INFO Centre** – 24/7 available service, which provides technical assistance and provide support , including with regard to the requests to block access to Payment instruments/Security elements, according to the Agreement, as well as the communication of general information regarding potential doubts related to the operation of products/services, at phone numbers *2020 (normal rate call in mobile networks of Telekom Romania, Vodafone, Orange, RCS&RDS), 021 200 20 20 (normal rate call in Telekom Romania landline network) or 0800 888 111(free call; phone number available only for blocking/unblocking of Payment instruments/Security elements). **Payment instrument** – any customised devices and/or any set of procedures agreed between the Bank and the Client in order to initiate a payment operation, including cards, physical or virtual, barcodes and remote payment instruments (Online B@nking, Mobile B@nking). **Mobile B@nking** - remote access payment instrument based on a Mobile Banking-type of IT solution. **Online B@nking** - remote access payment instrument based on an Internet banking-type of IT solution. **Payment Order** - the instruction sent to the Bank (as the payment service provider) to perform a credit transfer operation - payment operation. **Standing order** - the instruction sent to the Bank (as the payment service provider) to carry out, automatically, a sending money - payment operation at predefined deadlines. **Limit hours** - limit hours established for the receipt of payment orders/instructions, inclusively for the authorisation of operations by Online B@nking/Mobile B@nking /BNA so that they are processes (the Client's account is debited) in the same Business Day, unless explicitly specified otherwise. A payment order which had been denied for payment by the Bank is considered as not received. **Payment operation** – the action initiated by the payer or by the beneficiary of the payment in order to deposit, transfer (by standing orders, credit transfer or direct debiting) or withdraw funds from an account used for that purpose. **Publicly exposed persons** - natural persons who hold or held important public offices. In the meaning of Law no. 129/2019, important public office means: a) heads of state, heads of the government, ministers or deputy ministers or secretaries of state; b) members of the Parliament or of similar central legislative authorities; c) members of the management bodies of political parties; d) members of the supreme courts, or the constitutional courts or of other legal courts of high level whose decisions can only be appealed by means of extraordinary methods of appeal; e) members of bords of the courts of auditors or of the boards of central bank; f) ambassadors, business envoys and high-rank officers of the armed forces; g) members of the boards of directors and supervision councils and persons in management positions of public corporations, state-owned companies and national companies ; h) directors, deputy directors and members of the board of directors or members of the management entities within international organisations. **Family Members of the Publicly Exposed Person** are, in the meaning of Law no. 129/2019: a) the spouse of the Publicly exposed person or their partner with whom they are in spouse-like relationships; b) the children and their spouses or partners, persons with whom the children are in spouse-like relationships; and c) parents. **Persons known as close associates of Publicly Exposed Persons** are: a) natural persons known as beneficial owners of a legal entity, of an entity without legal personality or of a legal construction similar thereto together with any of the Publicly Exposed Persons or as having any other close business relationship with such person; b) natural persons who are the only beneficial owners of a legal person, of an entity without legal personality or of a legal construction similar thereto, known as established in the *de facto* benefit of Publicly Exposed Persons. **POS** – the device which allows, by electronic means, the collection, processing, storage and transmission of information on card payment performed at the retailers' sales points. **Public office hours** – the period in the Business Day when the Bank allows the Client's access in its local units to perform banking operations, according to the specific limit hours for each type of operation. **Third party payment service provider** – a provider of payment services, other than the Bank, authorised by the National Bank of Romania or by a competent authority in a Member State of the European Union to provide information services with regard to accounts and/or payment initiation services and/or services for the confirmation of fund availabilities. **Penalties** – any restrictions and obligations (undertaken by UniCredit

Group) with regard to goods, persons, territories, adopted by the European Union, the Security Council of the United Nations, the Government of the United States, by other international organisations or by unilateral decisions of Romania or of other states, including the by-laws issued for the application thereof, in order to maintain peace and international security, prevent and counter terrorism, ensure the observance of human rights and fundamental liberties, development and consolidation of democracy and rule of law and achievement of other purposes, according to the goals of the international community, with international law and European Union law. **Notification service with regard to accounts** - on-line service, provided by a third-party service provider (other than the Bank), which provides consolidated information with regard to one or more Payment Accounts accessible on-line, held by the Client with the Bank and/or multiple providers of payment services. **Payment initiation service** - initiation service for a Payment Order with regard to a Payment Account accessible on-line held by the Client with the Bank, provided by a third-party payment service provider (other than the Bank), on the Client's demand. **Apple Pay** – digital platform provided by Apple Distribution International Limited to make payments on the Internet and contactless payments to merchants' POS with an Apple Pay compatible mobile device. **Google Pay Service** - The service provided by Google Ireland Limited to make payments on the Internet and contactless payments to merchants' POS with a Google Pay compatible mobile device. **Durable medium** - any instrument (e.g., e-mail, SMS, Online B@nking, Mobile B@nking) which allows the Client to store information sent to him, in a manner accessible for further access and for a period of time appropriate to the purposes of the respective information, which allows the identical reproduction of the stored information. **Sending money - intrabank payments** – transfer of funds between the accounts, where the account of the payment beneficiary is opened with the Bank. **Sending money - "INSTANT" type intrabank payments** - fast transfer of funds in LEI, between accounts opened at UniCredit Bank, through Online B@nking and Mobile B@nking, which are identified in the details of the transaction generated by the Online and Mobile B@nking services, by the acronym "IPTR" or "Instant". **Sending money - interbank payments** – transfer of funds between the accounts, where the account of the payment beneficiary is opened with another credit institution than the Bank or State Treasury. **Offline transaction** - represents the transaction made with the physical card at a terminal that accepts transactions without obtaining an authorization code from the card issuing bank and for which the funds are not blocked on the date of the transaction, but the Client's account is debited with the transaction value on the date of its settlement. **Business Day** – any day of the week, less Saturdays, Sundays and any national and/or legal holidays, when credit institutions in Romania are open for public and perform banking activities, as well as any other days considered business days by the corresponding banks/payment systems with external settlement in case of payment operations performed by means of them. With regard to payment operations, "**Business Day**" means any day of the week when the Bank can perform them, according to the Limit Hours for any type of instruction.

CHAPTER 2. GENERAL PROVISIONS ON THE CURRENT ACCOUNT AND PAYMENT OPERATIONS

2.1 Proxies. The Client can authorise one/more persons ("Proxies") to perform Cash Desk operations or online operations using Online B@nking/Mobile B@nking in its Current, deposit, savings accounts, either by the Specimen signature enclosed to the Application or Online B@nking/Mobile B@nking Application, or by means of a separate power of attorney authenticated by a Notary Public/consular offices (in case of power of attorney issued abroad, they must be apostilled/authenticated, as applicable, and if they are prepared in a foreign language, their notarised Romanian translation must also be submitted). The Client will submit all documents requested by the Bank for the identification of the Proxy and will notify the Bank immediately, in writing, with regard to the termination or substitution of a Proxy, the Specimen signature/power of attorney being valid until termination/substitution.

2.2 Statement of account. a) The statement of account issued by the Bank is complete evidence of transactions performed in the Client's account and of the balance of account and is valid without the stamp or authorised signature of the Bank. Information related to each collection/payment/settlement made in/from the Client's account (reference, operation value, currency, fees, interest/interest rate, exchange rate, Currency date for the credit/debit of the account) are made available to the Client in the statement of account. "INSTANT" transactions carried out on Saturdays, Sundays and national and / or legal holidays related to the end of the month will be recorded in the statement of account corresponding to the next calendar month; **b)** The Bank ensures the free communication of the monthly account statement in one of the following ways: (i) by e-mail, (ii) in the Online B@nking application, in electronic format, (iii) in any of the Bank's branches, on paper, at the Client's request. The Bank ensures the communication of the monthly account statement by Post, on paper in which case it owes the fee mentioned in the Annex. Also, throughout the Contract, the Client will be able to view: (i) through Online B@nking, the history of all transactions performed in the account, starting with 01.01.2015 and (ii) in Mobile B@nking, the history of all transactions performed in the account for at most 1 year ago. The Bank is exonerated from liability for any deficiencies and / or errors that may occur in the process of sending account statements, according to the Client's option; **c)** The statement of account is the means of communication/method with which the Bank sends to the Client the mandatory information and notifications required by the law (including, without being limited to any amendment occurred with regard to the interest rate); **d)** the Client must check the information in the statement of account.

2.3 "Statement of Fees" a) The Bank shall provide to the Client, at its request, in the Bank's branches, free of charge at least once a year, with a statement of all fees incurred during a previous 12-month period and, as the case may be, information on the interest rate applied on the overdraft on the Payment account and the total amount of interest charged on the overdraft over the previous

12-month period, as the case may be, and the credit rate applied to the amounts available in the Payment account and the total amount of interest accrued over the previous 12-month period, as the case may be; **b)** The Statement of Fees represents the manner in which the Bank shall provide to the Client the mandatory information on fees and information on the interest rate referred to above, as required by Law no. 258/2017 on the comparability of charges for payment accounts, the change of payment accounts and access to Payment account with basic services; **c)** The "Statement of Fees" document may be communicated to the Client, at its request, by any of the means agreed jointly with the Client.

2.4 Account operations with the acceptance/as per the Client's instructions

2.4.1 Collection instructions. (1) For processing purposes, the following information must be received cumulatively by the Bank: **a)** sole identification code necessary for the correct performance of the collection ("Sole identification code"), consisting of: i) account number opened by the Client with the Bank or the IBAN code and ii) the identification code of the Bank (BIC/ SWIFT) – BACXROBU; **b)** complete information regarding the payer: name, account number/IBAN and address, which can be substituted with the date and place of birth, the identification number of the payer or national identity number.

(2) The Bank charges, from the transferred funds, the value of fees/commissions related to the collection, prior to crediting the Client's account with the respective amount. The Bank will indicate separately the total value of the payment operation and the charged fees.

(3) Throughout the Agreement, the Bank accepts collections and deposits of cash in the Client's payment account, including from third parties, the Bank not being responsible for these operations. Cash deposits made in the Client's account will be credited and remunerated with the corresponding interest coefficient in the deposit day. Cash deposits made in a non-business day are processed in the following Business Day.

2.4.2 Sending money/payment instructions. (1) For processing purposes, all of the following conditions must be met: **a)** the instructions shall be indicated d by the Client correctly, completely, clearly and unequivocally, on the forms made available by the Bank in its local units or by various means of communication (e.g., phone, Online B@nking, Mobile B@nking) according to Special Conditions; **b)** the balance of account is sufficient to perform the payment, respectively covers both the value of payments and of the related fees, and is not made unavailable; **c)** the Client provided the Bank with the sole identification code, consisting of: i) the account number of the payment beneficiary or the related IBAN account and ii) the identification code of the payment beneficiary (BIC/ SWIFT/ Routing Code). The provision of the BIC code is not mandatory for: (i) EUR payments to beneficiaries in the European Union [EU] or from European Economic Area [EEA] and (ii) payments in RON to a bank in Romania.

(2) Details entered by the Client in the Payment Order, with regard to the use of money, are solely with regard to the payment beneficiary and are not intended for the Bank.

2.5 Execution deadlines and Currency Date. a) The Bank will make sure that, after having received the payment order, the amount of the payment operation is debited from the Client's account and credited to the account of the payment service provider of the payment beneficiary at the latest on the dates specified under art.13.10, depending on the limit hour of receipt of the instruction, the currency of the operation and the type of credit transfer.

b) the Bank credits the Current Account of the Client with the funds collected immediately as they are credited in the Bank's account, in case that: (i) there is no currency conversion, (ii) there is a currency conversion between EUR and a currency of a EU and EEA Member State or between two currencies of EU and EEA Member States. The currency date used for the credit of the account cannot be later than the Business Day when the amount in the scope of the payment operation is credited in the Bank account.

2.6 Interbank payment operations (collection of amounts from the account opened with another service provider – interbank collections/ sending money–interbank payments) will be performed according to the instructions in the payment message and the GCU provisions. If the currency for the credit/debit is different from the currency of the Client's account indicated for collection/payment, the Bank is authorised expressly to convert the amount of the payment operation according to the exchange rate set by the Bank on the date of performance of the Operation (crediting/debiting) in/from the Client's account, so that the amount received/paid by the Client is credited/debited into the account indicated in the payment operation, according to the GCU.

2.7 Standing orders. (1) The Client may instruct the Bank (by filling in the Standing order form) to perform automatically intra- or interbank payments from its account, on pre-set dates, regardless of the currency in which the account of nominated, indicating: **(i)** the payment amount, fixed or variable, **(ii)** the date of debiting the account and frequency of payments and **(iii)** the period for which the activation is requested. The Standing order can be initiated by the filling of the form both in a branch office of the Bank (the option is available until 01.12.2020), and via Online B@nking & Mobile B@nking. The fees owed for the opening/amending/closing of a Standing order is debited automatically from the Client's account in the moment of opening/amending/closing, as applicable. **(2)** Through Mobile B@nking, intrabank and interbank payments can be made only in RON currency, the Client having the possibility to modify or cancel them according to the options available in the mobile application. **(3)** For the instruction of a sending money - payment operation at predefined deadlines, the Client must enter in the mobile banking application the following informations: debit account, details about the beneficiary, payment details (amount, payment frequency, start date, end date). **(4)** The editing of a sending money - payment at predefined deadlines in Online B@nking / Mobile B@nking must be made with at least one working day before the execution

of the payment.

2.8 Authorisation of payment operations. Receipt. Revocation. (1) In order to perform the Client's instruction, the payment operation must be authorised prior to its execution, respectively the Client expressed its consent for the performance of the respective payment operation, in the form agreed by the Bank. In the absence of such consent, a payment operation is considered unauthorised.
The consent consists of: **a)** for operations on paper support – the handwritten signature of the Client/proxy/authorised person for the account, according to the Specimen signatures; **b)** for operations ordered by various means of communication (fax, phone, etc.), as well as for operations ordered by other Payment Instruments (Online-B@nking, Mobile B@nking, BNA, card etc.) – according to the related special directives.
(2) The Client can withdraw its consent at any time until the receipt of the Payment Order by the Bank. The consent expressed for the performance of multiple payment operations can be withdrawn (i) in writing or (ii) by other means of communication, according to the related special directives, and all future payment operations will be considered unauthorised. The withdrawal of consent comes into force on the Business Day following the day when the Bank receives the cancellation.
(3) The Client cannot revoke a payment order after the said order has been received by the Bank. If the Client and the Bank agreed that the performance of the Payment Order commences on a subsequent date, the Client can revoke the Payment Order until the end of the public hours in the Business Day prior to the day agreed for the debiting of funds.
(4) In case the Payment Operation is initiated by means of a third-party Provider of payment initiation services or by or through the beneficiary of the payment , the Client cannot revoke the Payment Order after giving the consent to the third-party Payment Initiation Service Provider to initiate the Payment Operation or after giving the consent to the beneficiary of the payment to perform the Payment Operation. As an exception, in case of direct debit, without prejudice to repayment rights, the Client can revoke the Payment Order until the end of the working program with the public in the Business Day prior to the day agreed for the debiting of funds, at the latest.
(5) The payment operation can also be revoked subsequently to deadlines under para. (3) and (4), if possible, and if the Bank and Client expressly agree to that end in writing. The circumstance specified under para. (4) also requires the express agreement of the payment beneficiary.

2.9 Acceptance and performance of Client instructions. (1) For each Payment Order, in the moment of receipt, the Bank issues a reference which allows the identification of the payment order.
(2) The moment of receipt represents the moment when the bank comes in the possession of the Payment Order, sent directly by the Client or indirectly by or by means of a payment beneficiary. The stamp of the Bank applied on the Payment Order does not represent acceptance for execution purposes, but only confirms the receipt of the said Order by the Bank.
(3) In case the Client and the Bank agreed that the performance of the Payment Order commences on a subsequent date (in a particular day/at the end of a particular period/in the day when the Client made funds available to the Bank), the moment of receipt is considered in the agreed day; in case the agreed day is not a Business Day, the Payment Order is considered received in the following Business Day.
(4) For any instructions received following the limit hours, as well as in a day that is not a business day for the Bank, the payment Order is considered received in the following Business Day. If a foreign currency exchange order is received after the limit hours, the exchange rate used will be the first exchange rate valid in the following Business Day. Sending money - intrabank payments in LEI made through Online B@nking and Mobile B@nking are executed and recorded as follows:
(i) for those carried out with the “INSTANT” option on Saturdays, Sundays and national and / or legal holidays, the time limits referred to in Article 13.10 do not apply, they may be initiated 24/7 and executed on the day of receipt, except those of utilities to suppliers who are partners of the Bank, which cannot be performed during those days; “INSTANT” payments during this period will be recorded in the account statement for the next Business Day with the Currency Date on the day of receipt; (ii) for those carried out with the “INSTANT” option, during the period Monday - Friday, the time limits referred to in Article 13.10 do not apply, they may be initiated 24/7 and executed on the day of receipt, except for those of utilities to suppliers who are partners of the Bank, which cannot be performed on Friday between 23:00-23:59; payments made during this period, but between 23:00-23:59 and only by exception between 22:00-23:59 will be recorded in the account statement for the next Business Day with the Currency date the next calendar day; (iii) standard payments initiated in Online B@nking and Mobile B@nking on Saturdays, Sundays and national and / or legal holidays with the Currency Date of the next Business Day are executed and will be recorded in the account statement for that day.
(5) Reprinted payment orders will have the same contents as the original payment orders, applying the same provisions of the GCU.
(6) According to the Law, differences generated by rounding resulting following the transactions in any currency are dealt with as follows: (i) for operations related to interest, rounding is performed at two decimals; (ii) for fees, rounding is performed to an integer. They will be covered by the Client.
(7) The Bank is entitled to ignore the request for cancellation of a foreign currency exchange if the original transaction has been performed on the basis of negotiations agreed with the Client by means of a recorded telephone conversation or based on a written instruction of the Client.
(8) In case of sending money - intrabank payments in LEI made with the “INSTANT” option through Online B@nking and Mobile

B@nking, the date of debiting the paying account and the date of crediting the beneficiary account can be identified in the transaction details, in the section “Data procesare/ Request Processing Date”.

2.10 Notification of the Client by the Bank with regard to the refusal to execute Payment Orders. In case the Bank refuses to execute a Payment Order or initiate a Payment Operation (including those ordered by Online B@nking, Mobile B@nking and BNA) it makes available to the Client/User, at the Bank offices or via INFO Centre/Online B@nking/Mobile B@nking, as applicable, the notification for refusal, and, if possible, the reasons for such refusal, in the extent that this is not prohibited by the law, as well as the method to remedy any factual error which led to such refusal. In case the Bank's refusal to execute is justified objectively, respectively any of the conditions specified by the Agreement for the processing of the Payment Order is not observed, the Payment Order will be considered as not received.

2.11 Blocking payment instruments. (1) The Bank is entitled to block the payment instrument or the access thereto for reasons justified objectively, related to: **a)** security of the payment instrument, **b)** a suspicion of unauthorised or fraudulent use thereof, **c)** in case of a payment instrument with access to a credit line, with a significant increase of the risk that the payer is unable to observe the payment obligation.
Under such circumstances, the Bank notifies the Client/User by phone or by electronic communication (Online B@nking, Mobile B@nking, e-mail, SMS etc.), inclusively with regard to the reasons of such blockage, of possible, prior to blocking and, at the latest, immediately after blockage. The Bank is not under the obligation of providing any notification if this generates prejudice to safety reasons justified objectively or it is prohibited by other relevant legislative directives.
The Bank unblocks the Payment Instrument or replaces it with a new Payment Instrument, as the case may be, once the reasons for blocking cease to exist.
(2) The Client/ User can request the blocking/unblocking of Payment Instruments/Security elements **a)** by phone, via the INFO Centre, at any time, or **b)** in writing, directly at the bank offices, during the working program with the public or **c)** by accessing the dedicated menu within the Online B@nking **and** can request at any time the temporary blocking of the cards attached to the Mobile B@nking service by accessing the dedicated menu in the application. The Bank will make available to the Client/User, on demand, evidence of registration of its request for a period of 18 months following the date of such request. The Client understands and agrees with the final blocking of the card, physical or virtual, in case of his initiation of a refusal to pay, in case of suspicion of fraud, and the card can be replaced at the express request of the Client.

2.12 Collections/payments in any currency from/to abroad or on the territory of Romania in foreign currency
Corresponding Banks with account relationship are credit institutions with direct access to international settlement systems, where the Bank maintains a NOSTRO account and which mediate for the Bank the international transfers of funds in foreign currency. Intermediary banks are credit institutions, other than the Bank or the Corresponding bank with account relationship, involved in the settlement of foreign currency funds. The beneficiary Bank is the credit institution identified in the credit transfer instruction as bank of the intended addressee of transferred funds. The ordering Bank is the credit institution identified in the credit transfer-payment instruction as bank of the release authority of the transferred funds.
(1) With regard to payments in any foreign currency abroad or on the territory of Romania in foreign currency, the Bank will direct the payment operations instructed by the Client by: (i) payment systems provided by the law or, where applicable, (ii) settlement channels where it is connected or the network of corresponding Banks with account relationships.
(2) The Bank does not undertake any responsibility with regard to collections/transfers or credit - payments in any foreign currency from/to abroad or on the territory of Romania in foreign currency in the following circumstances: **a)** suspension of payments, moratorium upon payments, sequestration of the amounts of money, blocking or delay by the corresponding Banks with account relationship, by the intermediary Banks or by authorities in their countries; **b)** if the beneficiary refuses to collect; **c)** the absence of information necessary to process the operation. In case that the Bank, in good faith, relying on the payment message sent by the payer's provider of payment services, credited the Client's account with the amount corresponding to the collection operation and intervene any of the circumstances mentioned above, it is entitled to debit the Client's account with the credited amount and, if the credit balance of the Client's account does not cover this amount, to perform foreign currency exchange according to the Bank's exchange rate of the respective day.
(3) In case of operations performed by means of a corresponding bank with account relationship, the Bank will not be responsible if: **(i)** the instructions sent to this bank are not observed due to reasons not imputable to the Bank, **(ii)** in case of delay in the receipt of credit instructions from instructing banks due to legal holidays, the external banking circuit or by any other reasons not imputable to the Bank; **(iii)** the loss of results from the foreign currency exchange performed by the intermediary/beneficiary bank, with the application of regulations from the respective countries.
(4) The Bank performs banking operations by means of SWIFT (Society for Worldwide Interbank Financial Telecommunication), registered in Belgium. The SWIFT network operates through its servers in Europe and the United States of America (USA), which stores temporarily all data of the payment operation (including personal data). The operational centre in the USA is subject to the American Law, and the US Treasury Department is entitled to request access to personal data stored in the SWIFT operational centre in the US, for specific and limited purposes, respectively only to prevent money laundering and counter the funding of terrorism.

Thus, the US Treasury Department can collect personal data of Bank Clients who order payment operations and are processed via SWIFT.

(5) In connection with payments in any currency performed abroad and / or on the territory of Romania in foreign currency, the Bank may at any time, for justified reasons, deactivate / limit / suspend, temporarily or permanently, the specific functionalities of the services offered to Clients and that allow the initiation of such payments.

(6) In the case of transfer operations, such as online payment via 3D Secure, performed by the Client by accesing the "Add money" functionality in Mobile B@nking, if the Client initiate the payment refusal and, following the investigation carried out by the issuing bank of the card, it is confirmed that the refusal to pay is justified, the Bank is authorised by the Client to recover, at any time, the amounts credited in advance to Client's account, representing the value of the transaction made with the card, by authorised debit of any account opened with the Bank, no matter the account's currency, without notification or fulfilment of another prior formality and to make foreign currency exchange at the exchange rate of the Bank on that day, if applicable.

2.13 Notification and correction of Payment Operations that are unauthorised or performed incorrectly. The Client may obtain, according to the directives of the GCU, the correction of a payment operation that is unauthorised or performed incorrectly, inclusively in case that this payment is initiated by means of a third-party payment initiation service provider, only if it notifies to the Bank, without undue delay, not later than 13 months following the debit date, the fact that it found such an operation leading to complaints. The 13-month period is not applicable when the Bank failed to observe its obligation to provide or make available information related to this payment operation according to the provisions of the Agreement. The Client may request the correction of payment operations that are unauthorised or performed incorrectly **a)** by phone, via the INFO Centre, at any time or **b)** in writing, directly at Bank offices, during the working program with the public or **c)** by accessing the dedicated menu within the Online B@nking application.

2.14 Bank responsibility towards the payer Client for unauthorised payment operations. In case of unauthorised payment operations, including in case it had been initiated by means of a third-party provider of payment initiation services, with regard to which Client responsibility is not applicable according to art.2.15, the Bank: (i) returns to the Client the value of the respective unauthorised payment operation immediately or at the latest at the end of the next Business Day, after having found or being notified with regard to art. 2.13, unless there are reasonable causes to suspect fraud, (ii) if applicable, it restores the debited payment account to the state in which it would have been had the unauthorised payment operation not taken place, (iii) it makes sure that the Foreign Currency date of crediting the payment account is not subsequent to the date when the amount is debited. The Bank responsibility in case of unauthorised payment operations is limited to the specifications herein.

In case the Bank credited the account of the Client and subsequently it finds that there were the conditions required to involve the responsibility of the Client, it shall debit the Client's account with the value of amounts returned to the Client. The Bank is authorised by the Client to compensate automatically, at any time, the amounts owed to the Bank according to the Agreement, with the funds available in any account opened with the Bank, regardless of the currency of the account, without any notification of prior formality and, in case of compensation between the accounts with different currencies, to perform the foreign exchange according to the exchange rate of the Bank in the respective day.

2.15 Responsibility of the Payer Client for unauthorised payment operations.

(1) In case the Client acted fraudulently, it shall bear all consequences arising out of the unauthorised payment operation.

(2) If the Client did not act fraudulently, it shall not bear any financial consequences arising out of the use of a payment instrument that is lost, stolen or used without permission in any of the following circumstances: a) loss, theft or unauthorised use of a payment instrument could not be detected by the payer prior to the making of a payment; b) the loss had been caused by an action or by the absence of action from the Bank or Bank employees or Bank proxies; c) following the notification of the Bank with regard to the loss, theft, unauthorised use of the payment instrument/ customised security elements, performed according to the provisions of the Agreement; d) in case that the Bank does not request strict authentication of the Client; e) should the Bank fail to make available the means specified in the Agreement to allow notification at any time of a payment instrument that is lost, stolen or used without permission.

(3) In other circumstances than those under para. 1 and 2 of the above, the Client shall cover all losses related to any unauthorised payment operation if such losses are generated by the payer following the intentional disregard or due to gross negligence of one or more obligations regarding: a) the implementation of all reasonable measures for the safe keeping of customised security elements b) notification of the Bank without undue delay, as soon as it acknowledges the loss, theft, unauthorised use of its payment instrument or any other unauthorised use thereof.

(4) **In circumstances other than those mentioned under para. 1, 2 and 3 above,** the Client shall cover, up to a quantum of maximum EUR 30 or RON equivalent of this amount on the date of performance of the unauthorised transaction, losses related to any unauthorised payment operation arising out of the use of a payment instruments that is lost or stolen or by the unauthorised use thereof, in case the Client did not act fraudulently and did not infringe intentionally its obligations on a) taking all reasonable measures for the safekeeping of customised security elements b) notification of the Bank without undue delay as soon as it becomes aware of the loss, theft, unauthorised use of its payment instrument or by any unauthorised use thereof.

2.16 Return of payment operations initiated by or by means of the payment beneficiary. (1) The provisions of the present article apply according to the law only for the Payment operations performed within the EU and the EEA, in any currency, if both the payer's provider of payment services and that of the payment beneficiary or the single provider of payment services in the Payment Operation are on the territory of the EU and EEA.
(2) Within 10 Business Days following the receipt of a request for return of an authorised payment operation initiated by or by means of a payment beneficiary (inclusively in case of direct debit operations), the Bank can return the entire amount related to the payment operation or may justify the refusal to return the amount, according to the law. The return consists in the total value of the performed payment operation. The foreign currency date of the credit operation of the Client's payment account is not subsequent to the date when the amount had been debited.
(3) The Client is not entitled to any return in case that it expressed its consent to execute the Payment Operation directly to the Bank and, if necessary, the information on the future payment operations has been sent/made available to the Payer Client in the agreed form, at least 4 weeks prior to the due date, by the Bank or by the payment beneficiary.

2.17 Incorrect sole identification codes. According to the law, the Bank is responsible for the performance of the payment operation exclusively based on the sole identification code provided by the Client according to the Agreement, regardless of the other additional information received by the Bank (regarding the payer, Client, transaction etc.). If the sole identification code provided by the Client for the performance of a payment order is incorrect, the Bank is not responsible for the non-performance or faulty performance of the payment operation, however it will take, in exchange of the related fee, all reasonable efforts for the recovery of funds involved in the payment operation.
In case it is not possible to recover the funds, the Bank provides to the payer Client, based on a written application, all information available and that is relevant, in order to allow it to initiate legal actions in order to recover the funds.

2.18 Bank responsibility for the non-performance or faulty or delayed performance of payment operations. (1) The provisions of the present article apply according to the law only for the Payment operations performed within the EU and the EEA, in any currency, if both the payer's provider of payment services and that of the payment beneficiary or the single provider of payment services in the Payment Operation are on the territory of the EU and EEA.
(2) In case of the payment order initiated by the Client, the Bank can be responsible towards the Client for the correct performance within the deadlines specified in the GCU of the payment operation, only if the Client observed its obligations correctly and completely. Under such circumstances, the Bank **a)** returns to the payer Client, without delay, the amount in the scope of the non-performed payment operation (in case the Client's payment account has been debited, however the Bank did not credit the account of the payment services provider of the payment beneficiary) or performed incorrectly and, if applicable, restores the debited payment account to the condition in which it would have been had the incorrect payment operation not taken place; or
b) immediately makes available to the client - payment beneficiary, the amount in the scope of the payment operation and, if applicable, credits the corresponding amount in its payment account.
The foreign currency date of the Payment account of the Client that is the payer/beneficiary of the payment will not be subsequent to the date when the amounts would have had the foreign currency date had the Operation been performed correctly.
(3) The Bank responsibility is excluded if it can be proven to the Payer Client and, if applicable, to the Provider of payment services of the payment beneficiary, that the latter (the beneficiary's service provider) received the amount in the scope of the payment operation within the performance deadlines specified in the GCU.
(4) In case that a payment order is initiated by the Client, beneficiary of the payment, or by means of it, the Bank is responsible towards the Client for the correct transmission of the Payment Order to the payment service provider of the payer within the deadlines of performance specified in the GCU. The value of the payment operation is made available to the Client immediately as this amount is credited in the Bank Account. In case of delayed performance of the Payment Operation, the Bank resubmits immediately the respective Payment Order to the payer's provider of payment services, the Bank resubmits immediately the respective Payment Order to the payer's provider of payment services, the amount having as currency date in the payment account of the beneficiary client at the latest the date when the amount would have had the currency date had the operation been performed correctly.
(5) In case of a payment operation not performed or performed incorrectly where the payment order is initiated by the Client payer/beneficiary of the payment or by means of it, the Bank takes, on demand, immediate efforts, regardless of its responsibility according to the present article, to identify and monitor the payment operation and notifies the Client with regard to results.
(6) Also, the Bank is responsible for potential fees and interests applied to the Client as a result of the non-performance or faulty performance (including delayed performance) of the payment operation.

2.19 The Bank will be held responsible only in the extent and in the circumstances specified by the law and by the Agreement. The Bank will not be held responsible for the default of any obligation specified in the Agreement, if the performance of such obligation would result in the default of a normative act in force. The Bank responsibility does not occur in case it acts on the basis of legal provisions.
The Bank will not be held responsible: **(i)** if the Client cannot access a product/service due to reasons outside the responsibility of the Bank (e.g., interruption or incorrect operation of any means of communication or faults of data processing/transmission systems); **(ii)**

messages/information/payment instructions received by the Bank or by the service provider of the payment beneficiary is incomplete, incorrect for any reason not imputable to the Bank, inclusively due to the interruption or incorrect operation of any means of communication.

2.20 Abnormal and unforeseeable circumstances. The responsibility provided in the Agreement does not apply to abnormal and unforeseeable circumstances, outside the control of the party that claims them, including technical deficiencies that render it impossible to provide the contracted service, with consequences which could not have been avoided despite all efforts taken to that end. Under such circumstances, the deadlines for the performance of obligations are postponed accordingly. The parties will take the necessary efforts to decrease the effects generated by such event.

2.21 Frozen accounts. The Bank is entitled to perform operations in the Client's accounts (including, without being limited to foreign currency operations) without the Client's permission, in the following circumstances: **(i)** on the basis of a writ of execution; **(ii)** in case of garnishment or sequestration ordered according to the law, on the basis of a document issued by competent authorities, proceeding to the blocking of accounts; **(iii)** any other circumstances specified by the law. In any of these circumstances, the Bank will be entitled to debit/credit the Client's account with the respective amounts (including the related interest).
In case of freezing the balance of an account, the blocked amounts can be transferred by the Bank in a special account available to the enforcement authority only in case they are at least equal to the amounts mentioned in the writ of execution/document issued by the competent authorities and the fees related to the payment and/or in case it had been ordered to suspend the forced execution. Should the current account not be open in the currency in which payment must be made according to the writ of execution, the Bank is entitled to open one or more special accounts according to
the currencies in which this payment must be made. As a result of this operation, the rest of availabilities will remain in the Client's accounts and can be used by the Client. The amounts frozen on the basis of a writ of execution do not bear any interest.
Throughout the period when the account balance is frozen, , the Bank will make available to the Client, according to the law, the amounts collected as salary, pension, daily allowance, alimony etc. (the "agreed amounts"), as follows: (i) at the Bank desks, in the currency of the account, and for the amounts agreed in RON, the Bank will open automatically to the Client an account where it will transfer the respective amounts that will be made available to the Client and (ii) at the Bank terminals (ATM, BNA), within the limit of maximum RON 2,000, by means of a code generated automatically by the Bank and sent to the Client by SMS, hereinafter referred to as "the garnishment bar code", in case it does not have an active debit card, physical or virtual, or (iii) by means of the active debit card, physical, and to that end the Bank will attach automatically the active debit card to this account. In this account, the Client cannot deposit/collect amounts of money, as it is intended exclusively for the Bank to make available the due amounts subsequent to the establishment of the garnishment. After the cancellation of garnishment, the Bank will automatically: (a) transfer the availabilities existing in this account to the current account of the Client, (b) will enclose the debit card, physical or virtual, to the current account and (c) will close the account intended exclusively to the making available of amounts due, after 90 calendar days following the moment when the last transaction had been registered in this account.

2.22 Refusal of payment operations. The Bank is entitled to deny the collection of amounts in the accounts of the Client and/or perform the transactions ordered by the Client/Proxy if: **(i)** the information requested and provided by the Client is illegible, incomplete or incorrect, or there are no sufficient funds for such transaction, including the case of garnishment or freezing of the Account **(ii)** the Client does not make available to the Bank, upon its demand, whenever the Bank deems necessary, any documents and/or statements considered necessary to justify the operations performed by the Bank and/or to determine the real circumstances of the Client, including, without being limited to the appropriate identification of the Client, inspection of the beneficiary's identity and/or origin of funds; **(iii)** the operation is not according to the applicable laws (including foreign currency regulations in force), bank regulations and practices or the Client used the current account for illegal purposes or the Bank has suspicions of fraud o with regard to the purpose or nature of the transaction (e.g., the operation is connected to transactions for the funding of terrorism or money laundering), payment operations involve goods, persons, territories with regard to which Sanctions are ordered and/or other reasons with objective justification or in accordance with the applicable legal directives; **(iv)** the payment operation is performed through/towards countries with which the Bank does not cooperate, according to the legal provisions or regulations and policies of the Bank; **(v)** the written explanations on the nature of the ordered transaction use foul language; **(vi)** the Bank has suspicions with regard to the accuracy of those declared by the Client/of the documents provided by the Client.

2.23 The Bank is entitled to block the Payment Instruments, to suspend totally or partially, temporarily or permanently or to deactivate the service/product/feature immediately without prior notification and/or terminate the present Agreement, in the circumstances specified under art. 2.22, para. (ii)-(vi).

2.24 In order to reverse erroneous operations, as well as those specified as “under reserve” (with supporting documents enclosed in excerpt), the Bank is entitled to perform operations in the Client's accounts (including, without being limited to foreign exchange operations), without the Client's permission.

CHAPTER 3. BANK RELATIONSHIP RULES

3.1 The Client has all the rights and obligations specified by the Agreement and by the law and is responsible for the default of obligations undertaken by the execution of the Agreement. The Client must use the contracted service/product according to the provisions of the Agreement and of the law. The Client will send clear, complete, unequivocal and accurate instructions for the performance of operations and is responsible for the observance of the procedures of transmission of information according to the Agreement.

3.2 The Client shall not request the closure of accounts specified for the automated debiting of fees, taxes and other costs of the provided product/service, until the payment of all amounts owed according to the Agreement.

3.3 The Client will make available to the Bank, upon its request, any documents and/or statements, in the form and content agreed by the Bank, considered necessary for the performance of the Agreement and justification of operations performed through the Bank, determination of the real circumstances of the Client. Any document issues by a foreign authority must meet the authentication/apostille conditions according to the law. The Bank is entitled to request the Client to confirm the instructions sent according to the Agreement, as a precaution and prior to execution, by the same means of communication of by different means of communication, on the Client's expense, depending on the nature of the existing situation.

3.4 The Client will take all **measures necessary for the protection of Payment instruments, Security elements, barecode, garnishment bar code and MCash code** against theft/damage/loss/fraudulent use, including, without being limited to **a)** safekeeping and not to alienate/disclose/communicate them to any other person, allow the use by third parties; **b)** memorise security elements instead of writing them down on media that would allow it to be recognised and used by unauthorised persons and, if necessary, destroy the envelope with which the Bank sent the Payment Instruments/Security Elements; **c)** make sure that, when entering/using them, no one can see them; **d)** in case of setting/changing, a Security Element must not be chose to be easily associated with the name/date of birth/phone number etc. The Bank is not responsible for potential debiting of the account caused by the disregard of such measures.

3.5 The Client **will notify the Bank immediately** in case of finding that it is in one of the following circumstances with regard to the Payment Instruments/Security Elements/mobile phones for the installation of applications provided according to the Agreement: **a)** loss, theft, damage, destruction, blocking; **b)** unlawful use, any unauthorised, fraudulent use, respectively the registration in the personal account of unauthorised transactions; **c)** any error, irregularity occurred as a result of the account management by the Bank; **d)** if there are any suspicions with regard to the possibility of them becoming known to unauthorised persons, inclusively in case that the envelope with the Payment Instruments/Security Elements has been handed unsealed; **e)** finding of the occurrence of dysfunctions, including the circumstances where the Security Elements are incorrect; **f)** the renewed card is not received (for the physical cards), was not displayed in Mobile B@nking for the virtual ones. To that end, the Client undertakes to contact INFO Centre immediately, in order to request the blocking/cancellation/change of Payment Instruments/Security Elements. Upon the request of the Bank, such request must also be confirmed in writing, in one of its local branch offices. The moment of blocking the reported Payment Instruments/Security Elements is determined according to the time zone of Romania. Blocking is final, and the Bank will not be held responsible for the consequences of such blocking, including in case the Client generated damage to third parties by blocking them. In case the blocked payment instruments/Security Elements are found, the Client undertakes to return them to the Bank for destruction purposes, otherwise the Bank is not considered responsible.
The Client / User is obliged to immediately cancel the MCash code from the Mobile B@nking application, as soon as he has become aware of any of the situations provided in 3.5, letters (a) - (d), the Bank not being liable for damages resulting from such situations of violation of the obligations incumbent exclusively on the Client/User.

3.6 The Client must not use, otherwise it shall bear any and all of the related consequences, Payment Instruments/Security Elements to purchase goods prohibited by the Romanian Law or of any other country where the respective payment instruments is used or from where the goods originate.

3.7 The Client is under the obligation to notify the Proxies and the Users which, upon its demand, represent it in the relationship with the Bank, with regard to provisions of the Agreement, as they are equally binding upon them. The Client is responsible for the use of products/services by the Proxies/Users, all operations being binding upon the Client, who covers potential generated damages. The Client undertakes to notify the Bank with regard to any cancellation/amendment of any of the rights granted to the Proxies/Users, as they are binding upon the Bank, solely after the filling in of the specific form made available by the Bank.

3.8 The Client shall settle directly with the service/utility provider any potential litigations arising out of incorrect/delayed or undue payments, the Bank being exonerated from any responsibility, including with regard to delay penalties owed by the Client. The Bank is not responsible in case of partial or late payment of invoice values.

3.9 Unsuccessful attempts to connect by means of payment instruments trigger various blocking mechanisms to ensure security. In

case of remote payment instruments, the failure to use the specific applications/devices within a period pre-set by the Bank shall lead to the expiry of the session, requiring a new authentication.
The Client must (i) check periodically security warnings and information on Online B@nking, Mobile B@nking, BNA which the Bank publishes on the Internet/Online B@nking/Mobile B@nking page and (ii) develop at the sites where such services are used security measures intended to decrease any attempts of unauthorised access. The Client must ensure that, when using a mobile phone to access the bank products/services, the functions of the device that allow the detection thereof are deactivated. The Bank is not under the obligation of providing hardware or software services for the Client, except for Mobile Token, for which it provides software services.

In case of Online B@nking, if the URL (Uniform Resource Locator) address of the log-in page displayed in the web browser does not start with a series of characters "https://" or the "locked padlock" icon, to indicate a secure connection, is not present, the Client must leave urgently the accessed web page and notify the Bank immediately with regard to this incident by means of the INFO Centre.

3.10 The Bank will notify the Client with regard to any amendment occurred in the performance procedures of Online B@nking/Mobile B@nking/ BNA, other than the contractual amendments, by displaying them on the Bank/Online B@nking web page.

3.11 The Bank is entitled to foreclose any goods belonging to the client in order to recover the amounts owed according to the Agreement.

3.12 (1) the Bank/any other member of UniCredit Group can take any action considered appropriate to ensure, anywhere in the world, the observance of obligations related to the prevention and countering of fraud, money laundering, funding of terrorism, bribery, corruption, tax evasion and those related to the provision of services to some persons who can be subject to Sanctions. It may include, without being limited to the investigation and interception of payments made to and from the Client's account, investigation of the source of funds/their beneficiary, investigations to determine whether a person is subject to Sanctions. The performance of such actions by the Bank can lead to the delay/shutdown of execution of payment instructions or collection of the amounts/settlement of transactions but, in the extent possible, the Bank will notify the Client with regard to the reasons that determined these delays or shut down and with regard to the estimated duration of any delay.
(2) The Client will make immediately available to the Bank all documents, information, means of identification requested, in the manner and form determined by the Bank, with regard to: **(a)** changes related to any Proxies/Users (which may include their personal identification) or the written confirmation related to the non-occurrence of changes with regard to information and its status, **(b)** periodical update of information related to Client, financial position, beneficial owners and the Group of entities which includes them, if relevant, **(c)** information provided in advance with regard to any third party, beneficiary of payments.

3.13 Your personal data will be processed according to the conditions of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and the free circulation of such data, repealing Directive 95/46/EC ("Regulation") in order to perform the Agreement, observe legal obligations, as well as for legitimate purposes (e.g., prevention of fraud, execution of internal reports, application of customer review measures according to the applicable legislation etc.).
The Bank provides the security standards with regard to the processing of Personal Data according to art. 32 of the Regulation, by the taking and application of all appropriate technical and operational measures to protect Personal Data against any accidental or illegal destruction, loss, amendment, disclosure or unauthorised access and against illegal processing.
The Client has been notified with regard to the processing of its Personal Data (including the rights in the Regulation and the method of exercise), by the Notification Report enclosed hereto.

3.14 The Bank has the following obligations: (i) perform Payment Operations in the Client's Account, according to the Agreement, and allow the performance of operations in the Account by Proxies only within the limits of the mandate granted them by the Client; **(ii)** upon the Client's demand, the Bank will notify, prior to the performance of an individual Payment Operation, with regard to: (a) the maximum period of execution, (b) the value of related fees and (c) their separation, if applicable; **(iii)** to execute the Client's instructions within a reasonable period, according to the nature of the ordered transaction and to the provisions of the Law and Agreement; **(iv)** execute the orders for the purchase and sale of foreign currency according to the legislation in force. The year will be considered 360 days for all currencies traded by the Bank, except for GBP and PLN, with regard to which the year will be considered as 365 days; **(v)** make available to the Client, upon its express request, records related to transactions performed by means of a means of electronic payment [debit card, physical or virtual, remote access payment instruments], including the statements of account, on paper support, at their residence and/or at the Bank offices and/or by any other means of electronic remote communication (e.g., Online B@nking, Mobile B@nking, e-mail or SMS), within 72 hours following the date of receipt of the request.

CHAPTER 4. COSTS

4.1 (1) The Bank charges interest, fees, duties, taxes and, as applicable, provides interest rates according to the legislation in force and the Annex of fees and commissions. Information on the interest rate/exchange rate is displayed at the local Bank offices and on the web page in the dedicated section. Any foreign exchange shall be performed according to the exchange rate of the Bank on the day when the account is debited.
(2) For payment operations by credit transfer, performed within the EU and EEA, in any currency, if both the payer's provider of payment services and that of the beneficiary of the payment or the single provider of payment services within the Payment Operation is on the territory of the EU and EEA, the beneficiary of the payment covers the price charged by its service provider, and the payer covers the price of its provider of payment services (shared charging principle "SHA"- the principles of fees covered by each separate party).
(3) For the payment operations by credit transfer performed outside the EU and EEA, in any currency, the Client can choose to apply one of the following rules for fees: a) SHA; b) OUR – where all fees are paid by the payer, c) BEN – where all fees are paid by the payment beneficiary. Should the Client fail to indicate the fee charging rule by methods specific to the payment instrument, the Bank will process the payment operation using the SHA fee payment rule.
(4) If the following conditions are cumulatively met: (i) there are no transactions on the Client's account (s), including through the use of the debit card, for a period of 6 consecutive months (except for fees and commissions charged by the Bank) and (ii) the balance of the account is zero or less than zero, the monhly current account(s), attached debit card (s), as well as the Online Banking monthlyadministration feeswill no longer be charged. The fees will have the value 0 (zero) starting with the month following the one in which the two conditions are cumulatively fulfilled. The Client is entitled in arrears for the amounts owed to the Bank and due at the fulfillment of the previously mentioned term, these being still due and owed to the Bank until their full payment. Starting with the month from which, following the operations on the Client's account(s), the account balance becomes positive, the monthly current account/s administration fee, the fee for the provision (administration) of the debit card, as well as the Online Banking monthly administration fee, will have the value specified in the Fees and Commissions Annex.

4.2 The costs payable in other currency than that expressed in the Annex will be calculated and charged using the Bank exchange rate valid on the date of debiting the account, related to the performed operation, except for costs related to foreign currency payments that will be calculated and charged using the NBR exchange rate valid on the date of debiting the account, related to the performed operation.

4.3 The Bank provides interest for the availability in the accounts, respectively charges interest for unauthorised overdraft, during the existence of the debit, the interest being calculated according to the following formula: d = S x no. of days/360 x r %, where: **d** = interest; **S** = the amount registered in the credit or debit balance, as applicable; **r** = interest rate.

4.4 The amendment of the interest rate/exchange rate is applicable immediately and without any prior notification if (i) the amendment is more beneficial to the Client or (ii) is based on the rate of reference interest or according to the reference exchange rate generated by a verifiable public source (e.g., EURIBOR, ROBOR, the exchange rate published by the NBR or by Visa/MasterCard international card organisations).

4.5 The Bank is authorised by the Client to compensate automatically, at any time, the amounts owed to the Bank according to the Agreement, with the funds available in any account opened with the Bank, regardless of the currency of the account, without any notification of prior formality and, in case of compensation between the accounts with different currencies, to perform the foreign exchange according to the exchange rate of the Bank in the respective day.

4.6 The Bank is entitled to debit the Client's accounts with the amounts representing taxes and/or duties related to the operations/documents ordered/received from/for the Client. Should this not be possible, the Bank is entitled to discontinue the operation and return the documents. All costs covered by the bank, including without being limited to judicial and extra-judicial expenses, in case it is involved in a litigation with the Client and/or between the Client and a third party, will be recovered from the Client.

II.SPECIAL PROVISIONS

In addition to the General Provosions and Final Provisions, the following special provisions apply to each contracted product/service:

CHAPTER 5. SPECIAL PROVISIONS ON THE DEBIT CARD

5.1 Rules of use. (1) The debit card is a payment instrument, available in physical (in plastic format) as well as virtual (without a plastic format), which allows the Client to use the monetary availabilities existing in a current account. The physical or virtual debit card can be used by the Client, in Romania and abroad, on the basis of one/some of the Security Elements: PIN code (a personal identification number) for the physical card, card number, name on the card, expiry date, CVV/CVC (a code representing the 3 digits written on the card, which in case of the physical card can be found on the back side of the card, used to confirm authenticity of

data related to the card, sent during the performance of transactions), as well as, in case of websites with that support 3D Secure, security elements mentioned in art. 5.10, par. (3). The physical debit card incorporates the contactless technology, a technology that allows the authorisation of payments, using radio waves, by the mere approach of the card to the POS/other terminals that display the Visa PayWave logo and/or MasterCard PayPass. The debit card can be activated through Mobile Bnking, by calling the Info Center or can be set up through the Bank's ATMs and BNAs. Activation or deactivation of the contactless option can also be requested by the Client by calling Info Centre or at the Bank ATMs or BNAs.
In the sens of the present Contract, if not otherwise mentioned by using "Card/Debit Card", depending on context, it means both the physical and virtual debit card.
(2) The physical debit card can be used for the following payment operations and the Client's consent for their authorisation is performed by strict Authentication, as follows: (i) using the PIN Code for: a) payment of goods and services to retailers via POS, b) cash withdrawal from marked locations (ATMs, BNAs, bank office desks etc.) with identical logo (icon) to that on the card, c) performance of transactions by means of a CAT-type device (offers cash, goods or services and allows the performance of transactions without the need for the physical presence of a representative of the retailer), by inserting the card in the device for reading and sending information related thereto, d) procurement of information on the balance of the account attached to the card from ATMs and BNAs of the Bank/other special devices of the Bank/from the ATMs of other banks that allow this, e) performance of Cash Back transactions at the POS (offers cash withdrawals of maximum RON 150, concurrently with the performance of a payment transaction by card to a retailer, either at a UniCredit Bank POS, or at the POS of another bank that allows such transaction), f) performance of Quasi-Cash/Unique transactions (transactions by card to retailers in order to obtain goods convertible into cash, including without being limited to casino chips, lottery tickets); or (ii) using details mentioned under art. 5.10, in case the processing the payment for CNP transactions (transactions performed without the physical presence of the card) on the Internet on website which support 3D Secure.
(3) The virtual debit card can be accessed through Mobile B@nking and can be used for the following Payment actions and the Client consent for authorization is made through Strict Authentication, as follows: (i) in case the Client chose to enrol the card in Apple Pay/Google Pay, as well as by introducing the phone's PIN code, or scanning the print/FaceID set on the mobile device, for a) internet payments payment of goods and serices at merchants through POS b) Cash Back type of transaction performed at the POS (offers cash withdrawals of maximum RON 150, concurrently with the performance of a payment transaction by card to a retailer, either at a UniCredit Bank POS, or at the POS of another bank that allows such transaction),; c) Quasi-Cash type/Unique type of transactions (transaction made with the card at a merchant in order to obtain goods convertiblele in cash, such as casino chips, lottery tickets); or (ii) using the details mentioned in art. 5.10 in the case of CNP transactions (transactions made without the physical presence of the card on the Internet) on sites that support 3D Secure.
The virtual debit card cannot be used for cash withdrawals or balance inquiries from / at marked locations (ATMs, BNAs, bank office desks, etc.), nor for making transactions through a CAT type device (offers cash, goods or services and allows the performance of transactions without the need for the physical presence of a representative of the retailer).
(4) In case of CNP transactions on the Internet, performed at retailers on websites which do not support 3D Secure, the Client's consent for the authorisation of payment operations shall be taken by providing the card number, name indicated on the card, expiry date and CVV/CVC. This type of consent will only be given for: **(i)** payments at retailers outside the UE and EEA, regardless of amount; and **(ii)** for payments with retailers in the UE and EEA, with an individual value of less than EUR 30, and the cumulated value of such consecutive payments does not exceed EUR 100.
(5) The debit card, both physical and virtual, can also be used by means of: **(i)** the Apple Pay digital platform , made available by Apple Distribution International Limited, according to its technical characteristics and of the used device, according to the terms and conditions published on the website https://www.apple.com/apple-pay/ both for the performance of operations specified under para. (2), sub-para. (i), subsections a) and e) and para. (3), sub—para (i), subsection a) and b) above, for those made online at Apple Pay merchant partners, as well as for the payment of goods and services of minor value (value established by Visa or MasterCard international card organisations and displayed permanently on the Bank website) at a POS/terminal with contactless functionality, without the need to use the PIN code and/or sign the receipt related to the transaction, **(ii)** The Google Pay Service, provided by Google Ireland Limited, for the performance of the operations specified under para. (2), sub-para. (i), subsections a) and e) and para. (3), sub—para (i), subsection a) and b) above, as well as for those made online at GooglePay merchant partners by Mobile B@nking users, who have registered their card / cards in Google Pay, and the mobile device used for payment has Android operating system, NFC function ("Near Field Communication") enabled and compatible technical features, according to the terms and conditions of Google Pay, posted on https://pay.google.com.
(iii) In order to authorize the payment via Apple Pay/ Google Pay, the Client / User will select the card registered in Apple Pay / Google Pay that he wishes to use when making the payment or will use the card already set as the first payment option, will unlock the Apple Pay / Google Pay compatible mobile device by entering / using the set security element (PIN, fingerprint, face recognition or other data required in the process of registering cards in Apple Pay / Google Pay) and by approaching the merchant's POS in case of transactions made at these terminals.
In the case of the Google Pay Service, if payments are made with a physical card at the merchant's POS, the Client/ User will be able to authorize the payment withintroducing / using the security element necessary to unlock the mobile device according to the provisions of para. (6) below, as well as if the number of consecutive contactless transactions made since the last unlocking of the device is not more than 3 (three). In case of of payments done using a virtual card at merchant's POS, the Client/ User will be able

to authorize the payment by introducing / using the security element necessary to unlock the mobile device.
In the case of the Apple Pay digital platform, the Customer / User will be able to authorize the payment without introducing / using the security element necessary to unlock the mobile device, according to the provisions presented on the Apple website - https://developer.apple.com/support/sca/
The rules and conditions for using the 3D Secure e-commerce service specified under art. 5.10 are applied also for payments made on Internet via Apple Pay / Google Pay Service, on sites that support 3D Secure to Apple Pay / Google Pay partner merchants.
In the case of Internet transactions made with merchants on sites that do not support 3D Secure, the consent of the Client / User for the authorization of payment transactions will be made by entering the security element set, according to the above.
(6) For the payment of goods and services of small value (value established by Visa or MasterCard international card organisations and displayed permanently on the Bank website) at a POS/terminal with contactless functionality, the Client's consent for the authorisation of payment operations will be given by approaching the POS/terminal with the physical card, without the need to enter the PIN code and/or sign the receipt related to the transaction. However, the introduction of the PIN code will be necessary after each cumulation of consecutive contactless transactions with a value of more than EUR 150 or equivalent. The calculation of this limit shall not include the contactless transactions performed from an unassisted terminal in the European Economic Area in order to pay for transportation tickets or parking fees as well as those made at a POS/terminal with contactless functionality outside the European Economic Area.
(7) The consent of the Client for the payment of goods and services at retailers by means of Imprinter for the physica card will be expressed by signing the receipt and for the performance of CNP transactions, which can be performed on by mail/phone (MOTO transactions, which can be performed exclusively in case of an agreement with the Client), providing the card data, for the physical and virtual card,and the details requested by the retailer.
(8) There is no need for authorisation from the Client to the Bank **(i)** for recurrent transactions, in case of observance of the following conditions: **a)** for the initial transaction performed on the Internet related to recurring operations, the Client expressed its consent according to the present Agreement, and **b)** the recurring operations have the same beneficiary and are of the same value; and **(ii)** transactions performed as a result of the authorisation given by the Client directly to the retailer, by filling in the related form on its website or by other means, in order to debit the accounts attached to the card, for the payment of particular goods or services, according to the authorisation given to the retailer.
(9) The physical and virtual card shall remain the property of the Bank and can be used only by the Client; the Client cannot transfer it to another person and cannot use it as collateral. The physical card can be returned to the Bank on demand of the Bank or following the withholding by retailers/ATMs/special devices of the Bank.
(10) The daily usage limit and the maximum number of transactions/day are established in the Annex. The Client can request the amendment of the limits of use for determined periods, for both the virtual and physical card: **(i)** by calling the INFO Centre; **(ii)** by means of the Online B@nking; **(iii)** by means of the Mobile B@nking service; or **(iv)** in writing, directly at the Bank offices. The limits can be amended only with the express approval of the Bank. For security reasons and in order to avoid fraud, the Bank can limit the number, value of transactions and number of unsuccessful transaction attempts which can be made with a card in a calendar period (day, week, month) without the prior notification of the Client. The Bank is not responsible for the limitations of any kind applied by a third-party acceptor.

5.2 Validity. Renewal. The physical and virtual card is valid for the period mentioned on the front of the card, until the last day of the month of expiry. In case of renewal of the card, the conditions in force in the moment of renewal shall apply, including costs as specified in the Annex signed/communicated to the Client on Durable medium upon the renewal of the card. The Bank can decide not to renew the card if in the past 12 (twelve) calendar months prior to the expiry of the card there are no transactions with the card and the Account Holder does not request the Bank in writing the renewal of the card, at least two months prior to the expiry date of the card.

5.3 Debiting. a) Debiting of the Client accounts, in the order indicated by the Client, with the value of transactions made with the card shall be within maximum 30 days following the date of transaction. In case the balance of the first account indicated by the Client is not sufficient, the difference will be debited from the following accounts indicated by the Client in the Application. For debit card applications registered starting with 1 August 2019, a single current account will be attachable to the debit card, physical or virtual, and the value of card transactions will be debited from the only attached account.
b) The Bank is entitled to debit automatically the accounts of the Client with the amount of the respective transactions and in case the Client made transactions via the phone/e-mail (MOTO) which involved the card or used the card number in a way that did not generate a receipt, but involved the account in the respective transaction.

5.4 Recurring transaction. (1) The recurring transaction is a transaction performed as a result of the authorisation given by the Client directly to the retailer, by filling in the form on its website or by other means, in order to debit the accounts enclosed to the card on particular periods, for the payment of particular goods or services according to the authorisation of the retailer.
(2) For recurring transactions, the Client has the following obligations: **(i)** in case of replacement of the card regardless of reason, notify the retailer with regard to the data related to the new card so that the recurring transaction is not interrupted, the Client being the only one responsible for the recurring transactions related to the new card; **(ii)** request the retailer to withdraw the granted

consent, in case that these transactions must be eliminated for the respective retailer.
(3) The Bank is not responsible to the Client or the retailer with regard to the effects of the legal relationship between them, being a third party with regard to the contractual relationship (including with regard to the payment method) between the Client and the retailer, as well as in case that the Client cannot purchase the goods/services offered by the retailer by means of a recurring transaction due to insufficient funds or as a result of the default of obligations specified in the previous paragraph.

5.5 Settlement currency. (1) The currency for the settlement of transactions performed with Visa and MasterCard is:
(i) RON for transactions with receipts issued in RON and
(ii) EUR for transactions with receipts issued in a currency other than RON. In case of on-line and offline transactions, receipt will mean the retailer's display of the value of the transaction, in the stage prior to the completion of the transaction, on its website. In case of transactions done with debit cards attached to accounts with a different currency than LEI/EUR, regardless if it is done in the same currency as the attached account, the settlement will be done using a double currency exchange, according to the mentiones from para. (2) below that might lead to a high amount being settled from the account than the transaction one.
(2) The exchange rate existing on the date of transaction authorization may differ from the exchange rate applied on the settlement date of the transaction, therefore the amount withheld from the Client's account on the transaction authorization date may be different from the debited on the settlement date. For international transactions that are not in Euro, International Card Organizations exchange between the original transaction currency made with the card and the settlement currency, at the exchange rate established by the Card Organization on the settlement date of the transaction, to which is added the Bank's monetary conversion commission. Debiting, from the current account attached to the card, physical or virtual, of the value of the operation performed with the card, is made by foreign exchange between the value of the transaction in the settlement currency and its equivalent value in the currency of the current account, using the Bank's exchange rate. The exchange rate applied by the Bank for international card operations (or national in a currency other than the account) is available on www.unicredit.ro.
(3) In order to ensure the comparability of the total monetary conversion fees applied by the Bank, in the case of transactions in the European Union (EU) either in euro or in a national currency of a Member State other than the euro, which involves a foreign exchange, the Bank displays daily on www.unicredit.ro the total monetary conversion fees as a percentage addition to those most recent Euro reference exchange rates published by the ECB (European Central Bank). From 19 April 2021, for online and offline payments made by card in the EU denominated in any EU currency other than the account, Customers will receive each month in which the Bank receives a payment order denominated in the same currency, a single push electronic information message in the Mobile B @ nking application or an SMS message, regarding the exchange rate applied by the Bank when settling transactions. This message will be received by the Customer after the Bank receives the first payment order for a cash withdrawal at an ATM or a point-of-sale payment that is denominated in any EU currency other than the payer's account currency, free of charge, and for the modification of the electronic channel for receiving the notification or giving it up, it is necessary to contact the Bank by the Client by calling * 2020, the Info Center service available 24h / 7.

5.6 Supplementary card. a) A natural person ("User") can have access to the availabilities in the Client's account by means of a supplementary card, based on the express consent of the Client expressed in the Application or in another form agreed by the Bank. The Bank will not issue a virtual supplementary card. **b)** The provisions of the Agreement apply exactly to the user holder of an additional physical card. The Bank can cancel, block temporarily or definitively the supplementary card upon the demand of the Client in the circumstances specified in the present Agreement, without the prior notification or agreement of the User. The Client can limit the use of the supplementary card to a particular threshold (fixed amount) and for a particular period of time. The Client is not entitled to know the PIN code of the User. **c)** The Bank does not undertake any responsibility for the damages generated by the User to the Client. The Client and User are jointly responsible for the use of the supplementary card and the damages generated to the Bank or the third parties of this use. **d)** Throughout the Agreement, the expiry date of the supplementary card can be different from the expiry date of the main card. **e)** The Bank will register the transactions performed with the supplementary card on the current account of the Client without the need for any express and prior approval from the Client.

5.7 The Client has the following rights: (i) by means of the card, it has permanent access to the personal account; and **(ii)** to request the Bank, immediately, without any undue delays, the initiation of the procedure for the denial of payment for a particular operation, should it find the registration on its account or card transactions which it did not order/perform, in whole or in part, as well as any other errors of other nature. The payment denial shall be performed by the filling in and deposit at one of the local units of the Bank of a typical form of application for payment denial, accompanied by supporting documents, as applicable, or by the supplementation of an electronic form by means of Online B@nking, if this service is purchased. The Bank can request additional information in order to be able to investigate and settle the application for the denial of payment for transactions not acknowledged by the Client. Payment denials will be settled according to the rules of international card organisations and general practice for the use of the card. The process of recovering the disputed amounts, through chargeback process can take between 30 calendar days and maximum 180 calendar days. This deadline does not affect the provisions of article 2.14. If the Bank obtains documents in the chargeback process, confirming that the transaction was carried out by the cardholder in accordance with the terms and conditions of the merchant and that there is no reason to return the disputed amount, the refusal to pay is considered unjustified, in which case the Client owes the fee specified in the Annex.

5.8 The Client has the following obligations: (a) upon the release of the physical card and, if applicable, of other Security Elements of the physical card, to sign for confirmation of their receipt; **(b)** to sign the physical card immediately after receipt, in the special area on the back side of the card; **(c)** after the expiry, hand over the physical card to the Bank; **(d)** to use the card only within the limits of the amounts available in the current account; in case the performed transactions exceed the balance available in the account, the amounts are considered unauthorised overdraft.

5.9 Should the client want to close the accounts attached to the debit card, the card must be returned to the Bank 30 days prior to the closure of the accounts, and the virtual card must be closed from the Mobile B@nking app, branch or Info Center. Upon the termination of the debit card, physical or virtual, relationship: **(i)** all cards are cancelled, regardless of their expiry date, the Client/User being forced to return the physical ones; and **(ii)** the Client must regulate/pay any debts related to the card when they become due and provide the Bank with collateral for the payments made until the termination date, but which will be debited subsequently, as well as for banking expenses related to such debts.

5.10 Rules and conditions for the use of the 3D Secure electronic commerce service. (1) All cards, physical or virtual, issued by the Bank are enrolled in3D Secure service, which provides the possibility to perform electronic commerce transactions in strict security conditions. The 3D Secure Service is made available by the Bank by means of ROMCARD S.A., data processor with secured means (under the Verified by Visa and MasterCard Secure Code brand names) with the observance of the present rules and terms of use ("Rules"). The 3D Secure Service works provided that the website of the transaction supports the 3D Secure standards. Any amendment of the Rules will be notified on the Bank's website. Transactions performed by 3D Secure are under the incidence of the version in force of the Rules, in the moment when they are performed. Rules are available on the Bank website.
(2) the Bank, Visa International and MasterCard reserve the right to: **(i)** amend, improve or interrupt the provision of this service without prior notification; **(ii)** suspend at any time access to this service if it becomes proven that personal data are false, inaccurate, not up to date or incomplete; and **(iii)** deactivate the access to this service temporarily/permanently. In such circumstances, responsibility with regard to transactions already performed shall not change.
(3) The Consent of the Client for the authorisation of Internet payment operations via 3D Secure is made by by strict authentication, providing the card number, the name indicated on the card, the expiration date, CVV / CVC as well as the Security elements mentioned in the following paragraphs.
(4) If the Client/User has Mobile B@nking active/ Mobile Token active for Online B@nking, the consent of the client for the authorisation of Internet payment operations via 3D Secure shall be performed by strict authentication, as follows: **(a)** in case the Client did not activate the option to accept notifications of the "push message" type on the mobile phone (in cse of Mobile B@nking and Mobile Token) and in the application (only in case of Mobile B@nking), it shall access Mobile B@nking or Mobile Token and will authorise the respective payment operation by entering the PIN Code or by scanning the fingerprint / facial features set in the mobile phone, in case the Client selected these features, and **(b)** in case the Client activated the option to receive "push message" notifications on the mobile phone (in case of Mobile B@nking and Mobile Token) and in the application (only in case of Mobile B@nking), it will receive a message to include the details of the payment (e.g., the amount of the payment operation, the payment currency and the name of the beneficiary etc.) being redirected to Mobile B@nking/Mobile Token and will authorise the respective payment operation by entering the PIN code or by scanning the fingerprint / facial features set in the mobile phone, if the Client activated this option.
(5) Clients without any of the above services active will authorise Internet payment operations via 3D Secure by the use of: (i) a single code generated by the Bank for each payment operation and sent to the Client via SMS, at the mobile phone number declared to the Bank (the phone number must be registered with Romanian mobile operators), and (ii) the static password, as established in the application related to the supply and use of the card.
(6) By way of exception to the rules for strict authentication of payments, the Bank may agree, without obligation, on the basis of a real-time risk analysis carried out by the Bank or the merchant's bank, not to request the security features referred to in paragraph 4 or (5), the consent for the payment authorization being made by providing the card number, the name indicated on the card, the expiration date and the CVV / CVC code, following the merchant's instructions.
(7) The payment operation will not be authorised and the card will be blocked for Internet payment Operations, in the extent that the Client does not manage to provide authorisation after **(i)** five consecutive attempts, respectively: (a) three consecutive attempts to enter the PIN code, by Mobile B@nking/ Mobile Token, when Mobile B@nking/Mobile Token will no longer be accessible, being necessary to reactivate it afterwards (b) two consecutive attempts by the use of the unique code and of the static password, if there was a prior attempt of authorisation by Mobile B@nking/ Mobile Token or **(ii)** five consecutive attempts with the use of the sole code and static password, unless there was a prior attempt of authorisation by Mobile B@nking/ Mobile Token.
(8) **The 3D Secure Client/User has the following obligations: (i)** it shall read the Rules carefully; **(ii)** it shall not disclose, in any form, to virtual retailers or third parties its personal data or Security Elements; **(iii)** in case it is considered that the confidentiality of its data has been compromised (card number, expiry date, ID Digits, single code associated to each transaction) will notify immediately the Bank in order to block the Bank until the settlement of the situation, or will temporary or definitely block the card by using the functionality available in Online B@nking or Mobile B@nking; **(iv)** will notify the Bank immediately with regard to any amendment of its data; **(v)** will notify the Bank immediately with regard to any change of the phone number declared to the Bank, by calling the INFO Centre or by visiting any branch office of the Bank;
(vi) prior to the provision of any identification data for the performance of a payment, will check the authenticity of the payment website, checking as a minimum: (a) the display of the logos related to Verified by Visa and MasterCard Secure Code services; (b)

security certificates of the pages that require such data;(c) the display of prompt messages related to 3D Secure.
(9) **the 3D Secure Client/User is prohibited to: a)** substitute another person/entity which uses 3D Secure; **b)** send in any way virus programmes to interrupt, destroy or limit the functionality of any hard/soft component (including communications) of 3D Secure; **c)** send spam messages, in any way and invasion of the accessed Verified by Visa and MasterCard Secure Code websites; **d)** amendment, adaptation, decompilation or disassembly, sub-licensing, translation, sale of any portion of 3D Secure; **e)** erasure of any notification related to title (copyright, trademark) encountered by the access to 3D Secure; **f)** use of any means to retrieve or reproduce the navigation structure, presentation and contents of websites that display the brand names Verified by Visa and MasterCard Secure Code; **g)** interruption of other users' access to 3D Secure, servers or networks connected thereto; **h)** default of Rules and specific 3D Secure procedures in general or of any network connected thereto; **i)** intentional or unintentional default of any local, national, international regulations or of the rules and requirements established by Visa International and MasterCard for the use of 3D Secure.
(10) **The Client/User** is notified and agrees that: **(i)** 3D Secure contains information protected by the intellectual property right law and other applicable laws; **(ii)** the Bank will provide a non-exclusive licence to use 3D Secure and the 3D Secure mechanisms in the current form and the improvements to be added from time to time according to the Rules; **(iii)** will not copy, alter or use in any way the trademarks of the Bank (owned by the Bank), 3D Secure (property of Visa International and MasterCard International) or the logos, products and names associated to this service; **(iv)** has complete freedom to purchase goods/services from the Internet by accessing 3D Secure. However, correspondence with selected retailers, participation in on-line promotions, payment and delivery of purchased goods/services, any other conditions and warranties associated thereto are only within the scope of its relationship with the retailer; **(v)** the use of 3D Secure does not mean in any way whatsoever that the Bank, Visa International or MasterCard recommend any on-line retailer or warrant the quality of their goods/services; **(vi)** any litigation with regard to the default by the retailer of payment conditions, delivery, quality of goods/services purchased can be settled exclusively between the Client/User and the retailer; **(vii)** it is recommended to collect as much information on the retailer as possible and on the performed transaction, saving the terms of delivery, details of the transaction, correspondence with the retailer on the PC etc.
(11) **Responsibility**. a) the 3D Secure Client/User is responsible for the maintenance of confidentiality of Security Elements.
b) The Bank is nor responsible for: **(i)** the amendment, suspension or any interruption in the provision of 3D Secure due to reasons independent of the will of the Bank; **(ii)** defects of the computer or in the provision of telephony services occurred during the on-line transactions; **(iii)** potential damages generated by the equipment used during transactions becoming infected with viruses; **(iv)** compromise of identification data as a result of the default of rules; **(v)** transmission of the SMS message including the single code associated with each transaction to a phone number which is no longer valid and/or which has not been updated by the Client; **(vi)** the Bank, Visa International, Mastercard, are not responsible for any potential damages occurred following the direct relationships between the Client/User and the retailers or caused by the default of regulations of 3D Secure Regulations.

CHAPTER 6. SPECIAL PROVISIONS ON THE SAVINGS ACCOUNT

6.1 The savings account is the account which includes the funds necessary for savings and can be established in RON, EUR or USD.

6.2 The savings accounts can include the following operations: **(a)** cash deposits; **(b)** cash withdrawals; **(c)** sending money – intrabank payments from the Savings account in any account opened by the Client with the Bank.

6.3 Interest is specified in the Application and displayed at the local Bank offices and on the website. In case the interest is granted as a ratio of the deposited amounts (payments), the amount in excess of the limit of each payment is applied the interest rate corresponding to the immediately following payment. Interest will be calculated with regard to the daily balance of the Savings Account and, depending on the mentions specified in the application, it will be transferred on a monthly basis in the Current Account or it will be capitalised in the Savings Account.

CHAPTER 7. SPECIAL PROVISIONS ON TERM DEPOSIT ACCOUNT OPERATIONS

7.1 Instructions related to operations. (1) The Client can perform operations (opening, liquidation) in term deposit accounts based on instructions sent to the Bank as per the present Chapter. For term deposits opening, the Client will be able to send instructions to the Bank, according to the template provided by the Bank and made available in its local units, by Online B@nking, Mobile B@nking. The provisions of the GCU are applicable to each instruction. The Client must enter in all fields/options available on the form of instructions, including the amount of the deposit ("Original amount"), the currency of the deposit, the period of the deposit, the interest rate, its option with regard to automated extension, in the extent that such option exists, and capitalisation of interest etc.
(2) For the opening of the term deposit, the Original Amount is debited by the Bank from the current/savings account indicated in the instruction ("Original account") and credited in the deposit account opened automatically by the Bank depending on the currency of the deposit. The Bank is exonerated from the opening of the deposit in case the value of the balance existing in the Original Account is less than the Original Amount mentioned in the instruction for the opening of the deposit. The original account must be

maintained throughout the duration of the deposit.
(3) Upon the opening/restoration on the due date of a deposit, the Bank establishes minimum amounts (the "Minimum amount") depending on its currency. The minimum amount necessary for the opening of a deposit is mentioned in the instruction form, at the local offices of the Bank and on the website.

7.2 In the extent that the offer of the Bank for deposits, valid on the date of transmission by the Client of instructions for the opening of the deposit, there is an option to open deposits without automated extension and the Client, by means of the instruction sent to the Bank, requested the opening of such deposit, upon the maturity of the deposit, the initial Amount and the related interest will be credited in the Original Account.

7.3 In the extent that the offer of the Bank for deposits, valid on the date of transmission by the Client of instructions for the establishment of the deposit, there is an option to establish deposits with automated extension and the Client, by means of the instruction sent to the Bank, requested the opening of such deposit, consideration will be given to the following: (1) Extension is performed for a period equal to the original period, unless specified otherwise in the form of instructions. Upon maturity, the original amount and the related interest will be credited in the Original Account. For the deposits with the possibility to capitalise the interest, the deposit is re-established from the Original Account, with the Original Amount and the related interest. For the deposits without the option to capitalise on interest, the deposit is restored in the original account, only with the Original amount, the related interest remaining available in the Original Account.
(2) In case the Client registers debts of any sort on the Original Account, the deposit will be extended with the balance left following the recovery of debts, in the circumstances that this balance is at least equal to the Minimum Amount in force on the date of extension. Otherwise, the deposit will not be extended, and the balance remains available in the Original Account and will be subject to the Current Account terms and conditions of the Bank, in force on the date of the respective transfer.
(3) The waiver of the option for automated extension must be notified to the Bank until the extension date, at the latest.

7.4 The **Interest Rate** can be fixed (expressed as a fixed percentage) or variable throughout the agreement and is displayed in the local Bank offices and/or on the Bank website. The level and type of the interest rate (fixed or variable) applicable to the term deposit are established in the instruction form. In case of deposits with automated extension, the Bank will provide the Client, during the period related to each extension, the deposit interest rate in force on the extension date, corresponding to the respective deposit category (the deposit category refers to the option of automated extension, capitalisation of interest, as well as the channel used for the transmission of the instruction), without any prior formalities of notification or acceptance and without the execution of an addendum. Thus, the Client understands and agrees that, on the date of extension of the deposit, the interest rate agreed originally by the instruction for the opening of the deposit can be amended, in the extent that the interest rate of the Bank on the date of extension for the respective category of deposit is different from the one originally agreed upon.

7.5 Early liquidation. In case of liquidation of the deposit prior to the expiry of the period for which it had been established, the Current Account interest of the Bank in the liquidation moment will be granted, applied to the Original Amount. As a result of the recalculation of the interest, the Bank will withhold automatically from the deposit potential interest differences paid in excess, if any.

7.6 In case the maturity date of the deposit is not a Business Day, the deposit will be considered due in the immediately following Business Day.

7.7 The Bank will make available to the Client, at the office, free of charge, information with regard to the operations performed in the deposit accounts, for a period of 30 days prior to the request. The document issued by the Bank is complete proof of operations performed in the deposit account and the balance of the account. The Client must check such information.

7.8 All deposits will be established automatically with the Currency Date of the day when they have been ordered, if they are received until the limit hour. The transactions ordered after the Limit Hours or in non-business days are processed in the following Business Day.

7.9 In case of deposits opened by BNA, evidence of receipt by the Bank of the instruction for the opening of the deposit is the receipt issued by the BNA with all details of the deposit (the amount of the deposit, interest, period, with or without automated extension, with or without capitalisation etc). Evidence of opening of the deposit is the statement of account and the receipt released by the BNA.

7.10 The Client is responsible for any fiscal/legal consequences arising out of the change of nature of this banking product. Any request for regularisation with regard to the taxes/duties withheld and paid for by the Bank for the Client shall be performed by the Client directly to the competent fiscal authority, the Bank being exonerated from any obligation

CHAPTER 8. SPECIAL PROVISIONS ON PAYMENT INSTRUMENTS WITH REMOTE ACCESS

8.0 GENERAL RULES. TERMS USED (arranged alphabetically).

Token device - Digipass. This is a secure device which allows access to Online B@nking. In case of inappropriate operation for reasons not imputable to the Client/User, it shall be replaced free of charge by the Bank. In case that the Client/User wants to replace the Token Device **-** Digipass for reasons including without being limited to the destruction, loss or theft thereof, the Client will cover the entire cost of a new Token device - Digipass.

The price for the Digipass device is mentioned in the "Annex".

Transaction limit. The initial transaction limit per day and/or per payment operation, related to a Client/User is established in the Annex of Fees and Commissions related to banking products. The limit can be amended following the application sent to the Bank (e.g., in local units of the Bank, Online B@nking or INFO Centre), only with the express approval of the Bank. The Bank is entitled, in observance of the legal provisions in force, to amend this limit, notifying the Client in this regard. In case of activation of the Mobile B@nking service via INFO Centre, the Bank will notify the Client with regard to an original trading limit.

Mobile Token. This is a secure electronic application which allows access to Online B@nking. Mobile Token can be downloaded from the link sent by the Bank by means of an SMS message, valid for 72 hours, installed on a compatible phone, depending on its technical characteristics. After installation, the Client/User will activate the application using: **(i)** user name; **(ii)** a configuration code sent by the bank by means of an SMS message valid for 72 hours; and **(iii)** elements that will allow subsequent access to the Mobile Token, respectively the PIN code or (b) scanning of the fingerprint set in the mobile phone or (c) scanning of the facial characteristics set in the mobile phone, reading of the digital fingerprint or facial recognition being performed by the technology specific to the mobile phone (the option is available for compatible mobile phones with iOS or Android operating system, depending on their technical characteristics).
Mobile Token cannot be accessed, and it must be reactivated in the following circumstances: **(i)** the Client/User entered in an erroneous manner for 3 consecutive times the following information: Configuration code or User name; **(ii)** the Client/User lost/had been stolen the mobile phone where the application was installed; **(iii)** technical reasons (e.g., malfunction of the device where the application is installed); (**iv)** the Client/User did not access the SMS messages and their validity expired; and **(v)** the Client/User forgot the PIN code. In such circumstances, the Client/User must contact INFO Centre/one of the local offices of the Bank to receive a new Configuration Code. The bank will provide the link for the download of the Mobile Token and the new Configuration Code within maximum 2 Business Days following the day of request.

Payment operations ordered from the credit card limit. Should the contracted service allow such payments, these will be applied the provisions in the credit card agreement executed with the Bank (related to costs, applicable interest, trading limit, grace period etc.), as follows: (i) for the ordering of payment to other accounts that the agreed Utility Providers, the provisions related to cash withdrawals are applicable and (ii) for the ordering of payments to the agreed Utility Providers, the provisions related to the transactions with the credit card at retailers are applicable.

Receipt and execution of instructions. A credit - payment transfer instruction is considered received by the Bank after the moment when the Client/User/last User, as applicable, authorised the operation (expressed its consent for execution). If the moment of receipt exceeds the Limit Hours, the payment order is considered received for the execution by the Bank in the following Business Day. Authorisation of a credit transfer - payment instruction does not represent acceptance for execution purposes, but only confirms the receipt of the said credit - payment Order by the Bank. The Bank will execute the credit - payment instructions received from the Client/User only in case that it had been identified correctly and completely and the conditions of the Agreement are observed for the performance of a payment operation.

User. The user is the natural person authorised expressly by the Client view or to perform bank operations on its accounts in Online B@nking/Mobile, according tot he rights granted by the Client, as follows: (i) the "View" rights, in wich case the User has the possibility to view the status of accounts, loans and debit/credit cards associated to the service/product contractedby Client and also can access a series of functionalities, according to the provisions of art. art 8.1.3(ii). and 8.2.2.1(ii) and (ii) the "Transfer and other banking operations" rights in wich case the User can make transfers to the Client's accounts and send other instructions regarding products and services, according to the provisions of art 8.1.3(ii). and 8.2.2.1(ii), having at the same time the "View" rights. The user receive from the Bank the Security Elements.

The Client has the possibility to view in Online B@nking/Mobile B@nking, as applicable, all operations initiated by the Users, including those denied by the Bank, as well as the reasons leading to denial.

Subsequent versions. The Bank can supplement/improve the characteristics, method of view/access and may include new functionalities of the Online B@nking/Mobile B@nking services, and the reversal to prior versions being impossible. The Client can be notified with regard to amendments via Mobile B@nking/Online B@nking/statement of account. The amendments in the benefit of the Client (including the extent of permitted operations, limits of operations considered security operations) can be applied immediately. If the Client considers that the new functionalities come against its interests, it will have the possibility to terminate the Agreement according to the provisions specified herein.

Viewing of accounts. Upon the activation of Online B@nking and Mobile B@nking services, they will make available all accounts existing in the moment of activation. Access to any account opened subsequently will be granted automatically account holders and to his authorized persons who are not UniCredit Bank customers on the date of his appointment as proxy.

8.1 ONLINE B@NKING SERVICE

8.1.1 Rules of use. (1) Online B@nking is an IT service which can be accessed by the Client/User by: **Mobile Token** or Token device – Digipass, depending on the selected authentication method. Token device - Digipass is only available to Customers who have opted for this method of authentication in Online B@nking until November 30, 2021.
(2) Online B@nking is accessed from the Bank's website, by means of the Strict authentication procedure consisting in the entering of the Security Elements by the Client/User: **(i)** User name - an alphanumeric code established in the Application and which cannot be amended subsequently to the signature of the Application and **(ii)** Security Code, generated by the Mobile Token or by Token device - Digipass, depending on the selected authentication method.
The Security Code is generated by the Token device - Digipass as a result of the introduction of a **PIN Code**
The security code is generated by the Mobile Token as a result of **(i)** introduction of a **PIN code** or **(ii)** in case that the Client chooses so, as a result of the scanning of the digital fingerprint set in the mobile phone or of the scanning of facial features set in the mobile phone, reading of the fingerprint and facial recognition being performed by the specific technology of the mobile phone. This option is available for the phones with compatible iOS and Android operating systems, depending on their technical characteristics.
The PIN code is a secret identification number selected and entered personally by the Client/User upon the activation of the Mobile Token or upon the first use of the Token Device - Digipass.
(3) The erroneous entering on three consecutive times of the (i) User name/Security code and, (ii) in case of the Token Device - Digipass and of the Mobile Token, of the PIN code, will determine the blocking of access to Online B@nking. For unlocking, the Client/User will contact: for situation (i) INFO Centre/one of the local units of the Bank and for situation (ii) one of the local units of the Bank.

8.1.2 By means of Online B@nking, the **Client** can access a series of functionalities:
(i) Information on the accounts, credits and debit, physical and/or virtual / credit cards associated to the service or notifications from the Bank.
(ii) instructions with regard to products/services: (a) sending money – intrabank and/or interbank payments, including Standing orders, in LEI and foreign currency and/or foreign exchange (the credit card can only be used for sending money - intrabank and/or interbank payment operations in RON); credit transfer operations - payments in RON can also be performed in emergency conditions, and the intrabanking in LEI can also be performed with the "INSTANT" option; **(b)** amendment of the transaction limit of debit, physical or virtual,and credit cards, **(c)** amendment of the priority of debiting the accounts attached to the physical or virtual debit card, **(d)** chargeback process initated for a debit and credit card payment, **(e)** opening of the term deposit account, opening and liquidation of term deposits, **(f)** activation of a direct debit order, including within the credit card limit, **(g)** the possibility to temporarily block the card (s) associated with the service and the possibility to return to the previous situation by unlocking from Online B@nking **(h)** the possibility to modify the security image; (i) transfer of payment services from any payment service provider located in Romania to UniCredit Bank (j) other instructions in case the Bank provides this possibility by means of the application.
(iii) requests for the management of **products/services: (a)** re-issue/replacement of the physical debit/credit debit/credit card and or of the related PIN code, **(b)** change of the maturity date and/or partial or total early return of the loans contracted with the Bank only in case the Client is the sole borrower within the loan agreement. The Client must visit one of the local offices of the bank to collect and sign the new repayment schedule. The new repayment schedule can also be viewed in Online B@nking, **(c)** amendment of data with regard to the mail address, phone number, e-mail address, employer and position, **(d)** amendment of the option expressed in the Application to receive the statement of account/activity report, **(e)** in case of the credit card, the activation of the repayment facility by automated debit, in the circumstances of the credit card agreement contracted with the Bank, **(f)** change of the authentication methodfrom Digipass to Mobile Token, , **(g)** other requests in case the Bank provides this possibility by means of the application.
(iv) requests to contract products/services: (a) savings account, **(b)** provision of a debit card **-** release of a physical debit card, **(c)**

current account in a currency different from the currency of current accounts already opened with the Bank, **(d)** Info SMS; **(e)** Mobile B@nking; **(f)** other products/services in case the Bank provides this possibility by means of the application.
The updated list of functionalities is available on www.unicredit.ro, as well as in any local office of the Bank.

8.1.3 By Online B@nking, the **User** has access to several functionalities, as follows**:**

(i) The User with the right to "Transfer and other banking operations" can view the status of accounts, loans and debit/credit card associated to the service, and can send instructions with regard to products/services: **(a)** sending money – intrabank and/or interbank payments, including Standing orders, in LEI and foreign currency and/or foreign exchange (the credit card can only be used for sending money - intrabank and/or interbank payment operations in RON); credit transfer operations - payments in RON can also be performed in emergency conditions, and the intrabanking in LEI can also be performed with the "INSTANT" option;, **(b)** amendment of the transaction limit of the debit, physical or virtual, and credit cards, **(c)** amendment of requesting a debit card and updating its delivery address, **(d)** application for the denial of payment performed with the debit and credit card, **(e)** opening and liquidation of term deposits, **(f)** opening saving accounts , **(g)** amendment of modify the method of receiving the activity report or the account statement (h) early repayment of the mortgage loans; (i) activation of direct debit order, inclusively within the credit card limit (j) change of the authentication method from Digipass to Mobile Token, **(k)** temporary blocking of cards (physical or virtual), as well as their unlocking, **(l)** enable e-mail notifications; **(m)** the possibility to modify the security image; **(n)** transfer of payment services from any payment service provider located in Romania to UniCredit Bank **(o)** other instructions in case the Bank provides this possibility by means of the application. **(p)** enable/disable marketing consent.

(ii) The User with "View" rights can view the status of accounts, loans and debit/credit card associated to the service, and can send instructions with regard to products/services: **(a)** temporary blocking of cards (plastics or virtual), as well as their unlocking; **(b)** enable e-mail notifications; **(c)** the possibility to modify the security image; **(d)** enable/disable marketing consent.

8.1.4 Authorisation of payment operations
(1) For the performance of operations, the Client/User must fill in the corresponding fields in the Online B@nking application. The consent of the Client for the authorisation of credit transfer operations - payment will be performed by strict authentication, as follows:
(i) by the manual introduction of a valid security code in the special field displayed. The security code can be generated, depending on the selected method of authentication, by the Token device - Digipass or by the Mobile as a result of entering the PIN code. The security code generated by the Token Device - Digipass or by Mobile Token is unique and correlated dynamically with particular elements of the payment operation. The generation of the code shall be performed after entering the transition values and details on the beneficiary (e.g., the last 6 digits of the its IBAN account).
(ii) or by the automated generation of a valid security code, as follows: users who activated the option to authorise transactions with the use of "push messages" (a message displayed directly on the screen of the mobile phone in Mobile Token) will receive a message to include the details of the payment (e.g., the amount of the payment operation, the beneficiary account, the name of the beneficiary, etc.), and for the automated generation of the Security Code the PIN code must be entered. For the completion of the payment operation, the Client must approve the completion of the operation on the page displayed to this effect in Online B@nking. This security code generated by the Mobile Token is unique and correlated dynamically with particular elements in the payment operation (e.g., value of the payment operation and the beneficiary of the payment).
(2) in case of payment operations between Client's accounts opened with the Bank, strict authentication is not required, the consent of the Client being expressed by the push of the "Pay now" button.

8.2 MOBILE B@NKING SERVICE

8.2.1 Rules of use. (1) Mobile B@nking is a secured application which involves an internet connection and allows the Client/User to manage accounts and perform transactions by means of a mobile phone according to the terms of the Agreement.
(2) Mobile B@nking can be downloaded and installed on a compatible mobile phone, with internet access, respectively with iOS (e.g., iPhone) and Android operating system depending on their technical characteristics, following the instructions in (i) the dedicated menu available in Online B@nking, (ii) the link sent by the Bank by means of an SMS message, (iii) specialised stores such as Apple Store (App Store) and Google Play Store. After installation, the Client will activate the application by entering **(i) User name**, an alphanumeric code established in the Application and which cannot be amended subsequently to the signature of the Application, **or the data requested by the Bank within the application** (e.g., particular digits of a physical debit or credit card issued by the Bank and/or particular digits in the ID Digits and/or other elements), **(ii) Configuration code**, valid for 72 hours, sent by the Bank (a) by means of an SMS message within maximum 2 Business Days following the date of contracting the service in a local office of the Bank/by the phone or (b) in the menu of Message in Online B@nking, if requested by means of this application and **(iii) PIN code,** a secret identification number defined and entered personally by the Client/User, which will allow subsequent access to Mobile B@nking.
(3) Mobile B@nking is accessed by strict authentication consisting of: **(i)** entering of the **PIN code or (ii)** in case that the Client

chooses so, by the scanning of the digital fingerprint set in the mobile phone or of the scanning of facial features set in the mobile phone, reading of the fingerprint and facial recognition being performed by the specific technology of the mobile phone. This option is available for the phones with compatible iOS or Android operating systems, depending on their technical characteristics.
(4) Mobile B@nking can no longer be accessed, and it must be reactivated in the following circumstances: **(i)** the Client/User entered in an erroneous manner for 3 consecutive times the following information: User name/Configuration code/PIN code; **(ii)** the Client/User lost/had been stolen the device where the application was installed; **(iii)** technical reasons (e.g., malfunction of the device where the application is installed); **(iv)** the Client/User did not access the configuration code sent via SMS and their validity expired; and **(v)** the Client/User forgot the PIN code. In such circumstances, the activation process specified under para. (2) will be resumed. To that end, the Client/User will contact the Bank: calling the INFO Centre/by means of a written application to one of the local offices of the Bank/by filling in the dedicated form in Online B@nking.
(5) The Bank may restrict or block the access to Mobile B@nking as a result of the non-updating of the application by the Client / User, justified by the existence of technical, operational, security or other reasons. Access to the application will be restored after updating the application with the version available in the Apple Store (App Store) or Google Play Store.
(5) Blocking access to Online B@nking (the erroneous entering for 3 consecutive times of the User name/Security code/security image selected by the Client/User) leads to the blocking of access to Mobile B@nking, which can be accessed only after unlocking access in Online B@nking.

8.2.2 By means of Mobile B@nking, the Client can access a series of functionalities:
(i) Information on the accounts, active deposits, credits and debit (physical and/or virtual) as well as credit cards associated to the service or notifications from the Bank.
(ii) instructions with regard to services: **(a)** sending money operations - intrabank and/or interbank payments in RON and foreign currency to accounts in IBAN format, standard and urgent, and the intrabanking in LEI can also be performed with the "INSTANT" option, **(b)** credit transfer operations - payments to agreed Utility Providers – by scanning the bar code or by the manual entering of the invoice details, **(c)** foreign exchange, **(d)** possibility of temporary blocking of cards, physical or virtual, associated to the service and possibility to return to the prior circumstances requesting unlocking, as well as the possibility to request the reissuing of the physical debit card and updating of the card's delivery address, **(e)** possibility to close a debit virtual card, **(f)** possibility to view the card data (card number/CVV/expiration date) and copy the card number - by using the authorization credentials used to access the Mobile B@nking **(g)** possibility to amend the daily transaction limit at the POS (or on the Internet) and of the daily limit for cash withdrawals at the ATM of the cards associated to the service, **(h)** possibility to activate physical debit/credit/meal cards issued on Client/User name, **(i)** foreign currency calculator and information on exchange rates, **(j)** map of ATM network/local offices of the Bank, **(k)** definition of payment templates to beneficiaries, which can be used subsequently for the performance of payments to them, **(l)** use of payment codes - represents QR codes that embed the details of a transfer/payment instruction. By scanning the payment code, the related details are entered automatically in the transfer/payment form in Mobile B@nking, without the need to enter other identification elements. Payment codes can be created/used/sent by any client using Mobile B@nking, **(m)** possibility to receive messages displayed in the Mobile B@nking application and which can be viewed when Mobile B@nking is accessed and PUSH messages, the latter representing messages displayed directly on the mobile phone screen, regardless of Mobile B@nking service being accessed or not at that moment; receipt of PUSH messages can be deactivated from the mobile phone settings or from the Mobile B@nking settings, **(n)** the functionality "Add money"will allow the transfer of single or recurring amounts, such as payments on internet via 3 D Secure, in active current accounts opened in RON by the holder at the Bank, using a debit card or a credit card issued in any currency by a bank/financial institution (credit cards issued by UniCredit Bank and UniCredit Consumer Financing IFN are excluded, as well as Junior current accounts). The availability of the service and the limits of the "Add money" functionality can be found on www.unicredit.ro and in the Terms and Conditions of the functionality's use. The Client cannot request the change of the transaction limits. The mandate for recurring payments granted to the Bank's Client may be withdrawn at any time from the application, within its validity period and may end in the following situations: i) the end of the card' validitiy period, ii) if within 3 (three) consecutive months, at least one transaction authorized by the card issuing bank is registered, iii) at the closing of the current account opened with UniCredit Bank iv) when the card issuing bank rejects a transaction as a result of the card being blocked. In any of these situations, the Client will be notified by the Bank through a PUSH notification, **(o)** activating and administering (revocation and modification) of intra-bank Direct Debit mandates; this functionality is not available to MasterCard Young debit card holders, **(p)** enrolling / withdrawing in / from the "ShopSmart" cash-back program and activating the offers presented within it; the program allows participants to obtain discounts in the form of cash back for payments made to merchants with cards issued by the Bank with the Client'name; functionality will not be available to minor customers and users of additional cards, **(r)** sending money - intrabanking and interbank payment orders at predefined deadlines (standing orders) in RON, **(s)** other instructions in case the Bank provides this possibility by means of the application,
(iii) requests for the management of products/services: **(a)** opening and liquidation of term deposits, **(b)** early reinbursment for Bank loans, **(c)** signing using qualified electronic signature for specific documents, including pre-contracts and/or contracts for landing products, **(d)** the generation of MCash codes for cash withdrawals in RON from the current account (except the Junior current account) from ATM / BNA terminals belonging to UniCredit Bank, up to a maximum of RON 4,000 / day, respectively RON 2,000 / transaction. The limits are fixed and established by the Bank, their value cannot be modified at the Client's request. The functional characteristics of MCash Codes generated from Mobile B@nking are: (i) MCash codes can be generated from Monday to Friday (working days),

between 07:00-22:00, (ii) it is possible to generate a single MCash code in at the same time, which may be visible in the application until its use / expiration / cancellation, (iii) the generation of the MCash Code has the effect of making the amount unavailable and transferring it to a transitional account. After the expiration of the validity term or if the user cancels the MCash code before its expiration in the Mobile B@nking application, the amount of money unavailable is returned to the Client's account, (iv) the generation of MCash codes is possible only if there are sufficient funds in the account for which the code is requested, (v) Cash withdrawal from ATM / BNA will be made based on the MCash code and the instructions displayed to the Client in the Mobile B@nking application, **(e)** registration of the cards issued by the Bank and the cards issued by UniCredit Consumer Financing, on the name of the Client as cardholder in Apple Pay / Google Pay, in order to make online payments and contactless payments at POS installed at merchants directly with the mobile phone compatible with the Apple Pay / Google Pay Service **(f)** updating the identity document (available only to Customers / Users of adults, account holders residing in Romania and holding an identity card issued by the Romanian authorities) and updating the telephone number and e-mail address **(g)** other requests in case the Bank provides this possibility by means of the application.
iv) request to contract new products/services: (a) open a savings account, (b) issue a debit card – issuing of a virtual debit card; (c) Initiate the flow for contracting credits' UCFINUCFIN (viewing the main characteristics, preliminary declarations, checking eligibility criteria)., accessing the functionalities for: (i) granting credits directly by UCFIN, (ii) contracting products intermediated by UCFIN and (iii) enrollment for qualified electronic signature issued by the qualified trust service provider for which the Bank is registration authority, using the PIN code of the Mobile Banking for signing/accepting certain correlated documents.

8.2.2.1 Through Mobile B@nking, the User has access to several functionalities, as follows:
(i) the User with the rights of "Transfer and other banking operations" can view the status of accounts, loans and debit/credit card associated to the service, and can send instructions with regard to products/services:: **(a)** sending money - intrabank and / or interbank payments in LEI and foreign currency to IBAN accounts, using standard or urgent processing method, and the intrabanking in LEI can also be performed with the "INSTANT" option and/or foreign exchange; **(b)** sending money - payments to authorized utility providers by scanning the barcode or entering the invoice details manually, including granting / activating and administering (revocation and modification) of intrabank Direct Debit mandates according to the provisions of art. 8.2.2. (ii), letter n; **(c)** generation of MCash codes, according to the provisions of art. 8.2.2, (iii) letter e; **(d)** the possibility of requesting the reissue of the physical debit card and the updating of its delivery address; **(e)** the opening and liquidation of term deposits; **(f)** the opening of saving accounts **(g)** sending money - intrabank and interbank payment orders at predefined deadlines (standing orders), in RON. **(h)** possibility to view the card data issued on the User's name (card number/CVV/expiration date) and copy the card number - by using the authorization credentials used to access the Mobile B@nking , **(i)** early repayment of credit cards or mortgage loans; **(j)** transfer of single or recurring amounts, such as payments on internet via 3 D Secure, in active current accounts opened in RON by the holder at the Bank, using a debit card or a credit card issued in any currency by a bank/financial institution according to the provisions of art. 8.2.2. (ii), letter m; **(k)** registration of the cards issued by the Bank and the cards issued by UniCredit Consumer Financing, as cardholder in Google Pay/Apple Pay, in order to make online payments and contactless payments at POS installed at merchants directly with the mobile phone compatible with the Google Pay/Apple Pay Service; **(l)** amendment of the transaction limit of the debit, physical or virtual, and credit cards **(m)** temporary blocking of cards (plastic or virtual), as well as their unlocking; **(n)** enable/disable push notifications; **(o)** enable/disable marketing consent, (p) possibility to activate physical debit/credit/meal cards issued on Client/User name.
(ii) the User with"View" rights can view the status of accounts, loans and debit/credit card associated to the service, and can send instructions with regard to products/services: **(a)** registration in Apple Pay / Google Pay of the physical cards issued by the Bank and the cards issued by UniCredit Consumer Financing, in his name in order to make Internet payments at POS installed at merchants directly with the mobile phone compatible with the Apple Pay / Google Pay Service; **(b)** transfers of single or recurring amounts, such as payment on Interent via 3 D Secure, only to current active accounts opened in RON by the holder at UniCredit Bank, using a physical debit card or credit card issued in any currency of a bank/financial institution, according to the provisions of art.8.2.2, (ii), letter m. **(c)** possibility to view the card data issued on the User's name (card number/CVV/expiration date) and copy the card number - by using the authorization credentials used to access the Mobile B@nking , **(d)** the opening of saving accounts; **(e)** amendment of the transaction limit of the debit and credit cards; **(f)** temporary blocking of cards, as well as their unlocking; **(g)** the possibility of requesting the reissue of the physical debit card and the updating of its delivery address; **(h)** enable/disable push notifications; **(i)** enable/disable marketing consent, **(j)** possibility to activate physical debit/credit/meal cards issued on Custoemr/User name
The updated list of functionalities is available on www.unicredit.ro, as well as in any local office of the Bank.

8.2.3 Authorisation of payment operations. The Client's consent for the authorisation of payment operations will be given by strict authentication, by the automated generation of a valid Security Code. The security code is unique and correlated dynamically with particular elements of the payment operation (e.g., value of the payment operation and the beneficiary of the payment). The automated generation of the security code is performed by: **(i)** entering of the **PIN code or (ii)** in case that the Client chooses so, by the scanning of the digital fingerprint set in the mobile phone or of the scanning of facial features set in the mobile phone, reading of the fingerprint and facial recognition being performed by the specific technology of the mobile phone. The Client's consent for the authorisation of payment operations by scanning the digital fingerprint or by scanning facial features is valid only for amounts less than or equal to RON 800. At the same time, consideration will be given to the following rules before choosing to provide consent

by scanning the digital fingerprint or by scanning facial features: **(i)** the option is available for compatible phones with iOS or Android operating system, depending on their technical characteristics, **(ii)** once the Client chose this method of authorisation, the mobile phone will allow it to use any fingerprint or facial image stored in the memory of the mobile phone, so that it is prudent to activate additional security measures, to protect the mobile phone against unauthorised access by other persons and not save fingerprints or facial images of other persons in the memory of the mobile phone.

CHAPTER 9. SPECIAL PROVISIONS ON THE INFO SMS SERVICE

9.1 Rules of use. (1) By Info SMS, the Bank sends, according to the Client's option expressed in the Application/Online B@nking/INFO Centre, informative SMS messages regarding: **(i) Payment operations / collections** – messages sent in real time as a result of daily collection/payment operations (except for transactions performed at the cashier's office and transactions such as deposits/withdrawals of cash with card at the BNA) performed on the Current Accounts opened with the Bank: a) for any collection/payment operation or b) only for collections/payment operations that exceed an established amount ("Alarm threshold"), **(ii) Card Transactions** – messaged related to transactions performed with credit and/or debit cards which allow access to the accounts opened with the Bank, sent in real time for: a) any transaction or b) transactions in excess of the Alarm Threshold, **(iii) Expiry of the duration of the loan of the overdraft type** – messages related to the expiry of the Overdraft facility sent 3 days prior to the expiry date; the calculation of this deadline does not consider the expiry date, **(iv) Loan due date** – messages regarding the due date of loans taken from the Bank, sent 3 days prior to the due date; the calculation of this deadline does not consider the due date, **(v) Minimum payment amount for credit cards** – messages with regard to the minimum payment amount according to the credit card contracts executed with the Bank, **(vi) Current Account Balance** – messages related to the balance of Current Accounts opened with the Bank, sent with the following frequency: "B" – for each amendment of the balance or "D" – on a daily basis.
(2) The bank will send the messages if the information/instructions sent by the Client are correct and complete. The activation date of the service is the date when the Client receives SMS messages according to its options.
(3) In order to benefit from this service, the Client needs a mobile phone able to receive SMS messages and be connected only to national mobile telephony networks.
(4) The Client may request amendments related to phone numbers where messages are sent, the accounts with regard to which the service is activated, the Alarm Threshold, by means of a written application in the local offices of the Bank/Online B@nking/INFO Centre.
(5) The Client must notify the Bank immediately, in writing/by Online B@nking/INFO Centre, in case that the phone numbers specified for the receipt of SMS messages are no longer available regardless of reason (e.g., termination of telephony agreement, alienation of the phone number, loss of phone) and indicate other numbers of mobile phone. The Bank will be able to order the deactivation of the Info SMS service until the receipt of instructions from the Client.
(6) The Bank will charge fees according to the Annex, which will be collected in the last Business Day of the current month. Fees are also charged in case the Client's mobile phone is closed, and the sent messages are stored by the operator for 7 days calculated from the day when the message has been sent.
(7) The Info SMS service is for information purposes and does not substitute the statement of account issued by the Bank, with regard to the evidence of transactions made in the Client's account and the balance of the account.
(8) As an exception from the provisions of art. 1.1, para. (b) according to which the GCU supersede any previous form/directive to the contrary, the provisions of para. (1) above related to the types of SMS messages and those related to the rules for the charge of commissions are not applicable to this type of service (regardless of name) contracted on the basis of specific prior forms/contracts; these shall remain regulated by the previous provisions and can be amended only according to the law and to the Contract.

CHAPTER 10. SPECIAL PROVISIONS ON CASH MULTIPURPOSE MACHINES (BNA)

10.1 Rules of use. (1) BNA is a multi-purpose equipment for the release and deposit of cash intended for the operations below. Operations are performed by means of Payment Instruments (physical debit/credit card, garnishment bar code and MCash code) or without their physical presence (in case of foreign exchange, recharge of phone cards or payments to agreed utility providers).
The garnishment bar code represents a code consisting of: (i) 6 digits generated automatically by the Bank and sent to the clients via SMS, in the circumstances specified under art. 2.21 and (ii) the last 4 digits of the Client's ID Digits, which the Client must add to the code received from the Bank. The cash withdrawal of due amounts at the Bank's terminals is performed based on a Security Element - PIN Code (personal identification code) sent to the Client via SMS.
The erroneous entering of the PIN Code on three occasions involves the cancellation of the garnishment bar code, with the consequence of the impossibility to use it. For each cash transaction, BNA issues a receipt for the confirmation of the transaction.
(2)The Client has the possibility to perform the following bank operations: **(i)** deposit and withdrawal of cash by means of payment instruments physical debit/credit card; **(ii)** foreign exchange without the physical presence of the payment instruments (debit/credit

card); **(iii)** payments to agreed utility providers, by scanning the invoice issued by a utility provider; **(iv)** the recharge of phone cards sold by the agreed utility providers; **(v)** by means of the debit/credit card: mini-statement on card operations performed in the account, payment of utility invoices to agreed utility providers, visualisation of the account balance, change of the PIN related to the card. These operations are also applied the directives of Chapter 5; **(vi)** cash withdrawals within the limit of maximum RON 2,000 by means of the garnishment bar code; **(vii)** cash withdrawals by means of the MCash code **(viii)** arrangement of operations according to the related special directives.
(3) The following operations are allowed: **(i)** cash deposits only in the form of banknotes, in RON, EUR and USD, within the limits of EUR 15,000/day or equivalent. The Client must not include in such deposits any notes that are torn, tacked with adhesive tape, stained or very worn because they may lead to the BNA becoming jammed, **(ii)** cash withdrawals (only in the form of banknotes) in RON, with the following denominations: RON 1, 10, 50 and 100 and **(iii)** starting with 01.04.2021, cash withdrawals (only in the form of banknotes) in EUR, with denominations of EUR 50. If the card used for cash withdrawal is attached to a current account opened in a currency other than EUR, the exchange will be made at the exchange rate practiced by the Bank at the time of conversion, and it will be communicated on the BNA screen before processing the transaction.
(4) In case of case of cash withdrawals by means of the garnishment bar code, the Client must enter, subsequent to the garnishment bar code, the PIN code notified to the Client by the Bank via SMS. The PIN code represents the amount which the Client can withdraw at the Bank terminal.
(5) The garnishment bar code is valid for 30 calendar days following the date of release. The release of the bar code results in the freezing of the amount and transferring it into a transit account. Following the expiry of the validity term, the code becomes unusable and the frozen amount of money is returned to the client. The Bank will generate automatically a new code when the Bank credits this account next with the amounts owed to the Client, according to provisions of art.2.21 above.
(6) Regarding the generation of the MCash code from the Mobile B@nking application, its use and functional characteristics, the provisions of art.8.2.2, (iii), letter (e) will be applied accordingly.

10.2 Authorisation of payment operations. (1) The consent of the Client/User for the performance of bank operations by means of BNA by card /garnishment bar code/MCash code is considered expressed when entering the PIN code related to the card /garnishment bar code/MCash code, as applicable.
A Client instruction is considered received by the Bank following the moment when the Client authorised the payment operation, according to the provisions above. Cash deposits made after 8:00 pm will be operated in the following bank Business Day.
(2) Foreign exchange operations are limited to the amount of RON 5,000 or equivalent per transaction.
(3) In case that, for invoice payment purposes, the Client deposits: **(i)** an amount greater than the amount to be paid, and the BNA cannot release the difference, the Utility provider's account will be credited with the entire amount that has been deposited, the regulation following to be performed at the following invoice issued by the Provider; **(ii)** an amount less than the amount to be paid, the transaction will be performed if the Client wants to make a partial payment.

10.3 The Client has the obligation to: (i) notify the Bank immediately with regard to any BNA dysfunction, such as: impossibility to perform cash withdrawals/deposits, card blockage, inoperative BNA, the amount deposited into the account is different from the amount displayed following the deposit and/or registered on the receipt, failure to perform the deposit (the Client must have a payment denial document), amount released partially (the Client must have a payment denial document), the amount released at the foreign exchange is less than the RON equivalent for the amount collected in foreign currency; **(ii)** during the validity period of the garnishment bar code, request the Bank offices to resend the code or cancel it in case it is not possible to withdraw the amount available in the Bank terminals for reasons that are not imputable to him/her.

CHAPTER 11. SPECIAL PROVISIONS ON PAYMENT INITIATION SERVICES, NOTIFICATION SERVICES WITH REGARD TO THE ACCOUNT AND CONFIRMATION OF FUND AVAILABILITIES INITIATED BY A THIRD-PARTY PROVIDER OF PAYMENT SERVICES BY MEANS OF A UNIQUE DEDICATED INTERFACE (API)

11.1 Payment initiation service. The Client can initiate a payment order with regard to a Payment account held by the Client with the Bank, accessible on-line on the payment initiation date, by means of a third-party provider of payment initiation services and a unique dedicated interface (API). In order for the Bank to execute payment orders initiated as above, the Client must authenticate strictly in Online B@nking/Mobile B@nking and express consent in the same way as for payments initiated directly by Online B@nking/Mobile B@nking. After the expression of consent, the client cannot cancel the payment order by means of the third-party provider of payment services. Based on this consent, the third-party provider of payment initiation services, with which the Client initiated payment, can check the final status of the transaction. The Client can identify in the history of Mobile B@nking/Online B@nking transactions the data of the third-party provider of payment services by means of whom the payment has been initiated.

11.2 Notification service regarding the Payment accounts. The Client can request the following information on a Payment account accessible on-line on the request date, by means of a third-party provider of payment services: account details, balance of

account and history of transactions performed from or in the Payment account. The Bank will provide the information requested by the Client by means of the third-party provider of payment services by means of a unique dedicated interface (API). In order to submit this information, the Client must authenticate strictly in the Online B@nking/Mobile B@nking and accept the transmission of information as follows: (i) in Online B@nking - by entering the Security Code, which is generated by the Token device - Digipass or by Mobile Token, depending on the selected method of authentication; (ii) Mobile B@nking, by entering the PIN code or, should the Client choose so, by scanning the fingerprint or by scanning the facial features set in the mobile phone, fingerprint reading or facial recognition being performed by the technology specific to mobile phones. Consent is valid for 90 days following the day of release. In this period, the third-party provider of payment services can request the data maximum 4 times/day in its own name and whenever the request is made on behalf of the client, without the Bank requesting any other authentication from the Client. Following the expiry of the 90 days, consent is requested. The Client can view in Mobile B@nking/Online B@nking the history of consents released to third-party providers of payment services. Consent can be cancelled/ blocked/ unblocked or extended at any time in Mobile B@nking/Online B@nking during its validity period.
Service for the confirmation of availability of funds (check balance). By means of this service, the Bank will confirm immediately through a secured channel (API), upon the demand of a third-party provider of payment services who issues card-based payment instruments, if an amount required for the execution of a card-based payment operation is available in the Account of Payments accessible on-line. In order to activate the service and allow the transmission of information for the confirmation of fund availability, the Client must express its consent by: **(i)** Online B@nking - by entering the Security Code, which is generated by the Token device - Digipass or by Mobile Token, depending on the selected method of authentication; **(ii)** Mobile B@nking, by entering the PIN code or, should the Client choose so, by scanning the fingerprint or by scanning the facial features set in the mobile phone, fingerprint reading or facial recognition being performed by the technology specific to mobile phones. By providing consent, the third-party provider of payment services will be allowed to check at any time the availability of any amount in the Payment Account accessible on-line with regard to which consent has been given. The Bank will answer the third-party provider of payment services by "Yes" or "No" upon the check balance request. Consent is valid for an unlimited period after being released. The Client can check in Mobile B@nking/Online B@nking the history of all check balance requests and of all consents released to third-party providers of payment services. Consent can be cancelled, blocked or unlocked at any time from the Mobile B@nking/Online B@nking settings.

11.3 The Bank can deny access to the Payment Account accessible on-line for objective reasons related to the unauthorised or fraudulent access of the Payment Account accessible on-line by a third-party provider of payment services, inclusively by the unauthorised or fraudulent initiation of a Payment Operation. Under such circumstances, in the extent possible, the Bank notifies the Payer Client, if possible, prior to the denial of access and at the latest after such notification, by phone or by means of electronic communication (Online B@nking, Mobile B@nking, e-mail, SMS etc.) that access to the Payment Account is denied and the reasons for such denial, unless the provision of such information would compromise the safety reasons justified objectively or is prohibited by the law. The Bank allows access to the payment account once the reasons for denial cease to exist.

CHAPTER 12. FINAL PROVISIONS. DURATION AND TERMINATION OF THE AGREEMENT

12.1 The Agreement is executed for an undetermined period. The Bank provides the Client with the Agreement, free of charge, on paper support or another Durable medium, in order to commence the contractual relationship, which cannot be sooner than the expiry of the legal period of 15 days available to the Client for review prior to becoming a part of the Agreement, unless the Client requests expressly the decrease/waiver of this period. Particular circumstances: **(i)** directives regarding the rights and obligations of the parties related to the Current Account come into force in the moment when the Bank makes available to the Client the IBAN code, **(ii)** directives related to rights and obligations of the parties related to the physical debit card come into force when the card is handed over, **(iii)** dispositions regarding the rights and obligaitons of the parties in relation to the virtual debit card enter in force after the card is issued in Mobile B@nking.
(iv)directives on the rights and obligations of the parties related to Online B@nking come into force according to the selected method of authentication: a) in case of the Token Device - Digipass, when the Client receives the Token Device - Digipass or b) in case of Mobile Token, in the moment when Client activates the Mobile Token application using the Configuration Code sent by the Bank, **(iv)** directives related to the rights and obligations of the parties with regard to Mobile B@nking come into force in the moment when the Client activates the application by using the Configuration Code sent by the Bank and **(v)** in case of contracting the product/service by a remote means of communication, the moment of coming into force will be established upon mutual agreement between the Bank and the Client, but it cannot be prior to the moment of providing the information requested by the law on Durable medium.

12.2 The Agreement terminates by: (i) the written agreement of the parties, on the date and in the conditions agreed upon; **(ii)** unilateral termination, in whole or in part, at any time, with immediate effect, by means of a notification sent by: **a)** the Bank two months prior to the date of termination of the Agreement related to a Payment Account with basic services, in case the Client did not register any Payment Operations for a period of minimum 24 consecutive months;
b) the Bank two months prior to the date of termination of the Agreement related to any product/service, other than a Payment Account with basic services and **c)** the Client with one month prior to the termination date; **(iii)** notification sent 15 days prior to

the termination in the following circumstances**: a)** termination by one party for the other party's failure to observe their obligations which determines the impossibility to execute the Agreement, **b)** the impossibility to provide a product/service, for reasons that are not imputable to the Bank; **(iv)** the death of the Client, with immediate effect, any credit balance being available to successors according to the law; **(v)** without notification or other prior formality, with immediate effect if, starting with 01.07.2021, the balance of the account is zero or less than zero and there are no account operations (except for the fees and commissions charged by the Bank) for a period of minimum 24 months; **(vi)** in any other circumstances specified in the Agreement and/or legislative directives/decisions of authorities.

12.3 Effects of termination. Upon the termination of the Agreement in any way: **(i)** the Bank will close the related product/service, without any additional costs. The current account will not be closed in case it is garnished or frozen according to the law and/or in the account there are operations related to other products/services, **(ii)** the Client will return to the Bank the unused forms, as well as the other means of communication and data transfer made available by the Bank, **(iii)** throughout the legal statute of limitations applicable to the return of amounts representing credit balance on the date of closing the Current Account, the Bank will not owe any interest, **(iv)** all amounts owed to the Bank according to the Agreement become exigible (including amounts owed as a result of transactions performed with the debit card prior to termination), and the Client must pay to the Bank immediately the credit balance without the need of any notice of default to the Client or any other judicial/extra-judicial formality. The mere maturity of any deadline specified or provided according to/with regard to the Agreement involves the notice of default of the Client by the operation of law. Without prejudice to the directives of the Agreement on the notice of default to the Client, in particular circumstances, the parties agree that it is not be necessary to provide any notifications by means of the officer of the court, in order to provide a notice of default to the Client. In order to recover any owed amount, the Bank can use any means specified by the specific legislation, **(v)** in case the balance is credit, the Client must notify the bank with regard to the transfer of the balance (available after the payment of all of its obligations towards the Bank). Closure of all Client accounts determines the termination of all products/services contracted with the Bank.

CHAPTER 13. FINAL PROVISIONS

13.1 Communications/Notifications related to the Agreement. a) Any request, notification, approval, communication will be made by the Bank at the addresses/phone numbers of the Client specified in the Agreement, by any of the following means: direct delivery, mail, fax, electronic mail (e-mail), recorded telephone conversation, SMS message, Online B@nking, Mobile B@nking, specifications in the statement of account/activity report, including the display at the local bank offices, if necessary. The Bank can also use other means of communication, including remote communication techniques, in observance of the legislation in force. In order to view documents in PDF format sent by the Bank via electronic mail (e-mail), Online B@nking or Mobile B@nking, an application must be used to open such documents, which must be compatible with the device used by the Client (e.g., Adobe Acrobat Reader).
In case that notifications refer to the transmission of the Agreement on Durable medium or include amendments of the Agreement, the Bank will use these means of communication in observance of the legislation in force and without any prejudice to the legal provisions that limit/prohibit contractual amendments by means of such practices. Any type of correspondence by the means of communication specified in the present article represent complete evidence in front of any authority or court/court of arbitration. The Bank is exonerated from any responsibility with regard to the execution, performance and termination of the Agreement in case that any of the identification/contact data provided by the Client to the Bank are not accurate or the Client does not communicate to the Bank their amendment according to the provisions of the Agreement. Any communication performed by the Bank based on the identification/contact data provided by the Client is considered valid.
In case of suspected fraud or real fraud or in case of threats to security, the Bank notifies the Client/User by phone or by means of electronic communication (Online B@nking, Mobile B@nking, e-mail, SMS etc.) or by means of any other secured procedure.
Communication by direct delivery is considered received by the Client upon delivery. A communication by mail is considered received by the Client upon the expiry of the delivery deadline established/warranted by the provider of postal services (according to the normal post office circuit), if it has been sent to the last address notified to the Bank by the Client, even if the address is of a third party entitled to receive mail. A communication via fax/e-mail/SMS/Online B@nking is considered received by the Client in the transmission day. Communications are considered received by the Client and in case the Bank comes into the possession of a confirmation of any kind, of a copy of a notification with the original signature of the Client/proxies of the Client, or if the receipt is confirmed by means of an acknowledgement of receipt issued by the mail or by quick courier services, as applicable.
b) Any notification will be sent to the Bank by the Client by direct delivery or by registered letter with the acknowledgement of receipt. The communication of amendments of identification data/residence address and/or address for service/e-mail or any other data specified in the Agreement is binding upon the Bank starting with the Business Day following the receipt of the notification by the Bank, proven by the Bank registration stamp, applied on the Client's copy, or by the confirmation of receipt signed by the Bank. The failure to communicate these amendments involves the exclusive responsibility of the Client and will exonerate the Bank from responsibility of any damage suffered by the Client as a result of the failure to notify the amendment. Any communication received outside the public Business Hours is considered received starting with the following Business Day.
c)The Bank does not undertake any responsibility with regard to the effects and consequences of any nature arising from the use

of any means of communication for the transmission to the Client of any communications, including the communication of the Agreement on Durable medium, as well as from the delay, failure to receive, damage, loss or from other transmission errors of the messages, letters or documents, including those related to inter and intra-bank settlement operations, as a result of the use of the respective means of communication. Any communication made by the Bank on the basis of the Agreement at the e-mail address/phone number specified by the Client is considered valid, the Client being the only responsible party, with the obligation to ensure that (i) the e-mail address, phone number provided to the Bank. As well as the software, devices used to access them are not affected by settings, actions, inactions of any type, personal/of the third-party internet/telephony provider, which may lead to the alteration, corruption, failure to receive, blocking, delay, loss of communications sent by the Bank or any other similar events, (ii) does not create the possibility that such communications sent by the Bank are accessed, intercepted, copied, read, redirected to/by a third party.

(d) The Client undertakes to pick up mail from the Bank (including card issued/reissued) within a reasonable period, otherwise the Bank can destroy any correspondence that is not collected by the Client for 3 months following the date of release.

13.2 Supporting documents. (1) Telephone conversations held with the Bank by the Client/User/Proxy can be recorded, in order to provide maximum safety to transactions ordered to the Bank/performed by the Bank. The Bank can also register the telephone conversations related to the contracted banking product/service. The Bank can keep the records of conversations for a period of at least 5 years.
(2) Records can be used both in the relationship with the Client/User, and as evidence in front of any authority, including in front of courts of law/courts of arbitration or in other circumstances where the Bank understands that it is necessary to protect its interests.
(3) Original supporting documents, (ii) the Client's files with the Bank (iii) the messages authorised by the Client within Online B@nking (iv) communications sent to the Client by the Bank via Online B@nking/ Mobile B@nking or by e-mail at the address notified to the Bank, (v) recorded telephone conversations, (vi) contractual documents in electronic form, signed by the Client/Proxy together with electronic signature, either qualified, advanced or simple, inclusively by the application of the handwritten signature on the tablet/by means of a device that allows the collection/realisation of its image on the contractual document in electronic form, constitute by themselves the basis for the settlement of relationships between the Bank and the Client and can be used as evidence in front of any authority, including in front of courts of law/courts of arbitration. Evidence of performance of transactions in the Client's account is given by the statement of account.

13.3 Circuit of documents. The Bank does not undertake any responsibility for the authenticity, validity or completeness of documents or for any adverse effects that may occur as a result of the use of inappropriate materials, nor for the incorrect interpretation or translation of these documents, nor for the type, quantity or nature of goods that may be mentioned in these documents.
The documents issued by a foreign authority submitted to the Bank, such as identification documents/authorisations, shall be examined by the Bank with maximum care. However, the Bank does not undertake any responsibility with regard to their authenticity. The Bank is not under the obligation of checking the authenticity, completeness or validity of documents prepared in Romanian or in a foreign language with regard to the appointment of a guardian, curator, administrators of the will or other legal representatives. The Client will cover any current or future loss due to the falsification, legal invalidity or interpretation and/or incorrect translation of such document sent to the Bank.

13.4 Transfer of rights and/or obligations. The Bank can transfer in any way (assignment, novation, delegation or any other mechanism to transfer the rights and obligations acknowledged by the law), in whole or in part, any of its rights and obligations arising out of this Agreement. The Agreement will be considered executed in the benefit and will lead to the occurrence of valid and executory obligations for a purchaser or a person who takes over the Bank assets, a successor of the Bank or any assignee or agent thereof. The Client cannot assign/novate/transfer/delegate to any third party, at any moment, without the prior written consent of the Bank, its rights and obligations arisen out of the present Agreement.

13.5 Amendment of the Agreement. Any amendment of the provisions herein will be performed and will come into force after the lapse of two months following the prior notification of the Client with regard to the amendments, performed by the Bank by one of the means specified under art. 14.1 (information provided on Durable medium, according to the applicable legislation), unless, prior to the proposed date of coming into force, the Client provided a written notification to the Bank for the denial of the amendments. Under such circumstances, the Client is entitled to terminate the present Agreement unilaterally, free of charge, prior to the proposed date for the application of modifications. In the extent required by the legislation in force, the amendments will be performed by the agreement of the parties, specified in an addendum signed by the parties.
The bank can include additional technical conditions that amend the present agreement, in case of technical changes requested by the competent specific authorities or of those imposed by the operating systems of the Bank or of its service providers which would occur throughout the performance of the agreement. These amendments will be notified to the Client, on the Bank website.

13.6 Language of the Agreement. The present GCUs are concluded in Romanian. Should the Bank propose and the Client accept another language version, in case of disputes or discrepancies between the Romanian version and the foreign language version, the

Romanian version will prevail. In any case, any communication between the Bank and the Client throughout the contractual relationship is performed in Romanian. The terms and expressions in English, consecrated as such in the financial-banking language or in legal provisions, without any correspondent in Romanian, are used in the present GCUs with the related definitions/explanations.

13.7 Applicable Law. The law in force in Romania governs all the relationships between the Client and the Bank, even in case of a trial abroad.

13.8 Disputes. Litigations. The Client is entitled to send the Bank complaints. Within maximum 15 Business Days following the receipt of a complaint, the Bank: **(i)** will send an answer to the Client on paper support/Durable medium or **(ii)** in exceptional circumstances, when the answer can be sent within the period mentioned above, will notify the Client with regard to the reasons for such refusal an specify the period for the submission of the answer, without it being in excess of 35 business days.
The Client can also file complaints with the **National Authority for Consumer Protection (ANPC**), having its registered offices in 72 Bd. Aviatorilor, Sector 1, post code 011865, Bucharest, phone: 021/9551, e-mail: cabinet@anpc.ro, website www.anpc.ro or **its local offices** with regard to any issues related to the agreement, less those that are under the competence of the National Bank of Romania.
The Client can notify the **National Bank of Romania**, having its registered office in 25 Lipscani St., Sector 3, post code 0300031, Bucharest, website www.bnro.ro, according to the provisions of art. 222 corroborated with art. 150-165, art. 218-221 and art. 248 para. (3) of Law 209/2019, on **(i)** payment initiation services, information services with regard to the account and confirmation of fund availability initiated by means of a third-party provider of payment services through the dedicated unique interface (API), **(ii)** blocking of payment instruments by the bank, **(iii**) expense limits for payment instruments or, if necessary, **(iv)** operational and security risks associated with payment services, issues related to the strict authentication or exceptions from the application of strict authentication.
The Parties shall take all efforts to reach an amiable settlement of any litigation or discrepancy between them arising out of the present Agreement. For the amiable settlement of any potential litigations, the Client and/or the Bank can resort to mediation, on the grounds of provisions of Law no. 192/2006 on mediation and organisation of the mediator profession and/or alternative settlement procedure of litigations administered by the **Alternative Banking Dispute Resolution Centre** having its registered office in 24 Sevastopol St., et. 2, Sector 1, Bucharest, Phone: (021)9414, e-mail: office@csalb.ro, website www.csalb.ro., according to the Government Decree no. 38/2015 on the alternative settlement of litigations between consumers and retailers. Litigations are of the competence of Romanian courts.
In any judicial/extra-judicial procedure, the documents issued by the Bank with regard to the amounts owed by the Client represent complete evidence of the debt towards the Bank.

13.9 Other final provisions. Upon the written request of the Client, at any time during the contractual relationship, the Bank makes available, free of charge, on paper support or on any other Durable medium, the present GCUs to include the information and conditions specified in Law no. 209/2019 on payment services. In case that the requests of the Client, in the opinion of the Bank, are abusive by frequency, the Bank is entitled to select the least expensive transmission methods for the Bank.

No delay in the exercise by the Bank of its rights specified in the present Agreement shall be interpreted as a waiver of the Bank to the exercise of the respective right, and a singular or partial exercise of a right does not involve the subsequent non-exercise of any other right. In case any provisions of the present Agreement become illegal, invalid or inapplicable according to the law, the legality, validity and enforceability of the other provisions will not be affected by it.
The headings of chapters and marginal names of contractual provisions are a summary expression of their scope, instead of having individual significance.

For details on the requested products/services, the Client can contact any local office of the Bank, INFO Centre or may check the website of the Bank www.unicredit.ro.

The supervisory authority of the Bank is the National Bank of Romania, having its registered headquarters in Romania, Bucharest, strada Lipscani nr. 25, sector 3, postal code 030031.

13.10. Limit hours specific for each type of operation.

The amendments to the benefit of the Client, meaning the establishment of wider deadlines, can be applied immediately.

Payment operations Credit transfer - RON Payments	Payment instruments	Limit hours for the receipt of instructions (T-Day) for standard payments (from Monday to Friday)	Date of crediting the account** of the beneficiary's provider of payment services - Standard payment
Sending money - intrabank payment – with the debiting of the Client's account and crediting of the account of the payment beneficiary in the same day, except for standard and for transfers regarding the payment of utilities, instructed via Online B@nking / Mobile B@nking Friday between 23:00 and 23:59, on Saturdays, Sundays and in national and/or legal holidays, which will be processed in the following business day, which is not a national and/or legal holiday	Paper form	16:00	T+0
	Online B@nking/ Mobile B@nking	20:00 *For payments sent with the "INSTANT" option, the mentioned limit hour does not apply, they can be initiated 24/7, except for those of utilities to suppliers approved by the Bank, which cannot be made on Friday between 23:00-23:59, on Saturdays, Sundays and national and / or public holidays.*	T+0
Sending money - interbank payment on the territory of Romania – with the debiting of the Client's account and crediting of the account of the beneficiary's provider of payment services in the same day	Paper form <RON 50,000 ≥RON 50,000 or urgent payment*	12:30 14:00	T+0
	Online B@nking/ Mobile B@nking – <RON 50,000 ≥RON 50,000 or urgent payment*	14:30 15:15	T+0
Sending money - interbank payment on the territory of Romania – with the debiting of the Client's account in the day when the instruction is received and crediting of the account of the beneficiary's provider of payment services in the following banking business day	Paper form <RON 50,000 ≥RON 50,000 or urgent payment*	12:30-15:30 14:00-15:30	T+1
	Online B@nking/ Mobile B@nking – <RON 50,000 ≥RON 50,000 or urgent payment*	14:30-17:00 15:15-17:00	T+1
Sending money - RON payments outside the territory of Romania – with the debiting of the Client's account and crediting of the account of the beneficiary's provider of payment services in the same day	Paper form	12:30	T+0
	Online B@nking/ Mobile B@nking	15:15	T+0

**Urgent payment = small value payment (< RON 50,000) which will be sent by the ReGIS system and will be charged with fees according to the fee rules of this system.*

Payment operations Credit transfer - foreign currency payments	Payment instruments	Limit hours for the receipt of instructions (T-Day) for standard payments	Date of crediting the account** of the beneficiary's provider of payment services - Standard payment	Limit hours for the receipt of instructions (T Day) for urgent payments	Date of crediting the account** of the beneficiary's provider of payment services - Urgent payment
Sending money - intrabank payment with the debiting of the Client's account in the day when the instruction is received (T) and the crediting of the payer's account in the same day (T)	Paper form	16:00	T+0	Not applicable	Not applicable
	Online B@nking/ Mobile B@nking - to accounts in IBAN format	16:30	T+0	Not applicable	Not applicable
Sending money - interbank payment in EUR in the EU and EEA	Paper form	16:00	T+2	13:30	T+0
	Online B@nking/ Mobile B@nking - to accounts in IBAN format	16:30	T+1	14:30	T+0
Sending money - interbank payment, in EUR, outside the EU and EEA and in BGN, CHF, GBP, HUF, PLN, RUB, TRY, USD, outside and inside the EU and EEA	Paper form	16:00 - TRY	T+2	11:30	T+0
		16:00 - CHF	T+2	12:30	T+0
		16:00 - other currencies	T+2	13:30	T+0
	Online B@nking/ Mobile B@nking - to accounts in IBAN format	16:30 - TRY	T+2	12:30 - TRY	T+0
		16.30 - CHF	T+2	13.30 - CHF	T+0
		16:30 - other currencies	T+2	14:30 - other currencies	T+0
Sending money - interbank payment in CAD, CZK, DKK, NOK, SEK, ZAR, AUD	Paper form	16:00	T+2	13:30	T+1
	Online B@nking/ Mobile B@nking - to accounts in IBAN format	16:30	T+2	14:30	T+1
Sending money - interbank payment in JPY, CNY	Paper form	16:00	T+3	13:30	JPY - T+1 CNY – not applicable
	Online B@nking/ Mobile B@nking - to accounts in IBAN format	16:30	T+3	14:30	JPY - T+1 CNY – not applicable

***The Bank cannot guarantee the Foreign Currency Date applied by the provider of payment services of the beneficiary of the payment when its account is credited.*

Other types of operations		
Foreign exchange (FX)		
Foreign exchange	Paper form	15:30
	Online B@nking/ Mobile B@nking	16:30
Collections		
RON collections	ReGIS/SENT	17:00

Foreign currency collections	SWIFT/SEPA	17:00
	TARGET2	17:50
Cash transactions		
Withdrawals/Deposits/Foreign exchange	Cashier's office	17:00
Term deposits		
Term deposits initiated via Online/Mobile B@nking	Opening	17:00
	Licquidation	17:00

Terms used:

Payment system - set of instruments, procedures, rules that ensure the transfer of funds between the system participants (credit institutions/financial institutions), based on an agreement between them and the system operator, by means of an agreed technical infrastructure.
ReGIS - payment system with real-time gross settlement (RTGS) for RON payments provided by the NBR. The system is used for the settlement of interbank transfers, as well as of RON payments of high value (more than RON 50,000) or emergencies.
TARGET2 - payment system with real-time gross settlement (RTGS) for payments in EUR, provided by Eurosistem (Central European Bank and the central banks of EU Member States who adopted the EUR currency). The system is used for the settlement of high-value interbank transfers in EUR as well as of other Payments in EUR.
SENT - electronic system for the multilateral clearing of low-value and high-volume interbank payments in RON, operated by Societatea de Transfer de Fonduri şi Decontări - TRANSFOND S.A. The system processes both low-value interbank credit transfers and direct debit and debit instruments similar to cheques, bills of exchange, promissory notes.
SEPA - the EURO zone, a geographical area including Member States of the EU and Iceland, Liechtenstein, Norway, Switzerland and Monaco, referred to as the Single Euro Payments Area, where all payments are dealt with as national payments (without any differences between national and cross-border payments).
Countries in the EU and EEA area (European Economic Area) - Austria, Belgium, Bulgaria, Cyprus, Croatia, Denmark, Estonia, Finland, France, Germany, Greece, Ireland, Iceland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Norway, Poland, Portugal, the Czech Republic, Romania, Slovakia, Slovenia, Spain, Sweden, the Netherlands, Hungary.
BGN - Bulgarian Leva; **CHF** - Swiss Franc; **GBP** - Pound Sterling; **HUF** - Magyar Forint; **PLN** - Polish Zloty; **RUB** - Russian Rouble; **TRY** - Turkish Lira; **USD** - American Dollar; **CAD** - Canadian Dollar; **CZK** - Czech Crown; **DKK** - Danish Crown; **NOK** - Norwegian Crown; **SEK** - Swedish Crown; **ZAR** - South African Rand; **AUD** - Australian Dollar; **JPY** - Japanese Yen; **CNY** - Chinese Renminbi.

Statement. By the application of my signature, I hereby declare that I have been explained and I understood the terms and conditions, advantages and disadvantages of the selected product, I have been informed with regard to the total cost (fees, taxes, other costs).

I agree that the contractual relationship with the Bank regarding the requested product is governed by the provisions of the Agreement (GCU, Application, Annex with Fees and Commissions, Information note and agreement on the processing of personal data) and I undertake to observe it. I hereby accept that the Bank services can be performed by an affiliate of the Bank, a third party or their subcontractors, on contractual basis. I received one copy of the GCU, version/revision 36/2022.
The Parties hereby declare that they fully understand the provisions of the greement, which they accept expressly, and these provisions are reflective of the common and unhindered will of the parties.

The Agreement is executed in as many original counterparts as there are signatories and had been hand-signed this _____/
The Agreement has been signed in electronic form, in the presence of signatory bank representatives, one counterpart remaining with the Bank and one original counterpart being submitted to the account holder at his/her e-mail address, as well as on Online B@nking/Mobile B@nking. Should the Client fail to indicate an e-mail address and does not use Online B@nking or Mobile B@nking, an original counterpart is signed on paper support, handed to the Client, and the Bank keeps the original of the Agreement signed electronically.

UniCredit Bank SA, Branch / Agency / Lucrative facility, by:

_____ **and** _____

(name, surname, position, signature) (name, surname, position, signature)

and_____(Client's name and surname)

, identified with Identification Document/Passport, series_____, no._____, ID Digits I_I_I_I_I_I_I_I_I_I_I_I_I, hereinafter referred to as "the **Client**"

_____

(Client's signature)