REGULI SI CONDITII DE UTILIZARE 3D SECURE/ ***RULES AND CONDITIONS OF USE 3D SECURE***

(1) Toate cardurile emise de Bancă sunt înrolate în serviciul 3D Secure, ce oferă posibilitatea efectuării tranzacţiilor de comerţ electronic în condiţii de strictă securitate. Serviciul 3D Secure este pus la dispoziție de Bancă prin intermediul ROMCARD S.A., procesator de date ce dispune de mijloace securizate (sub brandurile Verified by Visa şi MasterCard Secure Code) dacă sunt respectate prezentele reguli şi condiţii de utilizare (“Reguli”). Serviciul 3D Secure funcţionează în condiţiile în care site-ul pe care se efectuează tranzacţia suportă standardele 3D Secure. Orice modificare a Regulilor va fi notificată pe pagina de internet a Băncii. Tranzacţiile efectuate prin 3D Secure se află sub incidenţa versiunii în vigoare a Regulilor, la momentul efectuării acestora. Regulile sunt disponibile pe pagina de internet a Băncii.

(1) All cards issued by the Bank are enrolled in the 3D Secure service, which offers the possibility of performing e-commerce transactions under strict security conditions. The 3D Secure service is provided by the Bank through ROMCARD SA, data processor with security means (under the Verified by Visa and MasterCard Secure Code) if these terms and conditions of use ("Rules") are complied with. The 3D Secure service runs when the site on which the transaction is made supports 3D Secure standards. Any changes to the Rules will be notified on the Bank's website. Transactions through 3D Secure are subject to the current version of the Rules, at the moment the transactions are made. The rules are available on the Bank's website.

(2) Banca, Visa Internaţional şi MasterCard îşi rezervă dreptul: (i) de a modifica, îmbunătăţi ori întrerupe furnizarea acestui serviciu fără o notificare prealabilă; (ii) de a suspenda în orice moment accesul la acest serviciu dacă se dovedeşte că datele personale sunt false, inexacte, neactualizate sau incomplete; (iii) de a dezactiva temporar/permanent accesul la serviciu. În aceste cazuri, răspunderea cu privire la tranzacţiile deja efectuate nu se modifică.

(2) The Bank, Visa International and MasterCard reserve the right to: (i) modify, improve or discontinue providing this service without prior notice; (ii) to suspend at any time access to this service if personal data proves to be false, inaccurate, outdated or incomplete; (iii) temporarily / permanently disable access to the service. In these cases, the liability for the transactions already performed does not change

(3) Consimţământul Clientului pentru autorizarea unei operaţiuni de plată pe internet prin 3D Secure se va efectua prin autentificare strictă, prin generarea automată a unui Cod de Securitate unic și legat dinamic de anumite elemente ale operațiunii de plată (de ex.: valoarea operațiunii de plată și beneficiarul plății), astfel:

(3) Client consent to authorize a payment transaction online by 3D Secure authentication will be performed by strict authentication, through automatically generating a unique Security Code that is dynamically linked to certain elements of the payment transaction (eg the value of the payment transaction and the payee), as follows:

(i) Clientul/ Utilizatorul care deține serviciul Business Mobile activ/ Mobile Token activ aferent serviciului BusinessNet: (a) daca nu are activată pe telefon (în cazul Business Mobile si Mobile Token) si in aplicatie (doar în cazul Business Mobile) opțiunea de a recepționa notificări de tip „mesaje push”, va accesa Business Mobile sau Mobile Token și va autoriza respectiva operațiune de plată prin introducerea Codului PIN sau scanarea amprentei digitale/trasaturilor faciale setate în telefon, dacă Clientul a optat în acest sens, iar (b) daca are activată pe telefon (in cazul Business Mobile si Mobile Token) si in aplicatie (doar in cazul Business Mobile) opțiunea de a receptiona notificari de tip „mesaje push” in aplicatie, va primi un mesaj care va cuprinde detaliile plății (de ex.: suma operațiunii de plată, valuta de plata si numele beneficiarului etc.) fiind redirectionat in Business Mobile/Mobile Token si va autoriza respectiva operaţiune de plată, prin introducerea Codului PIN sau scanarea amprentei digitale/trasaturilor faciale setate în telefon, daca Clientul a optat în acest sens.

(i) The Client / User who has the Business Mobile service active or Mobile Token for BusinessNet active: (a) if it has not activated on the phone (for Business Mobile and Mobile Token) and in the application (only for Business Mobile) the option to receive push notifications, will access Business Mobile or Mobile Token and authorize the payment operation by entering the PIN code or scanning the fingerprint / facial features set in the phone, if the Client opted for this, and (b) if it has activated on the phone (for Business Mobile and Mobile Token) and in the application (only for Business Mobile) the option to receive notifications of type "push notifications" in the application, will receive a message that will include the payment details (eg the amount of the payment transaction, the payment currency and the name of the beneficiary, etc.) being redirected to Business Mobile / Mobile Token and will authorize the payment operation, by entering the PIN code or scanning the fingerprint / facial features set in the phone, if the Client has opted for this.

(ii) Clienții care nu au activ nici unul dintre serviciile de mai sus, vor autoriza operatiunile de plata pe internet prin 3D Secure prin utilizarea unui cod unic generat de către Bancă pentru fiecare astfel de operatiune de plata si transmis către Utilizator prin SMS, la numărul de telefon mobil declarat Băncii impreuna cu o parolă statică. Codul unic este temporar, valabil exclusiv pentru tranzacția pentru care a fost generat.

ii) Clients who do not have any of the above services, will authorizae online payment operation via 3D Secure using a unique code generated by the Bank for each such payment operation and transmitted to the User by SMS to the mobile telephone number declared to the Bank together with a static password. The unique code is temporary, only valid for the transaction for which it was generated.

Din motive de securitate, parola statică inițială comunicată Clientului în scrisoarea în care este inclus cardul trebuie modificata astfel: (a) la prima plata cu cardul pe internet, in pagina autorizarii tranzactiei (prin introducerea parolei statice initiale, introducerea si reconfirmarea noii parole statice in campurile dedicate) sau (b) la orice ATM din reteaua UniCredit Bank (optiunea Setare/Schimbare parola statică) sau (c) contactând serviciul Info Center disponibil 24h/7 la *2020, (apel cu tarif normal în retelele mobile Telekom Romania, Vodafone, Orange, RCS&RDS) sau +40 21 200.20.20 (apel cu tarif normal in reteaua fixa Telekom Romania).

For security reasons, the initial static password comunicated to the Client in the letter in wich is the card includes, should be modified as follows : (a) at the first online payment with the business card in the transaction authorization page (by entering the initial static password, entering and reconfirming the new static password in the dedicated fields) or (b) at any ATM from UniCredit Bank ATMs network (option Set/Change the static password) or (c) contact the Info Center Service available 24h/7 at *2020 (regular fee in Telekom Romania, Vodafone, Orange, RCS&RDS mobile networks) or +40 21 200.20.20 (regular fee in Telekom Romania landline network).

Ulterior, parola statica setata poate fi modificata prin aceleasi canale de mai sus.

Furtner, the set static password can be modified through the same channels above.

Operațiunea de plată nu va putea fi autorizată și cardul va fi blocat pentru operațiuni de plată pe internet, în masura in care Clientul nu reușește autorizarea după (i) cinci încercări consecutive, respective: (a) trei încercări consecutive de introducere a Codului PIN, prin Business Mobile/ Mobile Token, caz în care Business Mobile/Mobile Token nu se mai poate accesa, fiind necesară reactivarea acesteia și după (b) două încercări consecutive prin utilizarea codului unic și a parolei statice, dacă anterior s-a încercat autorizarea prin Business Mobile/ Mobile Token sau (ii) cinci încercări consecutive prin utilizarea codului unic si a parolei statice, daca anterior nu s-a încercat autorizarea prin Business Mobile/ Mobile Token, caz în care este necesară schimbarea parolei statice la orice ATM prin setarea unei noi parole, accesând butonul „Setare/Schimbare parola statica" din meniu sau apeland *2020, serviciul Info Center disponibil 24h/7.

The payment will not be authorized and the card will be blocked for internet payment operations, in case the Customer fails to authorize after: (i) five consecutive unsuccessful attempts, namely:

(a) three consecutive attempts of authorization through Business Mobile / Mobile Token, in which case the Business Mobile/Mobile Token application will be blocked and will have to be reactivated and (b) two consecutive attempts of using the 3D Secure password and the static password, if the authorization was previously attempted via Business Mobile/ Mobile Token or (ii) five consecutive unsuccessful attempts of using the 3D Secure password or static password, if previously there wasn't an authorization via Business Mobile/ Mobile Token, in which case it is necessary to change the static password at any ATM by setting a new password, by entering the "Set/Change static password" button in the menu or calling *2020, the Info Center service available 24 hours a day.

(4) Clientul poate solicita modificarea numarului de telefon mobil pe care Utilizatorul va primi codul unic asociat fiecărei tranzacții autorizata online prin 3D Secure, printr-o solicitare scrisa in orice sucursala a Bancii, intelegand ca Utilizatorul va putea primi codul unic prin SMS la noul numar in aceeasi zi lucratoare, dupa ora 17.30, pentru solicitarile depuse pana in ora 16:00, respectiv in urmatoarea zi lucratoare, dupa ora 17:30, pentru solicitarile depuse dupa ora 16:00.

(4) Customer may request to change the mobile phone number on which the User will receive the unique code associated with every transaction authorized online through 3D Secure, by written request to any branch of the Bank, understanding that the User will be able to receive the unique code through SMS to the new phone number on the same working day after 17.30, for requests submitted until 16:00 and on the following working day after 17:30 for requests submitted after 16:00.

(5) Clientul/Utilizatorul 3D Secure are următoarele obligaţii: (i) va citi cu atenţie Regulile; (ii) nu va dezvălui, sub nici o formă, comercianţilor virtuali sau unor terţi datele sale personale sau Elementele de securitate; (iii) in situatia in care consideră că a fost compromisă confidenţialitatea datelor sale (număr card, data expirării, cod numeric personal, cod unic asociat fiecărei tranzacții) va notifica imediat Banca pentru blocarea cardului până la soluţionarea situaţiei; (iii) Clientul va informa de îndată Banca despre orice modificare a datelor oferite in vederea utilizarii sau, dupa caz, orice modificare a numărului de telefon declarat Băncii; (vii) înainte de furnizarea oricărei date de identificare în vederea realizării unei plăţi, va verifica autenticitatea site-ului de plată, urmărind cel puţin: (a) afişarea siglelor aferente serviciilor Verified by Visa şi MasterCard SecureCode; (b) certificatele de securitate ale paginilor ce solicită astfel de date; (c) afişarea mesajelor de întâmpinare aferente 3D Secure.

(5) The Customer / The 3D Secure User has the following obligations: (i) will carefully read the Rules; (ii) will not disclose in any way to any merchant or third party its Personal Data or Security Elements; (iii) if he / she considers that the confidentiality of his / her data (card number, expiration date, personal numeric code, unique code associated with each transaction) has been compromised, will immediately notify the Bank for blocking the card until the situation is resolved; (iii) the Customer shall immediately inform the Bank of any change in the data provided for use or, as the case may be, of any change in the telephone number declared to the Bank; (vii) before providing any identification data for a payment initiation, shall verify the authenticity of the payment site, verifying at least: (a) the display of the logos of the Verified by Visa and MasterCard SecureCode; (b) the security certificates of the pages requesting such data; (c) the display of 3D Secure welcome messages.

(6) Clientului/Utilizatorului 3D Secure îi este interzisă: a) substituirea unei alte persoane /entităţi care utilizează 3D Secure; b) trimiterea pe orice cale a unor programe tip virus care să întrerupă, distrugă sau să limiteze funcţionalitatea oricărei componente hard/soft (inclusiv de comunicaţii) a 3D Secure; c) trimiterea de spam, pe orice cale şi invadarea site-urilor Verified by Visa şi MasterCard Secure Code accesate; d) modificarea, adaptarea, decompilarea sau dezasamblarea, sub-licenţierea, traducerea, vânzarea oricărei porţiuni a 3D Secure; e) ştergerea oricărei notificări privind drepturile de proprietate (copyright, trademark) întâlnite prin accesul la 3D Secure; f) utilizarea oricăror mijloace pentru regăsirea sau reproducerea structurii de navigare, prezentare şi conţinutul site-urilor afişând brand-urile Verified by Visa şi MasterCard Secure Code; g) întreruperea accesului altor utilizatori la 3D Secure, la servere sau reţele conectate la acesta; h) nerespectarea Regulilor şi procedurilor specifice 3D Secure în general sau oricărei reţele conectate la acesta; i) încălcarea, în mod intenţionat sau nu, a oricăror reglementări legale locale, naţionale, internaţionale sau a regulilor şi cerinţelor stabilite de Visa Internaţional şi MasterCard pentru folosirea 3D Secure.

(6) The following are prohibited for The Customer / the 3D Secure User: a) substitution of another person / entity using 3D Secure; b) sending via any channel virus-based programs that interrupt, destroy, or restrict the functionality of any 3D Secure hard / soft (including communications) component; c) sending spam, by any means, and invading the accessed sites Verified by Visa and MasterCard Secure Code; d) modify, adapt, decompile or disassemble, sub-license, translate, sell any portion of 3D Secure; e) deleting any copyright notices (trademarks) encountered by accessing 3D Secure; F) use of any means to retrieve or reproduce the navigation structure, presentation, and content of sites displaying Verified by Visa and MasterCard Secure Code; G) interrupting other users access to 3D Secure, to servers or networks connected to it; H) non-compliance with the Specific Secure Rules and Procedures in general or any network connected to it; I) deliberate or unreasonable violation of any local, national, international, or legal regulations or rules and requirements established by International Visa and MasterCard for the use of 3D Secure

(7) Clientul/Utilizatorul este informat şi este de acord că: (i) 3D Secure conţine informaţii protejate de legea dreptului de proprietate intelectuală şi alte legi aplicabile; (ii) Banca va acorda o licenţă de

(7) The Customer / User is informed and agrees that: (i) 3D Secure contains information protected by the Intellectual Property Law and other applicable laws; (ii) The Bank will grant a non-exclusive

utilizare non-exclusivă a 3D Secure şi a mecanismelor 3D Secure în forma actuală şi a îmbunătăţirilor ce se vor adăuga în timp în concordanţă cu Regulile; (iii) nu va copia, altera sau folosi în nici un fel mărcile de comerţ ale Băncii (proprietatea acesteia), 3D Secure (proprietatea Visa International şi MasterCard International) şi nici logo-urile, produsele şi numele asociate acestui serviciu; (iv) are deplină libertate de a cumpăra bunuri/servicii de pe internet prin accesarea 3D Secure. Totuşi, corespondenţa cu comercianţii aleşi, participarea la promoţii on-line, plata şi livrarea bunurilor/serviciilor cumpărate, orice alte condiţii şi garanţii asociate cu acestea sunt numai de domeniul relaţiei sale cu comerciantul; (v) utilizarea 3D Secure nu înseamnă în nici un fel că Banca, Visa International sau MasterCard recomandă vreun comerciant de internet sau garantează calitatea bunurilor/serviciilor acestuia; (vi) orice litigiu cu privire la nerespectarea de către comerciant a condiţiilor de plată, livrare, calitate a bunurilor/serviciilor achiziţionate se pot rezolva exclusiv între Client/Utilizator şi comerciant; (vii) este recomandată reţinerea a cât mai multor informaţii despre comerciant şi despre tranzacţia efectuată, prin salvarea pe calculatorul personal a condiţiilor de livrare, detaliilor tranzacţiei, corespondenţei purtate cu comerciantul etc.

(8) Răspundere. a) Clientul/Utilizatorul 3D Secure răspunde pentru: (i) confidenţialitatea Elementelor de securitate; (ii) tranzacţiile pe internet efectuate utilizând 3D Secure, chiar şi în cazul în care Banca dezactivează temporar/permanent accesul utilizatorului la 3D Secure, intelegand ca aceste tranzactii sunt irevocabile şi nu pot fi contestate, anularea acestora şi soluţionarea oricărei probleme fiind posibile numai prin înţelegerea cu beneficiarul plăţii.

b) Banca nu răspunde pentru: (i) modificarea, suspendarea sau orice întreruperi în furnizarea 3D Secure datorate unor cauze independente de voinţa Băncii; (ii) defecţiuni ale calculatorului sau în furnizarea serviciilor telefonice apărute în timpul tranzacţiilor pe internet; (iii) eventuale pagube produse prin virusarea echipamentului utilizat în timpul tranzacţiilor; (iv) compromiterea datelor de identificare ca urmare a nerespectării Regulilor; (v) transmiterea mesajului SMS continând codul unic asociat fiecărei tranzacții către un numar de telefon care nu mai este valabil și care nu a fost actualizat de către Client vizitând orice sucursală a Băncii; (vi) Banca, Visa International, Mastercard nu răspund pentru eventuale pagube apărute în urma relaţiilor directe dintre Client/Utilizator şi comercianţi sau cauzate de nerespectarea Regulilor 3D Secure.

license of 3D Secure and 3D Secure mechanisms in their current form and of the improvements that will be added over time in accordance with the Rules; (iii) will not copy, alter or otherwise use the Bank's trade marks (its property), 3D Secure (the property of Visa International and MasterCard International), nor the logos, products and names associated with this service; (iv) has full freedom to buy goods / services from the Internet by accessing 3D Secure. However, correspondence with elected traders, participation in on-line promotions, payment and delivery of purchased goods / services, any other conditions and warranties associated with them are only subjected to its relationship with the merchant; (v) use of 3D Secure does not in any way mean that the Bank, Visa International or MasterCard recommends any internet merchant or guarantees the quality of its goods / services; (vi) any litigation regarding the merchant's failure to comply with the terms of payment, delivery, quality of the purchased goods / services can only be resolved between the Customer / User and the merchant; (vii) it is advisable to retain as much information as possible about the merchant and about the transaction, by saving the delivery terms on the personal computer, details of the transaction, correspondence with the merchant, etc.

(8) Liability. a) The Customer / the 3D Secure User is responsible for: (i) the confidentiality of the Security Elements; (ii) Internet transactions made using 3D Secure, even if the Bank temporarily / permanently disables the user's access to 3D Secure, understanding that these transactions are irrevocable and can not be challenged, their cancellation and resolution of any problem being possible only through an understanding with the payee.

b) The Bank is not responsible for: (i) modifying, suspending or interrupting 3D Secure provision due to causes beyond the Bank's will; (ii) computer malfunctions or the functionality of telephone services during internet transactions; (iii) any damage caused by virus infection of equipment used during transactions; (iv) compromising identification data as a result of non-compliance with the Rules; (v) sending the SMS message containing the unique code associated with each transaction to a phone number that is no longer valid and which has not been updated by the Client by visiting any branch of the Bank; (vi) The Bank, Visa International, Mastercard are not liable for any damage arising out of direct relationship between Customer / User and merchants or caused by non-compliance with the 3D Secure Rules.