

REGULI ȘI CONDIȚII 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 tranzacțiilor de comerț electronic în condiții 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 și MasterCard Secure Code) dacă sunt respectate prezentele reguli și condiții de utilizare ("Reguli"). Serviciul 3D Secure funcționează în condițiile în care site-ul pe care se efectuează tranzacția suportă standardele 3D Secure. Orice modificare a Regulilor va fi notificată pe pagina de internet a Băncii. Tranzacțiile efectuate prin 3D Secure se află sub incidența versiunii în vigoare a Regulilor, la momentul efectuării acestora. Regulile sunt disponibile pe pagina de internet a Băncii.

(2) Banca, Visa Internațional și MasterCard își rezervă dreptul: (i) de a modifica, îmbunătăți ori întrerupe furnizarea acestui serviciu fără o notificare prealabilă; (ii) de a suspenda în orice moment accesul la acest serviciu dacă se dovedește 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 tranzacțiile deja efectuate nu se modifică.

(3) Consimțământul Clientului pentru autorizarea unei operațiuni 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:

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

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

În măsura în care Clientul nu reușește autorizarea operațiunii de plată pe internet după trei încercări consecutive nereușite de introducere a Codului PIN prin Business Mobile/ Mobile Token, caz în care Business Mobile/Mobile Token nu se mai poate accesa, tranzacția poate fi autorizată prin introducerea codului unic generat de către Bancă și transmis către Utilizator prin SMS la numărul de telefon mobil declarat Băncii. Pentru a autoriza o nouă operațiune de plată pe internet prin aplicația Business Mobile/ Mobile Token, aceasta va trebui reactivată.

(4) Clientul poate solicita modificarea numărului de telefon mobil pe care Utilizatorul va primi codul unic asociat fiecărei tranzacții autorizată online prin 3D Secure, printr-o solicitare scrisă în orice sucursală a Băncii, înțelegând că Utilizatorul va putea primi codul

(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) 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) 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) 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) Clients who do not have any of the above services, will authorize 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. The unique code is temporary, only valid for the transaction for which it was generated.

In case the Client cannot authorize the internet payment operation after three consecutive attempts to enter the PIN through Business Mobile / Mobile Token, case in which Business Mobile / Mobile Token can no longer be accessed, the transaction can be authorised by entering the unique code generated by the Bank and communicated to the User through SMS to the mobile number declared to the Bank. In order to authorize a new internet payment operation through Business Mobile / Mobile Token, the application will need to be reactivated.

(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

unic prin SMS la noul numar in aceeași zi lucratoare, după ora 17.30, pentru solicitările depuse până în ora 16:00, respectiv în următoarea zi lucrătoare, după ora 17:30, pentru solicitările depuse după ora 16:00.

(5) Clientul/Utilizatorul 3D Secure are următoarele obligații: (i) va citi cu atenție Regulile; (ii) nu va dezvălui, sub nici o formă, comercianților virtuali sau unor terți datele sale personale sau Elementele de securitate; (iii) în situația în care consideră că a fost compromisă confidențialitatea datelor sale (număr card, data expirării, cod numeric personal, cod unic asociat fiecărei tranzacții) va notifica imediat Banca pentru blocarea cardului până la soluționarea situației; (iii) Clientul va informa de îndată Banca despre orice modificare a datelor oferite în vederea utilizării sau, după caz, orice modificare a numărului de telefon declarat Băncii; (vii) înainte de furnizarea oricărei date de identificare în vederea realizării unei plăți, va verifica autenticitatea site-ului de plată, urmărind cel puțin: (a) afișarea siglelor aferente serviciilor Verified by Visa și MasterCard SecureCode; (b) certificatele de securitate ale paginilor ce solicită astfel de date; (c) afișarea mesajelor de întâmpinare aferente 3D Secure.

(6) Clientului/Utilizatorului 3D Secure îi este interzisă: a) substituția unei alte persoane /entități care utilizează 3D Secure; b) trimiterea pe orice cale a unor programe tip virus care să întrerupă, distruge sau să limiteze funcționalitatea oricărei componente hard/soft (inclusiv de comunicații) a 3D Secure; c) trimiterea de spam, pe orice cale și invadarea site-urilor Verified by Visa și MasterCard Secure Code accesate; d) modificarea, adaptarea, decompilarea sau dezasamblarea, sub-licențierea, traducerea, vânzarea oricărei porțiuni a 3D Secure; e) ștergerea 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 și conținutul site-urilor afișând brand-urile Verified by Visa și MasterCard Secure Code; g) întreruperea accesului altor utilizatori la 3D Secure, la servere sau rețele conectate la acesta; h) nerespectarea Regulilor și procedurilor specifice 3D Secure în general sau oricărei rețele conectate la acesta; i) încălcarea, în mod intenționat sau nu, a oricăror reglementări legale locale, naționale, internaționale sau a regulilor și cerințelor stabilite de Visa Internațional și MasterCard pentru folosirea 3D Secure.

(7) Clientul/Utilizatorul este informat și este de acord că: (i) 3D Secure conține informații protejate de legea dreptului de proprietate intelectuală și alte legi aplicabile; (ii) Banca va acorda o licență de utilizare non-exclusivă a 3D Secure și a mecanismelor 3D Secure în forma actuală și a îmbunătățirilor ce se vor adăuga în timp în concordanță cu Regulile; (iii) nu va copia, altera sau folosi în nici un fel mărcile de comerț ale Băncii (proprietatea acesteia), 3D Secure (proprietatea Visa Internațional și MasterCard Internațional) și nici logo-urile, produsele și numele asociate acestui serviciu; (iv) are deplină libertate de a cumpăra bunuri/servicii de pe internet prin accesarea 3D Secure. Totuși, corespondența cu comercianții aleși, participarea la promoții on-line, plata și livrarea bunurilor/serviciilor cumpărate, orice alte condiții și garanții asociate cu acestea sunt numai de domeniul relației sale cu comerciantul; (v) utilizarea 3D Secure nu înseamnă în nici un fel că Banca, Visa Internațional sau MasterCard recomandă vreun comerciant de internet sau garantează calitatea bunurilor/serviciilor acestuia; (vi) orice litigiu cu privire la nerespectarea de către comerciant a condițiilor de plată, livrare, calitate a bunurilor/serviciilor achiziționate se pot rezolva exclusiv între Client/Utilizator și comerciant; (vii) este recomandată reținerea a cât mai multor informații despre comerciant și despre tranzacția efectuată, prin salvarea pe calculatorul personal a condițiilor de livrare, detaliilor tranzacției, corespondenței purtate cu comerciantul etc.

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) 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) 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) 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 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

UniCredit Bank S.A.

Bulevardul Expoziției nr. 1F,
Sector 1, București
Tel +40 21 200 2020
e-mail: infocenter@unicredit.ro

Bancă membră a UniCredit Group - Nr. de ordine
în Registrul Bancar: RB-PJR-40-011/ 18.02.1999
- Capital social: 455.219.478,30 RON - Nr. de
Ordine în registrul Comerțului: J40/7706/1991 -
Cod unic de înregistrare: 361536 - Operator de
date cu caracter personal nr. 10964, societate
administrată în sistem dualist, Cod SWIFT:
BACKROBU

(8) Răspundere. a) Clientul/Utilizatorul 3D Secure răspunde pentru: (i) confidențialitatea Elementelor de securitate; (ii) tranzacțiile pe internet efectuate utilizând 3D Secure, chiar și în cazul în care Banca dezactivează temporar/permanent accesul utilizatorului la 3D Secure, înțelegând că aceste tranzacții sunt irevocabile și nu pot fi contestate, anularea acestora și soluționarea oricărei probleme fiind posibile numai prin înțelegerea cu beneficiarul plății.

b) Banca nu răspunde pentru: (i) modificarea, suspendarea sau orice întreruperi în furnizarea 3D Secure datorate unor cauze independente de voința Băncii; (ii) defecțiuni ale calculatorului sau în furnizarea serviciilor telefonice apărute în timpul tranzacțiilor pe internet; (iii) eventuale pagube produse prin virusarea echipamentului utilizat în timpul tranzacțiilor; (iv) compromiterea datelor de identificare ca urmare a nerespectării Regulilor; (v) transmiterea mesajului SMS conținând codul unic asociat fiecărei tranzacții către un număr 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 relațiilor directe dintre Client/Utilizator și comercianți sau cauzate de nerespectarea Regulilor 3D Secure.

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