

REGULI ȘI CONDIȚII DE UTILIZARE 3D SECURE/ RULES AND CONDITIONS OF USE 3D SECURE

(1) Toate cardurile emise de Bancă, fizice sau virtuale, 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 International 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; și (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, furnizând numărul de card, numele indicat pe card, data expirării, CVV/CVC precum și elementele de Securitate menționate în aliniatele următoare.

(4) În cazul în care Clientul/Utilizatorul deține serviciul Mobile B@nking activ/Mobile Token activ aferent serviciului Online B@nking, consimțământul acestuia pentru autorizarea unei Operațiuni de plată pe internet prin 3D Secure se va efectua prin Autentificare strictă, astfel: (a) în cazul în care Clientul nu are activată opțiunea de a recepționa notificări de tip mesaje "Push" pe telefonul mobil (în cazul Mobile B@nking și Mobile Token) și în aplicație (doar în cazul Mobile B@nking), va accesa Mobile B@nking sau Mobile Token și va autoriza respectiva operațiune de plată prin introducerea Codului PIN sau scanarea amprente digitale / trăsăturilor faciale setate în telefonul mobil, în cazul în care Clientul a optat în acest sens, iar (b) în cazul în care Clientul are activată opțiunea de a recepționa notificări de tip mesaje "Push" pe telefonul mobil (în cazul Mobile B@nking și Mobile Token) și în aplicație (doar în cazul Mobile B@nking), va primi un mesaj care va cuprinde detaliile plății (de ex.: suma operațiunii de plată, valuta de plată și numele beneficiarului etc.) fiind redirectionat în Mobile B@nking/Mobile Token și va autoriza respectiva operațiune de plată, prin introducerea Codului PIN sau scanarea amprente digitale/ trăsăturilor faciale setate în telefonul mobil, în cazul în care Clientul a optat în acest sens.

(5) Clienții care nu au activ niciunul dintre serviciile de mai sus, vor autoriza operațiunile de plată pe internet, prin 3D Secure, utilizând: (i) un cod unic generat de către Bancă pentru fiecare operațiune de plată și transmis Clientului prin SMS, la numărul de telefon mobil declarat Băncii (numărul de telefon trebuie să fie înregistrat la operatori de telefonie mobilă din România), și (ii) parola statică, astfel cum este stabilită în cererea aferentă furnizării și utilizării cardului.

(6) Prin excepție de la regulile autentificării stricte a plăților Banca poate accepta, fără a fi obligată, în baza unei analize de risc efectuată în timp real de către Bancă sau banca comerciantului, să nu solicite elementele de securitate menționate la alineatul (4) sau (5), consimțământul pentru autorizarea plății realizându-se prin furnizarea numărului de

(1) All cards, physical or virtual, issued by the Bank are enrolled in 3D 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 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 case 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

card, numelui indicat pe card, datei expirării și codului CVV/CVC, urmând instrucțiunile comerciantului.

(7) Operațiunea de plată nu va putea fi autorizată și cardul va fi blocat pentru Operațiuni de plată pe internet, în măsura în care Clientul nu reușește autorizarea după (i) cinci încercări consecutive, respectiv: (a) trei încercări consecutive de introducere a Codului PIN, prin Mobile B@nking/Mobile Token, caz în care Mobile B@nking/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 Mobile B@nking/Mobile Token sau (ii) cinci încercări consecutive prin utilizarea codului unic și a Parolei statice, dacă anterior nu s-a încercat autorizarea prin Mobile B@nking/Mobile Token.

(8) 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, sau va bloca singur temporar sau chiar definitiv cardul utilizând funcționalitatea disponibilă în Online B@nking sau Mobile B@nking; (iv) va informa de îndată Banca despre orice modificare a datelor sale; (v) va informa de îndată Banca despre orice modificare a numărului de telefon declarat Băncii, apelând INFO Center ori vizitând orice sucursală a Băncii; (vi) 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 Secure Code; (b) certificatele de securitate ale paginilor ce solicită astfel de date; (c) afișarea mesajelor de întâmpinare aferente 3D Secure.

(9) Clientului/Utilizatorului 3D Secure îi este interzisă: a) substituirea unei alte persoane /entități care utilizează 3D Secure; b) trimiterea pe orice cale a unor programe tip virus care să întrerupă, distrugă 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.

(10) Clientul/Utilizatorul este informat și este de acord că: (i) 3D Secure conține informații protejate de legea dreptului de

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

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 International și Mastercard International) 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 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 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.

(11) Răspundere. a) Clientul/Utilizatorul 3D Secure răspunde pentru păstrarea confidențialității Elementelor de securitate. 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/sau care nu a fost actualizat de către Client; (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.

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 online 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 not 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.