

Intră în vigoare la 08.02.2021Aprobat la Comitetul de conducere al Băncii
proces verbal nr 06 din 03.02.2021

Condițiile de utilizare a serviciului "MICB 3D-Secure"

1. Dispoziții generale

1.1. Prezentele Condiții de utilizare a serviciului "MICB 3D-Secure" (în continuare Condiții de utilizare), stabilite de BC "Moldindconbank" S.A. (în continuare Banca), descriu modul în care Banca oferă clienților săi posibilitatea utilizării serviciului "MICB 3D-Secure" (în continuare Serviciu) cu scopul securizării plăților prin internet, precum și modul de utilizare a acestuia de către deținătorii de card.

1.2. Prezentele Condiții de utilizare completează și detaliază relația contractuală existentă între Deținător și Bancă, în conformitate cu Condițiile generale bancare pentru persoane fizice (în continuare Condiții generale bancare), care sunt puse la dispoziția oricărui Client sau potențial Client, pe panourile informative din cadrul subdiviziunilor Băncii precum și pe pagina web a Băncii, astfel încât acestea să poată fi accesate în orice moment.

1.3. Prezentele Condiții de utilizare pot fi modificate periodic, iar versiunea actualizată a acestora este întotdeauna publicată pe pagina web a Băncii, pentru a fi oricând accesată.

1.4. Tranzacțiile E-commerce, pe care Deținătorul le va efectua prin utilizarea Serviciului, cad sub incidența ultimei versiuni a Condițiilor de utilizare.

1.5. Client eligibil pentru abonarea și utilizarea Serviciului este orice persoană fizică ce deține în Bancă un cont de card de care este atașat un card valabil emis în numele clientului respectiv, sau orice persoană fizică ce deține un card secundar valabil.

1.6. Activarea Serviciului se efectuează automatizat, în cadrul procesului efectuării tranzacțiilor în rețeaua internet la comercianții/site-urile care suportă standardele 3D-Secure.

1.7. Pentru informații suplimentare despre acest Serviciu și tranzacțiile E-commerce sau pentru alte întrebări legate de activarea Serviciului, Deținătorul poate accesa pagina web a Băncii, <http://www.micb.md>, sau poate apela, pentru suport, la numărul de telefon **+373/ 22 54-89-40**.

2. Noțiunile utilizate

2.1. Serviciu "MICB 3D-Secure" - este un serviciu de securizare a plăților prin internet, în baza autentificării electronice a Deținătorului de card la efectuarea tranzacțiilor E-commerce pe internet-site-uri, care suportă tehnologia respectivă. Sistemul este bazat pe protocoalele internaționale 3D-Secure - *MasterCard Secure Code* și *Verified by Visa*. Aplicarea tehnologiei 3D-Secure pe un anumit internet-site, de obicei, se identifică prin afișarea logotipului "**MasterCard SecureCode**" – pentru cardurile emise sub egida Mastercard Worldwide și/sau "**Verified by Visa**" – pentru cardurile emise sub egida Visa International.

2.2. Autentificarea electronică - verificarea identității Deținătorului de card cu datele existente în bazele de date ale Băncii, prin intermediul factorilor de autentificare, cu scopul de a determina dacă persoana care efectuează tranzacția prin intermediul cardului emis de Bancă este, de fapt, Deținătorul real al cardului respectiv.

2.3. Factor de autentificare – parola obținută prin autentificarea de tip SMS OTP, ATM OTP sau Mobile OTP.

2.4. Autentificarea SMS OTP – tipul autentificării care prevede transmiterea de către Bancă în adresa Deținătorului (prin intermediul operatorului de telefonie mobilă cu care Banca a încheiat contract) a unei parole de unică folosință în cadrul unui mesaj SMS la numărul de telefon OTP și introducerea acestei parole de către Deținător în interfața serviciului "MICB 3D-Secure" afișată la efectuarea tranzacțiilor E-commerce.

Notă: Dacă accesul la numărul personal de telefon este limitat din cauza aflării peste hotare, ca alternativă, Deținătorul poate utiliza, la efectuarea tranzacțiilor prin Internet, un alt factor de autentificare – ATM OTP sau Mobile OTP:

- Mobile OTP – prin activarea **în prealabil** a aplicației [MICB Mobile-Banking](#) și setării codului de acces;
- ATM OTP – prin obținerea **în prealabil** a listei de parole unice la unul din bancomatele Băncii.

2.5. Număr de telefon OTP – numărul de telefon mobil utilizat pentru transmiterea parolei OTP stabilit de către Deținător:

- în cadrul serviciului "SMS-notificări", sau
- comunicat Băncii în cadrul Chestionarului pentru client – persoană fizică,

cu condiția că acest număr de telefon este gestionat de unul din următorii operatori de telefonie mobilă: Moldcell (ÎM "Moldcell" S.A.), Orange ("Orange Moldova" S.A.) și Unite ("Moldtelecom" S.A.).

Notă: La modificarea Numărului de telefon pentru SMS-notificări prin canalele Băncii, accesibile la momentul modificării, cu excepția modificării prin canalele Web- și Mobile-banking, se va modifica automat și Numărul de telefon OTP. În același timp, la modificarea Numărului de telefon OTP prin canalele Băncii accesibile la momentul modificării – automat se va modifica și Numărul de telefon pentru SMS-notificări.

2.6. Autentificarea ATM OTP – tipul autentificării care presupune recepționarea de către Deținător a unei liste de parole de unică folosință prin intermediul bancomatului Băncii și introducerea acestor parole, de către Deținător, în interfața serviciului "MICB 3D-Secure", afișată la efectuarea tranzacțiilor E-commerce.

2.7. Autentificarea Mobile OTP – tipul autentificării care presupune generarea de către Deținător a unei parole de unică folosință, prin intermediul aplicației **MICB Mobile Banking**, în baza codului generat în aplicația "MICB Mobile Banking" și introducerea acestei parole, de către Deținător, în interfața serviciului "MICB 3D-Secure", afișată la efectuarea tranzacțiilor E-commerce.

2.8. MICB Mobile Banking, Aplicație – sistem automatizat de deservire la distanță a Deținătorilor de carduri de tipul "mobile-banking", care utilizează tehnologia aplicațiilor mobile, disponibil spre a fi descărcat și instalat în magazinele virtuale oficiale "App Store" și "Google Play".

2.9. Codul de acces - cod numeric de acces la aplicație "**MICB Mobile Banking**" generat de către Deținător în aplicația respectivă.

2.10. Elementele de securitate ale cardului - codul PIN, codul CVV2/CVC2, numărul cardului, data expirării cardului, codul de acces și/sau alte elemente de securitate convenite în prealabil între Deținător și Bancă.

2.11. Tarife – [Tarifele și limitele privind deservirea cardurilor bancare emise de BC "Moldindconbank" S.A.](#), afișate pe panourile informative la subdiviziunile Băncii, precum și plasate pe pagina web a Băncii <http://www.micb.md/planuri-tarifare>.

2.12. Card – card de plată emis de BC "Moldindconbank" S.A. pe numele Deținătorului, în conformitate cu contractul încheiat între Deținător și Bancă.

2.13. Deținător de card (Deținător) – persoana fizică pe numele căreia este emis cardul.

2.14. Cont de card – contul deschis și menținut de către Deținătorul principal la Bancă, cu scopul înscrierii tranzacțiilor cu carduri, precum și a altor operațiuni prevăzute de [Condițiile generale bancare](#).

2.15. Bancă – prestatorul serviciului "MICB 3D-Secure" - BC "Moldindconbank" S.A.;

2.16. Tranzacții E-commerce – tranzacțiile financiare efectuate prin intermediul rețelei internet: în internet-magazine și alți furnizori de servicii.

2.17. Sistemele Internaționale de plăți – Visa International și/sau Mastercard Worldwide.

2.18. Serviciul suport carduri 24/24 - serviciul Băncii care asigură suportul Deținătorilor de card prin telefon / e-mail, 24/24 de ore. Linia telefonică fierbinte /+373 22/ 54 89 40, e-mail: client.service@micb.md.

3. Descrierea serviciului "MICB 3D-Secure"

3.1. Serviciul "MICB 3D-Secure" pune la dispoziția Deținătorului cel mai înalt standard internațional de securitate a tranzacțiilor E-commerce, care se bazează pe autentificarea sigură a Deținătorilor de card în procesul efectuării tranzacțiilor și le oferă acestora protecție maximă la comercianții/site-urile care suportă standardele 3D-Secure, prezentând logo-urile "MasterCard SecureCode" și/sau "Verified by Visa".

4. Activarea serviciului "MICB 3D-Secure"

4.1. Activarea Serviciului se efectuează în cadrul sesiunii de efectuare a tranzacției E-commerce.

4.2. Activarea Serviciului se efectuează prin introducerea numărului unui card valabil emis pe numele Deținătorului și efectuarea:

- Autentificării de tip "SMS OTP", sau
- Autentificării de tip "Mobile OTP", sau
- Autentificării de tip "ATM OTP".

4.3. La activarea Serviciului, Deținătorul atestă faptul că efectuarea tranzacției E-commerce cu utilizarea factorilor de autentificare reprezintă confirmarea acceptării exprese de către Deținător a prezentelor Condiții de utilizare și a Tarifelor Băncii, iar Banca și sistemele de plăți Visa International și/sau Mastercard Worldwide nu pot fi ținute responsabile pentru eventualele pagube cauzate de nerespectarea prezentelor Condiții de utilizare.

4.4. Banca, împreună cu sistemele de plăți Visa International și/sau Mastercard Worldwide își rezervă dreptul de a modifica, îmbunătăți ori întrerupe furnizarea acestui Serviciu, fără a fi necesară o notificare prealabilă.

4.5. Pentru utilizarea Serviciului, Deținătorul furnizează anumite informații care vor permite verificarea identității acestuia prin suprapunere cu datele existente în bazele de date ale Băncii, pentru a se determina dacă clientul respectiv este Deținătorul real al cardului cu care se dorește a se efectua plățile pentru tranzacții E-commerce.

4.6. Deținătorul nu are dreptul să utilizeze, în procesul activării Serviciului, cardul sau datele oricărui card, altul decât cel emis pe numele său.

4.7. Activarea Serviciului poate fi efectuată doar personal, de către Deținător.

4.8. Banca își rezervă dreptul de a refuza activarea Serviciului dacă Deținătorul nu furnizează informațiile necesare pentru verificarea identității sale.

4.9. Prin activarea Serviciului, Deținătorul autorizează Banca să rețină datele sale personale și informațiile despre cardurile deținute și să le folosească în conformitate cu prevederile prezentelor Condiții de utilizare și ale legislației în vigoare.

4.10. Deținătorul confirmă corectitudinea și veridicitatea datelor oferite și asigură Banca că va informa cu promptitudine despre orice modificare a acestora

5. Utilizarea serviciului "MICB 3D-Secure"

5.1. Ca urmare a activării Serviciului, Deținătorul poate beneficia de avantajele plăților securizate la efectuarea tranzacțiilor E-commerce la comercianții/site-urile care suportă standardele 3D-Secure.

5.2. Deținătorul înțelege și acceptă faptul că, pentru efectuarea tranzacțiilor E-commerce la comercianții/site-urile care suportă standardele 3D-Secure, acesta urmează să se autentifice în baza factorilor de autentificare accesibili la momentul efectuării tranzacției corespunzătoare.

5.3. La utilizarea Serviciului, Deținătorul atestă că efectuarea tranzacției E-commerce, cu utilizarea factorilor de autentificare, reprezintă confirmarea acceptării exprese de către Deținător a prezentelor Condiții de utilizare, Condițiilor generale bancare și Tarifelor Băncii, iar Banca și sistemele de plăți Visa International și/sau Mastercard Worldwide nu sunt responsabile pentru eventualele pagube cauzate de nerespectarea prezentelor Condiții de utilizare.

5.4. Banca își rezervă dreptul de a refuza utilizarea Serviciului și, eventual, efectuarea tranzacțiilor E-commerce la comercianții/site-urile care suportă standardele 3D-Secure, în cazul în care se dovedește că datele personale ale Deținătorului, furnizate Băncii pentru verificarea identității acestuia sunt false, inexacte, neactualizate sau incomplete, și/sau deținătorul nu respectă prevederile prezentelor Condiții de utilizare.

5.5. Deținătorul înțelege și acceptă necesitatea asigurării accesului său la factorii de autentificare pentru a putea beneficia de Serviciu.

6. Securitatea serviciului "MICB 3D-Secure"

6.1. Reieșind din faptul că factorul principal al securității sistemului este autentificarea, securitatea sistemului este asigurată prioritar de necompromiterea elementelor de securitate și a factorilor de autentificare. Astfel, Deținătorul trebuie să asigure:

- 6.1.1.** Necompromiterea elementelor de securitate ale cardului. Cerințele de securizare ale acestora sunt descrise în [Condițiile generale bancare](#);
 - 6.1.2.** Necompromiterea factorului de autentificare "SMS OTP". Compromiterea acestui factor este situația în care Deținătorul nu este ferm convins asupra faptului că mesajele transmise pe numărul de telefon OTP nu sunt accesibile persoanelor terțe;
 - 6.1.3.** Necompromiterea parolelor de unică folosință "ATM OTP". Compromiterea ATM OTP este situația în care Deținătorul nu este ferm convins asupra faptului că acestea nu sunt accesibile persoanelor terțe;
 - 6.1.4.** Necompromiterea factorului de autentificare "Mobile OTP". Compromiterea acestui factor este situația în care Deținătorul nu este ferm convins asupra faptului că telefonul / dispozitivul mobil la care este setată aplicația "MICB Mobile Banking" nu este accesibil persoanelor terțe și/sau codul de acces sau alți factori biometrici de autentificare setat pentru aplicația "MICB Mobile Banking" nu sunt accesibili persoanelor terțe.
- 6.2.** Cu scopul prevenirii compromiterii factorilor de autentificare, Deținătorul trebuie:
- 6.2.1.** să asigure protejarea calculatorului / telefonului mobil / dispozitivului mobil al său, utilizând softul specializat (antivirus, firewall etc.), politicile de limitare a accesului la resurse și alte metode de asigurare a securității informaționale;
 - 6.2.2.** să nu înscrie/păstreze codul de acces/parola pe un suport care permite compromiterea Serviciului, prin natura sau poziționarea sa.
- 6.3.** În cazul în care unul din factorii de autentificare este compromis, Deținătorul trebuie:
- 6.3.1.** să anunțe imediat Banca prin contactarea Serviciului suport carduri 24/24 și să comunice detaliile privind circumstanțele compromiterii și eventualele efecte ale acesteia;
 - 6.3.2.** să verifice atent tranzacțiile efectuate din numele său pentru a detecta înregistrarea tranzacțiilor frauduloase.
- 6.4.** În cazul în care parola (sau lista de parole) "ATM OTP" este compromisă, Deținătorul trebuie să solicite anularea listei respective de "ATM OTP" prin una din următoarele modalități:
- 6.4.1.** să genereze o nouă listă de ATM OTP;
 - 6.4.2.** să contacteze Serviciul suport carduri 24/24 al Băncii pentru a anula lista de parole ATM OTP.
- 6.5.** În cazul în care factorul SMS OTP este compromis, Deținătorul trebuie să întreprindă una sau mai multe din următoarele măsuri:
- 6.5.1.** să solicite operatorului de telefonie mobilă suspendarea numărului de telefon;
 - 6.5.2.** să solicite Băncii, prin contactarea Serviciului suport carduri 24/24, blocarea transmiterii SMS OTP la numărul de telefon OTP setat în sistemul informațional al Băncii;
- 6.6.** În cazul în care factorul Mobile OTP este compromis, Deținătorul trebuie să întreprindă una din următoarele măsuri:
- 6.6.1.** să modifice codul de acces;
 - 6.6.2.** să contacteze Serviciul suport carduri 24/24 al Băncii pentru a suspenda accesul la aplicația "MICB Mobile Banking".
- 6.7.** Banca protejează datele transmise între serverul Serviciului și telefonul mobil / dispozitivul mobil prin cifrarea acestora.
- 6.8.** Deținătorul va respecta următoarele recomandări ale Băncii, cu privire la modalitățile de utilizare securizată a Serviciului:
- 6.8.1.** Nu va divulga altor persoane elementele de securitate ale cardului, factorii de autentificare și alte informații confidențiale (parole, codul de acces, conturi, datele personale, etc.);
 - 6.8.2.** Nu va lăsa dispozitivul fără supraveghere, în special după procedura de autentificare și se va asigura că ecranul dispozitivului nu este vizibil altor persoane;
 - 6.8.3.** Va nimici securile cu parolele OTP dacă acestea nu vor fi utilizate;
 - 6.8.4.** Va descărca aplicațiile mobile numai din magazinele oficiale AppStore și GooglePlay. Toate alte surse nu sunt oficiale și Banca nu poartă răspundere pentru consecințele instalării aplicațiilor descărcate din aceste surse;
 - 6.8.5.** În cazul pierderii sau furtului dispozitivului mobil, va schimba urgent parola de acces la sistemul automatizat de deservire la distanță "MICB Mobile Banking", va informa imediat Banca pentru blocarea cardurilor și accesului la aplicație, după care va suna operatorul telefoniei mobile pentru blocarea cartei SIM;

- 6.8.6.** În cazul schimbării numărului de telefon sau neutilizării acestuia pentru o perioadă de timp mai mare decât valabilitatea lui, va informa Banca pentru deconectarea Serviciului de la numărul de telefon pentru a evita compromiterea modalității de autentificare SMS OTP;
- 6.8.7.** Va fi vigilent la atacurile de tip *phishing* scopul cărora este obținerea de la deținător a informației confidențiale. Nu va răspunde la e-mailuri sau SMS prin care se solicită divulgarea datelor confidențiale sau care direcționează către pagini web în care se solicită, sub diverse motive, informații confidențiale legate de conturi bancare, numărul de card, data expirării acestuia, codul PIN etc. Nici o bancă, magazin online sau orice altă instituție nu solicită prin e-mail sau SMS astfel de informații!
- 6.8.8.** Va monitoriza regulat operațiunile executate. Extrasul de cont și card va permite depistarea la timp și semnalarea operativă a Băncii despre neregulile identificate;
- 6.8.9.** În cazul nefuncționării cartelei SIM, va suna imediat la operatorul telefoniei mobile pentru a se asigura că acest fapt nu este o urmare a acțiunilor frauduloase, etc.

7. Interdicții

Deținătorul înțelege și acceptă, pe deplin, următoarele interdicții:

- 7.1.** 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 Serviciului accesat.
- 7.2.** Trimiterea de spam, pe orice cale, și invadarea site-urilor *Verified by Visa* și *MasterCard Secure Code* accesate.
- 7.3.** Modificarea, adaptarea, decompilarea sau dezasamblarea, sub-licențierea, traducerea, vânzarea oricărei porțiuni a serviciului "MICB 3D-Secure".
- 7.4.** Ștergerea oricărei notificări privind drepturile de proprietate (*copyright, trademark*) despre care a fost informat, prin accesul la acest Serviciu.
- 7.5.** Utilizarea oricăror mijloace (aplicații de căutare, device-uri, procese) pentru regăsirea sau reproducerea structurii de navigare, prezentare și conținutul site-urilor afișând brand-urile *Verified by Visa* și *MasterCard Secure Code*.
- 7.6.** Întreruperea accesului altor Deținători la acest Serviciu, la serverele sau rețelele conectate la acesta.
- 7.7.** Încălcarea, în mod intenționat sau din imprudență, a prezentelor Condiții de utilizare, Condițiile generale bancare, precum și a oricăror reglementări legale naționale, internaționale sau a regulilor și cerințelor stabilite de Visa și Mastercard pentru folosirea acestui Serviciu.

8. Drepturile și obligațiile părților

- 8.1.** Părțile își asumă drepturile și obligațiile menționate în prezentele Condiții de utilizare, cât și cele stabilite în Condițiile generale bancare.
- 8.2.** Banca este obligată:
 - 8.2.1.** să execute activarea și să asigure funcționarea Serviciului, în conformitate cu regimul de prestare a Serviciului respectiv definit în prezentele Condiții de utilizare precum și cu regulile Sistemelor Internaționale de plăți;
 - 8.2.2.** să ia toate măsurile necesare pentru prevenirea riscurilor ce pot apărea în urma utilizării frauduloase a Serviciului și să asigure măsurile aplicate în vederea identificării Deținătorului și asigurării confidențialității, autenticității și non-repudierii tranzacțiilor electronice;
 - 8.2.3.** să asigure Deținătorului posibilitatea de a anunța situațiile de urgență și de a lua toate măsurile necesare pentru a stopa imediat executarea tranzacțiilor frauduloase prin intermediul Serviciului din momentul în care a fost înștiințată, asigurând deținătorul cu mijloace care să poată dovedi că comunicarea a fost efectuată (data, ora înregistrării și numărul de înregistrare a comunicării);
- 8.3.** Deținătorul este obligat:
 - 8.3.1.** să ia cunoștință de prezentele Condiții de utilizare și de Condițiile generale bancare, înaintea activării Serviciului, și să utilizeze Serviciul în strictă conformitate cu prevederile acestora;
 - 8.3.2.** să asigure confidențialitatea și să nu divulge, sub nici o formă, elementele de securitate ale cardului;
 - 8.3.3.** să asigure confidențialitatea și să nu divulge, sub nici o formă, factorii de autentificare (SMS OTP, ATM OTP, Mobile OTP), să ia măsuri rezonabile de protejare a acestora împotriva compromiterii și să nu admită utilizarea acestora de către terțe persoane;

8.3.4. să înștiințeze imediat Banca (prin intermediul Serviciului suport carduri 24/24 sau la ghișeele Băncii) în cazul în care::

- a. are suspiciuni cu privire la posibilitatea cunoașterii de către persoane neautorizate a factorilor de autentificare deținute de Deținător;
- b. are suspiciuni cu privire la cunoașterea de către persoane neautorizate a elementelor de securitate a cardurilor (codul PIN, codul CVV2/CVC2, numărul cardului, data expirării cardului, codul de acces și/sau alte elemente de securitate convenite în prealabil între Deținător și Bancă);
- c. constată erori sau nereguli apărute în urma utilizării Serviciului;
- d. constată disfuncționalități ale Serviciului, erori la autentificare;
- e. recepționează (inclusiv din numele Băncii) prin orice canal de comunicare (SMS, e-mail, telefon, rețele de socializare etc.) solicitări de a comunica elementele de securitate ale cardului, factorii de autentificare și alte informații confidențiale (parole, codul de acces, conturi, datele personale, etc.).

8.3.5. Înainte de furnizarea oricăror elemente de securitate și/sau factori de autentificare în vederea realizării unei tranzacții E-commerce, Deținătorul se obligă să verifice autenticitatea site-ului, urmărind cel puțin: (i) afișarea siglelor *Verified by Visa* sau *MasterCard SecureCode*; (ii) certificatele de securitate ale paginilor ce solicita astfel de date; (iii) afișarea mesajelor de informare aferente serviciul "MICB 3D-Secure".

8.3.6. să manifeste o atitudine responsabilă privind respectarea securității Serviciului.

8.4. Banca are dreptul:

8.4.1. să perceapă taxele și comisioanele conform Tarifelor;

8.4.2. să nu primească spre executare, prin intermediul Serviciului, tranzacțiile electronice, dacă obligația de primire a acestora nu este prevăzută în prezentele Condiții de utilizare.

8.5. Banca nu poartă răspundere pentru daunele suportate de deținător de pe urma nerespectării Condițiilor de utilizare.

9. Responsabilitatea părților

9.1. Deținătorul este responsabil de veridicitatea și corectitudinea informației transmise prin intermediul Serviciului, pentru confidențialitatea și necompromiterea elementelor de securitate a cardului, factorilor de autentificare și, implicit, pentru tranzacțiile E-commerce efectuate accesând Serviciul, în cazul în care a avut loc autentificarea deținătorului bazată pe factorii de autentificare deținute de deținător, inclusiv cele efectuate fraudulos de către persoanele terțe, până la suspendarea factorilor de autentificare (ATM OTP, SMS OTP, Mobile OTP) cu utilizarea cărora a fost autentificată tranzacția respectivă.

9.2. Banca și Deținătorul recunosc puterea juridică a tranzacțiilor E-commerce efectuate cu accesarea Serviciului.

9.3. Banca și Deținătorul recunosc că documentele electronice transmise în cadrul Serviciului sunt echivalente celor depuse personal și semnate cu semnătura olografă, și produc aceleași drepturi și obligațiuni ale părților.

9.4. Banca va lua toate măsurile necesare pentru prevenirea riscurilor ce pot apărea din utilizarea frauduloasă a Serviciului. Banca este responsabilă:

9.4.1. pentru neexecutarea sau executarea necorespunzătoare a tranzacțiilor E-commerce efectuate cu accesarea Serviciului, în cazul în care executarea necorespunzătoare este atribuită unei disfuncționalități a Serviciului sau a unei componente a acestuia, această disfuncționalitate fiind determinată de acțiunile sau responsabilitate Băncii și, de asemenea, cu condiția că disfuncționalitatea nu a fost cauzată intenționat de către Deținător;

9.4.2. pentru tranzacțiile E-commerce inițiate **după** momentul notificării Băncii de către Deținător referitoare la pierderea controlului asupra elementelor de securitate ale cardului și/sau factorilor de autentificare;

9.5. Banca nu poate fi responsabilă și nu poartă răspundere pentru: (i) modificarea, suspendarea sau orice întreruperi în furnizarea Serviciului datorate unor cauze independente de voința Băncii; (ii) defecțiuni ale calculatorului sau executarea necorespunzătoare, inclusiv, cu întârziere, de către operatorul de telefonie mobilă a serviciilor sale telefonice de expediere a SMS-urilor către Deținător, la inițierea de către Deținător a tranzacțiilor E-commerce sau pe parcursul derulării tranzacțiilor E-commerce; (iii) eventuale pagube produse prin virusarea echipamentului deținătorului în timpul tranzacțiilor E-commerce.

9.6. Plățile efectuate cu ajutorul serviciului "MICB 3D-Secure" sunt irevocabile și nu pot fi contestate la Bancă din motive de fraudă.

10. Relația cu comercianții

10.1. Deținătorul are deplina libertate de a efectua tranzacții E-commerce prin accesarea serviciului "MICB 3D-Secure". În același timp, corespondența cu comercianții aleși, participarea la promoții on-line, plata și livrarea bunurilor/serviciilor cumpărate, orice alte condiții și garanții asociate cu acestea țin numai de domeniul relației Deținătorului cu comerciantul respectiv. Banca și sistemele internaționale de plăți nu pot fi ținute responsabile sub nici o formă de eventualele pagube apărute în cadrul relației directe a Deținătorului cu comercianții.

10.2. Deținătorul recunoaște pe deplin că utilizarea Serviciului nu înseamnă în nici un fel că Banca și Sistemele Internaționale de plăți recomandă vreun comerciant sau garantează calitatea bunurilor/serviciilor sale.

10.3. Orice litigiu cu privire la nerespectarea de către comerciant a condițiilor de plată, livrare, calitate a bunurilor/serviciilor achiziționate urmează a fi soluționat exclusiv între Deținător și acesta. În acest sens trebuie reținute cât mai multe informații despre comerciant și salvată pagina conținând dovada efectuării tranzacției, condițiile de livrare, detaliile tranzacției, corespondența purtată cu comerciantul etc.

11. Dispozițiile finale

11.1. Relațiile dintre Bancă și Deținător care apar în rezultatul utilizării Serviciului 3D Secure și care nu sunt specificate în prezentele Condiții de utilizare, vor fi reglementate în conformitate cu regulile Sistemelor Internaționale de plăți și legislația în vigoare a Republicii Moldova.

11.2. Toate neînțelegerile și/sau litigiile apărute între Deținător și Bancă pe marginea utilizării Serviciului vor fi soluționate pe cale amiabilă, prin negociere. În cazul epuizării tuturor mijloacelor de soluționare pe cale amiabilă a litigiilor, acestea vor fi soluționate de către instanțele de judecată competente, în conformitate cu legislația Republicii Moldova.

11.3. Banca va informa Deținătorii privind modificarea prezentelor Condiții de utilizare, Condițiilor generale bancare și/sau Tarifelor prin afișarea versiunii(lor) modificate a(ale) acestor documente pe pagina Web a Băncii: (<https://www.micb.md>) și panoul informațional în cadrul subdiviziunilor Băncii.