MOLDINDCONBANK

Republica Moldova,MD 2012
Chișinău, str. Armenească, 38
Tel.:+373 22 **54-89-40**

Intră în vigoare la 09.01.2019
Aprobat la Comitetul de conducere al Băncii
la 02.11.2018, procesul verbal nr. 133

Condițiile de utilizare a serviciului ”MICB 3D-Secure” (în redacție nouă)

1. Dispoziții generale

1.1. Prezentele Condiţii 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 clienţilor săi posibilitatea utilizării serviciului ”MICB 3D-Secure” (în continuare Serviciu) cu scopul securizării plăţilor prin internet, precum şi modul de utilizare a acestuia de către deținătorii de card. Prezentele Condiţii de utilizare sunt accesibile pe pagina web a Băncii http://www.micb.md/sec/3D-secure/.

1.2. Prezentele Condiţii de utilizare completează şi detaliază relaţia contractuală existentă între Deţinător şi Bancă, în conformitate cu Regulile de funcționare a contului de card și utilizare a cardului atașat. Regulile sunt accesibile la orice ghişeu al Băncii sau pe pagina web http://www.micb.md/img/smartbanking/reguli-utilizare-carduri.pdf.

1.3. Prezentele Condiţii de utilizare pot fi modificate periodic, fiind accesibile pe pagina web a Băncii http://www.micb.md/sec/3D-secure/. Tranzacţiile E-commerce pe care Deţinătorul le va efectua prin utilizarea Serviciului cad sub incidenţa ultimei versiuni a Condiţiilor de utilizare.

1.4. Client eligibil pentru abonarea şi utilizarea Serviciului este orice persoană fizică care deţine în Bancă un cont de card de care este ataşat un card valabil emis în numele clientului respectiv, sau orice persoană fizică care deţine un card secundar valabil.

1.5. Activarea Serviciului se efectuează automatizat în cadrul procesului efectuării tranzacţiilor în reţeaua internet la comercianţii/site-urile care suportă standardele 3D-Secure. î

1.6. Pentru informaţii suplimentare despre acest Serviciul şi tranzacţiile E-commerce sau pentru alte întrebări legate de activarea Serviciului, Deţinătorul poate accesa pagina de internet a Băncii, http://www.micb.md/sec/3D-secure/, sau la numărul de telefon **/+373/ 22 54-89-40**.

2. Noţiunile utilizate

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

2.2. Autentificarea electronică - verificarea identităţii Deţinătorului de card cu datele existente în bazele de date a Băncii, prin intermediul factorilor de autentificare, cu scopul determinării că persoana care efectuează tranzacţia prin intermediul cardului emis de Bancă, este de fapt Deţinătorul real al cardului respectiv.

2.3. Factor de autentificare – parola obţinută 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 Deţinătorului (prin intermediul operatorului de telefonie mobilă cu care Banca a încheiat contract) a unei parole de unică folosinţă în cadrul unui mesaj SMS la numărul de telefon OTP şi introducerea acestei parole de către Deţinător în interfaţa serviciului ”MICB 3D-Secure” afişată la efectuarea tranzacţiilor E-commerce.

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

- Mobile OTP – prin activarea **în prealabil** a aplicaţiei MICB Mobile-Banking şi setării codului de acces,

- ATM OTP – prin obţinerea **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 Deţinător:

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

cu condiţie 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.) şi Unite (”Moldtelecom” S.A.).

Notă! La modificarea Numărului de telefon SMS prin canalele Băncii accesibile la momentul modificării, cu excepţia modificării prin canalele Web- şi Mobile-banking, automat se va modifica şi Numărul de telefon OTP. În acelaşi timp la modificarea Numărului de telefon OTP prin canalele Băncii accesibile la momentul modificării – automat se va modifica şi Numărul de telefon SMS.

2.6. Autentificarea ATM OTP – tipul autentificării care prevede primirea de către Deţinător a unei liste de parole de unică folosinţă prin intermediul bancomatului Băncii şi introducerea acestei parole de către Deţinător în interfaţa serviciului ”MICB 3D-Secure”, afişată la efectuarea tranzacţiilor E-commerce.

2.7. Autentificarea Mobile OTP – tipul autentificării care prevede generarea de către Deţinător a unei parole de unică folosinţă prin intermediul aplicaţiei **MICB Mobile Banking**, în baza codului generat în aplicația ”MICB Mobile Banking”; şi introducerea acestei parole de către Deţinător în interfaţa serviciului ”MICB 3D-Secure”, afişată la efectuarea tranzacţiilor E-commerce.

2.8. MICB Mobile Banking, Aplicaţie – este un sistem automatizat de deservire la distanţă a Deţinătorilor de carduri de tipul ”mobile-banking”, care utilizează tehnologia aplicaţiilor mobile, fiind accesibil a fi instalat din magazinele virtuale oficiale ”App Store” şi ”Google Play”.

2.9. Codul de acces - cod numeric de acces la aplicaţie **”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 şi/sau alte elemente de securitate convenite în prealabil între Deţinător şi Bancă.

2.11. Tarife – Tarifele şi limitele privind deservirea cardurilor bancare emise de BC ”Moldindconbank” S.A., publicate pe panourile informative ale subdiviziunilor Băncii, precum şi pe pagina web http://www.micb.md/planuri-tarifare/.

2.12. Card – card de plată emis de BC ”Moldindconbank” S.A. pe numele Deţinătorului, în conformitate cu Contractul încheiat între Deţinător şi Bancă.

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

2.14. Cont de card – contul deschis şi menţinut de către Deţinătorul principal la Bancă, cu scopul înscrierii tranzacţiilor cu carduri, precum şi a altor operaţiuni prevăzute de contractul respectiv.

2.15. Bancă – BC ”Moldindconbank” S.A., furnizorul Serviciului;

2.16. Tranzacţii E-commerce – tranzacţiile financiare efectuate prin intermediul reţelei internet: în internet-magazine şi alţi furnizori de servicii.

2.17. Sistemele Internaţionale de plăţi – Visa International şi/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 dispoziţia Deţinătorului cel mai înalt standard internaţional de securitate a tranzacţiilor E-commerce, care se bazează pe autentificarea univocă a Deţinătorilor de card în procesul efectuării tranzacţiilor şi le oferă acestora protecţie maximă, la comercianţii/site-urile care suportă standardele 3D-Secure, prezentând logo-urile "MasterCard SecureCode" şi/sau "Verified by Visa".

4. Activarea serviciului ”MICB 3D-Secure”

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

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

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

4.3. La activarea Serviciului Deţinătorul recunoaşte faptul că efectuarea tranzacţiei E-commerce cu utilizarea factorilor de autentificare reprezintă confirmarea acceptării exprese de către Deţinător a prezentelor Condiţii de utilizare şi Tarifelor Băncii, iar Banca, Visa International şi/sau Mastercard Worldwide nu pot fi făcute responsabile pentru eventualele pagube cauzate de nerespectarea prezentelor Condiţii de utilizare.

4.4. Banca, Visa International şi/sau Mastercard Worldwide îşi rezervă dreptul de a modifica, îmbunătăţi ori întrerupe furnizarea acestui Serviciu fără a fi necesară o notificare prealabilă.

4.5. Pentru utilizarea Serviciului Deţinătorul furnizează anumite informaţii care vor permite verificarea identităţii acestuia cu datele existente în bazele de date a Băncii, pentru a determina faptul că clientul respectiv este Deţinător real al cardului cu care se doreşte de a efectua plăţile pentru tranzacţii E-commerce.

4.6. Deţinătorul nu are dreptul să utilizeze în procesul activării cardul sau datele unui alt card decât cel emis pe numele său.

4.7. Activarea poate să fie efectuată doar personal de către deţinător şi nu poate fi efectuată de către mandatar, tutore, reprezentant legal sau orice altă persoană terţă.

4.8. Banca îşi rezervă dreptul de a refuza activarea Serviciului dacă Deţinătorul nu furnizează informaţiile necesare pentru verificarea identităţii.

4.9. Prin activarea Serviciului Deţinătorul autorizează Banca să reţină datele sale personale şi informaţiile despre cardurile deţinute şi să le folosească în conformitate cu prevederile prezentelor Condiţii de utilizare şi legislaţiei în vigoare.

4.10. Deţinătorul certifică acurateţea şi veridicitatea datelor oferite şi asigură Banca că va informa cu promptitudine despre orice modificare a acestora. În cazul în care se dovedeşte că datele personale sunt false, inexacte, neactualizate sau incomplete Banca îşi rezervă dreptul de a suspenda în orice moment accesul Deţinătorului la acest Serviciu.

5. Utilizarea serviciului ”MICB 3D-Secure”

5.1. Ca urmare a activării Serviciului, Deţinătorul poate beneficia de avantajele plăţilor securizate la efectuarea tranzacţiilor E-commerce la comercianţii/site-urile care suportă standardele 3D-Secure.

5.2. Deţinătorul înţelege şi acceptă faptul că pentru efectuarea tranzacţiilor E-commerce la comercianţii/site-urile care suportă standardele 3D-Secure acesta urmează să se autentifice în baza factorilor de autentificare accesibili la momentul efectuării tranzacţiei corespunzătoare.

5.3. La utilizarea Serviciului Deţinătorul recunoaşte faptul, că efectuarea tranzacţiei E-commerce cu utilizarea factorilor de autentificare reprezintă confirmarea acceptării exprese de către Deţinător a prezentelor Condiţii de utilizare şi Tarifelor Băncii, iar Banca, Visa International şi/sau Mastercard Worldwide nu sunt responsabile pentru eventualele pagube cauzate de nerespectarea prezentelor Condiţii de utilizare.

5.4. Banca îşi rezervă dreptul de a refuza utilizarea Serviciului şi eventual efectuarea tranzacţiilor E-commerce la comercianţii/site-urile care suportă standardele 3D-Secure, în cazul în care se dovedeşte că datele personale ale Deţinătorului furnizate Băncii pentru verificarea identităţii Deţinătorului sunt false, inexacte, neactualizate sau incomplete, şi/sau deţinătorul nu a respectat prevederile prezentelor Condiţii de utilizare.

5.5. Deţinătorul înţelege şi acceptă necesitatea asigurării accesului său la factorii de autentificare pentru a putea beneficia de Serviciu.

6. Securitatea serviciului ”MICB 3D-Secure”

6.1. Reieşind din faptul că factorul principal al securităţii sistemului este autentificarea, securitatea sistemului este în cea mai mare măsură influenţată de necompromiterea elementelor de securitate şi a factorilor de autentificare:

6.1.1. Necompromiterea elementelor de securitate ale cardului. Cerinţele de securizare ale acestora sunt descrise în Regulile de funcționare a contului de card și utilizare a cardului atașat;

6.1.2. Necompromiterea factorului de autentificare ”SMS OTP”. Compromiterea acestui factor este situaţia în care Deținătorul nu este ferm convins asupra faptului că mesajele transmise pe numărul de telefon OTP nu sunt accesibile persoanelor terţe;

6.1.3. Necompromiterea parolelor de unică folosinţă ”ATM OTP”. Compromiterea ATM OTP este situaţia în care Deținătorul nu este ferm convins asupra faptului că acestea nu sunt accesibile persoanelor terţe;

6.1.4. Necompromiterea factorului de autentificare ”Mobile OTP”. Compromiterea acestui factor este situaţia în care Deținătorul nu este ferm convins asupra faptului că telefonul / dispozitivul mobil la care este setată aplicaţia ”MICB Mobile Banking” nu este accesibil persoanelor terţe şi/sau codul de acces sau alți factori biometrici de autentificare setat pentru aplicaţia ”MICB Mobile Banking” nu este accesibilă persoanelor terţe.

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 şi alte metode de asigurare a securității informaţionale;

6.2.2. să nu înscrie/păstreze codul de acces/parola pe un suport care permite compromiterea Serviciului, prin natura sau poziţionarea sa.

6.3. În cazul în care unul din factorii de autentificare este compromis, Deținătorul trebuie să:

6.3.1. anunţe imediat Banca prin contactarea Serviciul suport carduri 24/24 şi să comunice detaliile privind circumstanţele compromiterii şi eventualele efecte ale acesteia;

6.3.2. verifice atent tranzacţiile efectuate din numele său pentru a exclude înregistrarea tranzacţiilor 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 modalităţi:

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 informaţional 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 aplicaţia ”MICB Mobile Banking”.

6.7. Banca protejează datele transmise între serverul Serviciului şi telefonul mobil / dispozitivul mobil prin cifrarea acestora.

6.8. Deţinătorul va respecta următoarele recomandări ale Băncii cu privire la modalităţile de utilizare securizată a Serviciului:

6.8.1. Să nu divulge altor persoane elementele de securitate ale cardului, factorii de autentificare şi alte informaţii confidenţiale (parole, codul de acces, conturi, datele personale, etc.);

6.8.2. Să nu lase dispozitivul fără supraveghere în special după procedura de autentificare şi să asigure că ecranul dispozitivului nu este vizibil altor persoane;

6.8.3. Să nimicească cecurile cu parolele OTP dacă nu vor fi utilizate;

6.8.4. Să descarce aplicaţiile mobile numai din magazinele oficiale AppStore şi GooglePlay. Toate alte surse nu sunt oficiale şi Banca nu poartă răspundere pentru consecinţele instalării aplicaţiilor descărcate din aceste surse;

6.8.5. În cazul pierderii sau furtului dispozitivului mobil, să schimbe urgent parola de acces la sistemul automatizat de deservire la distanţă ”MICB Mobile Banking”, să informeze imediat Banca pentru blocarea cardurilor şi accesului la aplicație. Apoi să sune operatorul telefoniei mobile pentru blocarea cartelei SIM;

6.8.6. În cazul schimbării numărului de telefon sau neutilizării acestuia pentru o perioadă de timp mai mare decât valabilitatea lui, să informeze Banca, pentru deconectarea Serviciului de la numărul de telefon pentru a evita compromiterea modalităţii de autentificare SMS OTP;

6.8.7. Să fie vigilent la atacurile de tip phishing scopul cărora este obţinerea de la deținător a informaţiei confidenţiale. Să nu răspundă la e-mailuri sau SMS prin care se solicită divulgarea datelor confidenţiale sau care direcţionează către pagini web în care se solicită, sub diverse motive, informaţii confidenţiale legate de conturi bancare, numărul de card, data expirării acestuia, codul PIN etc. Nici o bancă, magazin online sau altă instituţie nu solicită prin e-mail sau SMS astfel de informaţii!

6.8.8. Să monitorizeze regulat operaţiunile executate. Extrasul de cont şi card va permite depistarea la timp şi semnalarea operativă a Băncii despre neregulile identificate;

6.8.9. În cazul nefuncţionării cartelei SIM să sune imediat la operatorul telefoniei mobile pentru a se asigura că cauza nu este urmare a acţiunilor frauduloase, etc.

7. Interdicţii

Deţinătorul înţelege şi acceptă pe deplin următoarele interdicţii:

7.1. 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 Serviciului accesat.

7.2. Trimiterea de spam, pe orice cale, şi invadarea site-urilor Verified by Visa şi MasterCard Secure Code accesate.

7.3. Modificarea, adaptarea, decompilarea sau dezasamblarea, sub-licențierea, traducerea, vânzarea oricărei porţiuni a serviciului ”MICB 3D-Secure”.

7.4. Ștergerea oricărei notificări privind drepturile de proprietate (copyright, trademark) întâlnite prin accesul la acest Serviciu.

7.5. Utilizarea oricăror mijloace (aplicaţii de căutare, device-uri, procese) pentru regăsirea sau reproducerea structurii de navigare, prezentare şi conţinutul site-urilor afişând brand-urile Verified by Visa şi MasterCard Secure Code.

7.6. Întreruperea accesului altor Deţinători la acest Serviciu, la servere sau reţele conectate la acesta.

7.7. Încălcarea, în mod intenționat sau nu, a prezentelor Condiții de utilizare, Regulilor de funcționare a contului de card și utilizare a cardului atașat, precum şi oricăror reglementări legale interne, naţionale, internaţionale sau a regulilor şi cerințelor stabilite de Visa şi Mastercard pentru folosirea acestui Serviciu.

8. Drepturile şi obligaţiile părţilor

8.1. Părţile îşi asumă drepturile şi obligaţiile menţionate expres în capitolul curent, în alte capitole ale prezentelor Condiţii de utilizare, cererile depuse de către Deținător şi alte documente transmise de către o parte celeilalte părţi în legătură cu obiectul prezentelor Condiţii de utilizare.

8.2. Banca este obligată:

8.2.1. să execute activarea şi funcţionarea Serviciului, în conformitate cu regimul de prestare a Serviciului respectiv definit în prezentele Condiţii de utilizare precum şi regulile Sistemelor Internaţionale de plăţi;

8.2.2. să ia toate măsurile necesare pentru prevenirea riscurilor ce pot apărea în urma utilizării frauduloase a Serviciului şi să asigure măsurile aplicate în vederea identificării Deţinătorului şi asigurării confidenţialităţii, autenticităţii şi non-repudierii tranzacţiilor electronice;

8.2.3. să asigure Deţinătorul cu posibilitatea de a anunţa situaţiile de urgenţă şi să ia toate măsurile necesare pentru a stopa imediat executarea tranzacţiilor frauduloase prin intermediul Serviciului din momentul în care a fost înştiinţată, asigurând deţinătorul cu mijloace care să poată dovedi că comunicarea a fost efectuată (data, ora înregistrării şi numărul de înregistrare a comunicării);

8.3. Deținătorul este obligat:

8.3.1. să ia cunoştinţă de prezentele Condiţii de utilizare şi Regulile de funcționare a contului de card și utilizare a cardului atașat înaintea activării Serviciului şi să utilizeze Serviciul în strictă conformitate cu prevederile acestora;

8.3.2. să asigure confidenţialitatea şi să nu divulge sub nici o formă elementele de securitate ale cardului;

8.3.3. să asigure confidenţialitatea şi să nu divulge sub nici o formă factorii de autentificare (SMS OTP, ATM OTP, Mobile OTP), să ia măsuri rezonabile de protejare a acestora contra compromiterii şi să nu admită utilizarea acestora de către terţe persoane;

8.3.4. să înştiinţeze Banca imediat (prin intermediul Serviciului suport carduri 24/24 sau la ghişeele Băncii) ce constată:

a. suspiciuni cu privire la posibilitatea cunoaşterii de către persoane neautorizate a factorilor de autentificare deţinute de Deţinător;

b. suspiciuni cu privire la cunoaşterea de către persoane neautorizate a elementelor de securitate a cardurilor (codul PIN, codul CVV2/CVC2, numărul cardului, data expirării cardului, codul de acces şi/sau alte elemente de securitate convenite în prealabil între Deţinător şi Bancă);

c. orice eroare sau neregulă apărută în urma utilizării Serviciului;

d. disfuncţionalităţi ale Serviciului, erori la autentificare;

e. recepţionarea (inclusiv din numele Băncii) prin orice canal de comunicare (SMS, e-mail, telefon, reţele de socializare etc.) prin care se solicită elementele de securitate ale cardului, factorii de autentificare şi alte informaţii confidenţiale (parole, codul de acces, conturi, datele personale, etc.).

8.3.5. Înainte de furnizarea oricăror elemente de securitate şi/sau factori de autentificare în vederea realizării unei tranzacţii E-commerce, Deţinătorul se obligă să verifice autenticitatea site-ului, urmărind cel puţin: (i) afişarea siglelor ”Verified by Visa” sau ”MasterCard SecureCode”; (ii) certificatele de securitate ale paginilor ce solicita astfel de date; (iii) afişarea mesajelor de întâmpinare aferente serviciul ”MICB 3D-Secure”.

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

8.4. Banca are dreptul:

8.4.1. să perceapă taxele şi comisioanele conform Tarifelor;

8.4.2. să nu primească spre executare prin intermediul Serviciului tranzacţiile electronice, dacă primirea acestora nu este prevăzută în prezentele Condiţii de utilizare.

8.5. Banca nu poartă răspundere pentru daunele suportate de deţinător de pe urma nerespectării Condiţiilor de utilizare.

9. Responsabilitatea părţilor

9.1. Deţinătorul este responsabil de veridicitatea şi corectitudinea informaţiei transmise prin intermediul Serviciului, pentru confidenţialitatea şi necompromiterea elementelor de securitate a cardului, factorilor de autentificare şi implicit pentru tranzacțiile E-commerce efectuate accesând Serviciul, în cazul în care a avut loc autentificarea deţinătorului bazată pe factorii de autentificare deţinute de deţinător, inclusiv cele efectuate fraudulos de către persoanele terţe, până la suspendarea factorilor de autentificare (ATM OTP, SMS OTP, Mobile OTP) cu utilizarea cărora a fost autentificată tranzacţia respectivă.

9.2. Banca şi Deţinătorul recunosc puterea juridică a tranzacţiilor E-commerce efectuate cu accesarea Serviciului.

9.3. Banca şi Deţinătorul recunosc că documentele electronice transmise în cadrul Serviciului sunt echivalente celor depuse personal şi semnate cu semnătura olografă, şi produc aceleaşi drepturi şi obligaţiuni ale părţilor.

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 tranzacţiilor E-commerce efectuate cu accesarea Serviciului, în cazul în care executarea necorespunzătoare este atribuită unei disfuncţionalităţi a Serviciului sau a unei componente a acestuia, această disfuncționalitate fiind determinată de acțiunile sau responsabilitate Băncii și de asemenea, cu condiţia că disfuncţionalitatea nu a fost cauzată intenţionat de către Deţinător;

9.4.2. pentru tranzacţiile E-commerce iniţiate **după** momentul notificării Băncii de către Deţinător a pierderii controlului asupra elementelor de securitate a cardului şi/sau factorii 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 voinţa Băncii; (ii) defecţiuni ale calculatorului sau executarea necorespunzătoare și 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 tranzacţiilor E-commerce; (iii) eventuale pagube produse prin virusarea echipamentului deţinătorului în timpul tranzacțiilor E-commerce.

9.6. Plăţile efectuate cu ajutorul serviciului ”MICB 3D-Secure” sunt irevocabile şi nu pot fi contestate din motive de fraudă.

10. Relaţia cu comercianţii

10.1. Deţinătorul are deplina libertate de a efectua tranzacţii E-commerce prin accesarea serviciului “MICB 3D-Secure”. În acelaşi timp, corespondența cu comercianţii aleşi, participarea la promoţii on-line, plata şi livrarea bunurilor/serviciilor cumpărate, orice alte condiţii şi garanţii asociate cu acestea ţin numai de domeniul relației Deţinătorului cu comerciantul respectiv. Banca și sistemele internaționale de plăți nu pot fi făcute responsabile sub nici o formă de eventualele pagube apărute în urma relaţiei directe a Deţinătorului cu comercianţi.

10.2. Deţinătorul recunoaşte 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 condiţiilor de plată, livrare, calitate a bunurilor/serviciilor achiziţionate se pot rezolva exclusiv între Deţinător şi acesta. În acest sens trebuie de reţinut cât mai multe informaţii despre comerciant şi de salvat pagina conţinând dovada efectuării tranzacţiei, condiţiile de livrare, detaliile tranzacţiei, corespondenţa purtată cu comerciantul etc.

11. Dispoziţiile finale

11.1. Relaţiile dintre Bancă şi Deţinător care apar în rezultatul utilizării Serviciului şi care nu sunt specificate în prezentele Condiţii de utilizare, vor fi reglementate în conformitate cu Regulile de funcționare a contului de card și utilizare a cardului atașat, regulile Sistemelor Internaţionale de plăţi şi legislaţia în vigoare a Republicii Moldova.
11.2. Toate neînţelegerile şi/sau litigiile apărute între Deţinător şi Bancă pe marginea utilizării Serviciului vor fi soluţionate pe cale amiabilă, prin negociere. În cazul epuizării tuturor mijloacelor de soluţionare pe cale amiabilă a litigiilor, acestea vor fi soluţionate de către instanţele de judecată competente, în conformitate cu legislaţia Republicii Moldova.
11.3. Banca va informa Deţinătorii privind modificarea prezentelor Condiţii de utilizare şi/sau Tarifelor prin afişarea versiunii(lor) modificate a(ale) acestor documente pe pagina Web a Băncii: www.micb.md.