MOLDINDCONBANK

Republica Moldova, MD 2012
Chişinău,str. Armeneasca, 38
Tel.: /+373/ 22 **54-89-40**

Intră în vigoare la 12.10.2017
Aprobat de Comitetul de Conducere al Băncii
PV nr. 124 din 11.10.2017

Condițiile de utilizare a Sistemului „MICB Mobile Banking”

Cuprins:

1. Prevederi generale

1.1. Prezentele Condiţii de utilizare a Sistemului „MICB Mobile Banking” (în continuare Condiţii de utilizare), stabilite de BC „Moldindconbank” S.A., descriu modul în care Banca oferă Clienţilor săi posibilitatea utilizării Sistemului „MICB Mobile Banking” (în continuare Sistem), precum şi modul de utilizare a acestuia de către Abonaţi.

1.2. Prezentele Condiţii de utilizare completează şi detaliază relaţia contractuală existentă între Deţinător şi Bancă, în conformitate cu Regulile de utilizare a cardului accesibile la orice Ghişeu / pe panoul informativ al Băncii și pe pagina web.

1.3. Client eligibil pentru abonare la Sistem este orice persoană fizică care deţine în Bancă un cont de card de care este ataşat un card activ sau orice persoană fizică care deţine un card secundar activ.

1.4. Sistemul „MICB Mobile Banking” este disponibil Clienților săi prin intermediul aplicaţiei mobile „MICB Mobile Banking” pentru sistemele de operare Android și iOS.

1.5. Pentru informaţii suplimentare despre Sistemul „MICB Mobile Banking”, Deținătorul de card poate apela Serviciul Suport Carduri Bancare 24/24 la numărul de telefon **/+373/ 22 54-89-40.**

1.6. Este interzisă posesia, furtul, multiplicarea, denaturarea, ștergerea, reproducerea și folosirea integrală ori parțială a acestui document fără a dispune de drept autorizat.

2. Noţiunile utilizate

În cuprinsul Condiţiilor de utilizare şi în orice document care derivă sau are legătura cu acestea, termenii de mai jos vor fi înţeleşi după cum urmează:

- **MICB Mobile Banking, Aplicaţie** – aplicaţia mobilă care oferă acces rapid şi sigur la conturile de card, direct de pe telefonul mobil sau tableta personală conectată la internet, în conformitate cu prezentele Condiții de utilizare, fiind accesibilă a fi instalată din magazinele virtuale oficiale “App Store” şi “Google Play”.
- **Sistem de deservire bancară la distanţă** (în continuare Sistem) – soluţie informatică, pusă la dispoziţie de către Bancă clienţilor săi, ce permite deţinătorului să aibă acces la distanţă la mijloacele aflate în contul său bancar, în scopul obţinerii de informaţii privind starea contului bancar şi a operaţiunilor realizate, efectuării de plăţi în numele şi din ordinul deţinătorului prin intermediul unei aplicaţii informatice, a unei metode de autentificare electronică şi al unui mijloc de comunicaţie.
    - **Sistemul de deservire bancară la distanţă informaţional** este un sistem utilizat în scopul obţinerii de informaţii privind starea contului bancar şi a operaţiunilor realizate.
    - **Sistemul de deservire bancară la distanţă tranzacţional** este un sistem utilizat în scopul efectuării de plăţi în numele şi din ordinul deţinătorului.
- **Condiţii de utilizare** – prezentul document, ce vine să detalieze modul în care Clienţii Băncii pot accesa şi ulterior utiliza Sistemul „MICB Mobile Banking”.
- **Tarife** – Tarifele şi limitele referitoare la deservirea cardurilor bancare emise de BC „Moldindconbank” S.A în vigoare – lista taxelor, comisioanelor şi a limitelor aplicate de către Bancă la administrarea Cardurilor publicate pe panourile informative ale subdiviziunilor Băncii, precum şi pe pagina web.
- **Card** – card de plată emis de Bancă pe numele Deţinătorului, în conformitate cu Contractul încheiat între Deţinător şi Bancă.
- **Card principal** – card emis pe numele titularului Contului de card.
- **Card secundar** – card emis pe numele Utilizatorului autorizat.
- **Deţinător de card, Deţinător** - Persoana fizică pe numele căreia este emis Cardul în conformitate cu Cererea de emitere a Cardului. Cuprinde termenii „Deţinătorul principal” şi „Utilizatorul autorizat”.
- **Deţinător principal** - Deţinătorul, posesor al Contului de card deschis în conformitate cu Cererea.
- **Utilizator autorizat** – Deţinător de card, altul decât Deţinătorul principal: persoana fizică pe numele căreia este emis Cardul în conformitate cu Cererea, şi este nominalizată de către Deţinătorul principal ca Utilizator autorizat al Contului de card.
- **Cont de card** - Contul deschis şi menţinut de către Deţinătorul principal în cadrul Băncii, cu scopul înscrierii tranzacţiilor cu carduri, precum şi a altor operaţiuni prevăzute de Regulile de utilizare a Cardului, Tarifele şi Cererea.
- **Bancă** – proprietarul Sistemului MICB Mobile Banking - BC „Moldindconbank” S.A.

- **Client** – Deţinătorul Cardului care efectuează autentificarea în sistem. Client eligibil pentru utilizarea amprentei digitale pentru autentificarea la Sistem este orice persoană fizică care deţine card bancar emis de bancă și cel puțin un dispozitiv (telefon, tabletă) cu funcționalitatea autentificării prin amprenta digitală.
- **Abonat** – Clientul care este abonat la Sistem.
- **Beneficiar –** persoana care utilizează Codul „Cash by Code” pentru retragerea numerarului din bancomatele Băncii și Codul ”Cash-In by Code” pentru alimentarea contului cu numerar în bancomatele Cash-In ale Băncii în conformitate cu Condiţiile de utilizare a Serviciului “Cash by Code”.
- **Abonament** – totalitatea relaţiilor reglementate dintre Abonat şi Bancă aferente Sistemului, precum şi înregistrarea parametrilor şi statutului acestei relaţii.
- **Abonare la Sistem** – procesul în urma căruia Clientul obţine calitatea de Abonat în sensul prezentelor Condiţii de utilizare, se stabileşte Abonamentul şi Banca îi alocă Clientului Loginul şi Parola.
- **Telefon mobil / dispozitiv mobil** – echipament de tip smartphone sau tabletă, utilizat de către Abonat pentru conectarea la Sistem și utilizarea ulterioară a acestuia.
- **Dispozitiv “touch id / FingerPrint”** – dispozitiv mobil (smartphone, tabletă) dotat cu funcționalitatea “touch id”, care permite înregistrarea și utilizarea amprentei digitale pentru accesarea dispozitivului.
- **Server „MICB Mobile Banking”, Serverul Sistemului** – este totalitatea echipamentului electronic şi programelor Băncii, pe care rulează Sistemul şi cu care telefonul mobil / dispozitivul mobil al Abonatului stabileşte legătura cu scopul stabilirii Sesiunii de utilizare a Sistemului.
- **Instrucţiuni** – Instrucţiunile de utilizare a Sistemului „MICB Mobile Banking” – document perfectat de Bancă şi accesibil de pe pagina https://wb.micb.md, în care este descrisă modalitatea utilizării Sistemului de către Abonat. Instrucţiunile sunt parte integrantă a prezentelor Condiţii de utilizare şi sunt obligatorii de respectat în cadrul Abonării şi utilizării Sistemului.
- **Login** – identificator alfanumeric alocat de Bancă Clientului pentru identificarea Clientului în calitate de Abonat.
- **Parolă** – identificator alfanumeric alocat de Bancă Clientului sau stabilit de către Client în procesul de Abonare sau modificat ulterior de către Abonat în cadrul Sesiunii de utilizare a sistemului, necesar pentru Autentificarea Clientului în Sistem în calitate de Abonat.
- **Sesiune de utilizare a Sistemului** – sesiunea stabilită dintre telefonul mobil al Abonatului şi Serverul Sistemului, în baza Autentificării Abonatului în Sistem, pe parcursul căreia Abonatului îi sunt accesibile Serviciile Sistemului.
- **Log out / Ieșire / Выход** - acțiunea de finisare securizată a sesiunii de utilizare a Sistemului.
- **Autentificare electronică (a Abonatului) în Sistem** – Autentificarea electronică, procesul de verificare a identităţii Abonatului prin Login şi metodele de autentificare stabilite în prezentele Condiţii, cu scopul stabilirii Sesiunii de utilizare a Sistemului.
- **Serviciu** – serviciul oferit de Bancă Abonatului prin intermediul Sistemului, conform funcţionalităţii Sistemului şi produselor / serviciilor deţinute de către Abonat (conturilor, cardurilor etc.), cu ajutorul căruia Abonatul poate comanda executarea unui Document electronic, inclusiv efectuarea de către Bancă a unei Tranzacţii, obţinerea sau modificarea unui produs sau serviciu (inclusiv şi unui oferit în afara Sistemului) sau obţinerea din partea Băncii a unei informaţii.
- **Document electronic** – orice document perfectat şi/sau transmis Băncii de către Abonat prin intermediul Sistemului.
- **Tranzacţie electronică, Tranzacţie** – operaţiune efectuată în formă electronică în cadrul Sesiunii de utilizare a Sistemului în baza Documentului electronic, în cadrul utilizării unui serviciu şi protejată printr-un mecanism ce permite verificarea autenticităţii, integrităţii şi non-repudierii (imposibilităţii negării) acesteia.
- **Autentificarea suplimentară** – autentificarea **electronică a** identităţii Abonatului şi/sau acordului său de utilizare a Serviciului, alta decât prin Parolă, care poate fi solicitată de către Bancă în vederea utilizării Sistemului de către Abonat, în funcţie de nivelul de risc al Serviciului, suma Tranzacţiei sau alţi factori. Solicitarea sau nesolicitarea Autentificării suplimentare este efectuată la decizia Băncii. Totodată Autentificarea suplimentară poate fi utilizată în procesul Abonării la Sistem, precum şi pentru restabilirea Loginului şi/sau Parolei; în acest caz Autentificarea suplimentară are denumire de „**Autentificare alternativă**”.
- **Autentificarea suplimentară de tip „SMS OTP”, SMS OTP** – tipul Autentificării suplimentare care prevede transmiterea de către Bancă în adresa Abonatului a unei parole de unică folosinţă în cadrul unui mesaj SMS la Numărul de telefon OTP şi introducerea acestei parole de către Abonat în interfaţa Sistemului.
- **Număr de telefon OTP** – numărul de telefon mobil stabilit de către Client în cadrul Chestionarului clientului – persoană fizică sau comunicat prin intermediul Serviciului Suport Carduri 24/24 și este înregistrat în sistemul

informațional al Băncii, cu condiţia că acest număr de telefon este gestionat de unul din următorii operatori de telefonie mobilă: Moldcell (IM „Moldcell" S.A.), Orange („Orange Moldova" S.A.) şi Unite („Moldtelecom" S.A.).

- **Autentificarea suplimentară de tip „ATM OTP", ATM OTP** – tipul Autentificării suplimentare care prevede primirea de către Abonat a unei liste de parole de unică folosinţă prin intermediul bancomatului Băncii şi introducerea acestei parole de către Abonat în interfaţa Sistemului.
- **Autentificare suplimentară de tip „Mobile OTP"** – tipul Autentificării suplimentare care prevede generarea de către Abonat a unei parole de unică folosinţă prin intermediul Aplicaţiei, în baza unui cod generat în sistemul „MICB Web Banking".
- **Autentificare suplimentară prin aplicarea Codului de acces -** tipul Autentificării suplimentare care prevede setarea Codului de acces şi aplicarea acestuia pentru accesarea ulterioară a Sistemului Mobile Banking, fără a introduce Login-ul și Parola.
- **Codul de acces –** codul numeric alcătuit din 5 cifre generat de către Abonat prin intermediul Aplicației Mobile și utilizat de către Abonat pentru accesarea ulterioară a Sistemului Mobile Banking, fără a introduce Login-ul și Parola. Codul de acces se setează de către Client separat pentru fiecare Dispozitiv deţinut.
- **Autentificare suplimentară cu amprenta digitală** – opțiune disponibilă doar pentru Dispozitivele "touch id / FingerPrint" care prevede utilizarea amprentei digitale a Clientului, stocate în memoria Dispozitivului "touch id / FingerPrint" pentru autentificarea Clientului în Sistem. Sistemul scanează și identifică amprentele digitale salvate în dispozitivul / dispozitivele Clientului.
- **Factor de autentificare** – Parola obţinută prin Autentificarea de tip SMS OTP, ATM OTP, Mobile OTP, autentificarea prin aplicarea Codului de acces sau autentificarea cu amprenta digitală.
- **Serviciul „P2P MICB"** – serviciu care oferă posibilitatea de a transfera mijloacele băneşti de pe card pe card prin intermediul Portalului www.transfer.md, bancomatelor gestionate de către Bancă, sistemelor „MICB Web Banking" şi „MICB Mobile Banking" (accesibile *Deţinătorilor de carduri MICB*), precum şi de a alimenta cu numerar cardul în bancomatele Băncii de tip „CASH-IN".
- **Serviciul „Cash by Code", Serviciu** – este un serviciu destinat persoanelor fizice Deținătoare de carduri active emise de Bancă, accesibil în sistemul "MICB Web Banking" și sistemul „MICB Mobile Banking". Serviciul oferă Beneficiarului posibilitatea de a retrage numerar fără card la orice bancomat al Băncii în baza Codului special „Cash by Code". Retragerea numerarului în baza codului de bare „Cash by Code" poate fi efectuată doar la bancomatele care dispun de această funcționalitate. Lista bancomatelor este accesibilă pe **pagina Web a Băncii.**
- **Cod „Cash by Code" -** cod de unică folosință generat de Sistem, format dintr-o componentă din 6 cifre și/sau în format grafic - cod de bare (doar pentru sistemul "MICB Mobile Banking") care aparține și se află în posesia Deţinătorului de card. Acest cod poate fi utilizat pentru retragerea numerarului de către Beneficiar, din inițiativa şi cu participarea nemijlocită a Deţinătorului, cu condiţia respectării Condiţiilor de utilizare a serviciului „Cash by Code".
- **Serviciul "Cash-In by Code" –** este un serviciu destinat persoanelor fizice Deţinătoare de carduri active emise de Bancă, care permite Abonatului generarea unui cod unic de identificare a contului de card în Sistemul "MICB Mobile Banking" în baza căruia poate alimenta contul său de card cu o anumită sumă de bani în numerar direct la bancomatele Cash-In fără a utiliza un card bancar. Codul unic este reprezentat în format grafic (cod de bare).
- **Cod "Cash-In by Code" –** cod în format grafic (cod de bare) generat de Sistem care aparține și se află în posesia Deținătorului de card. Acest cod poate fi utilizat pentru alimentarea de către Beneficiar a contului de card la bancomatele Cash-In ale Băncii din inițiativa şi cu participarea nemijlocită a Deţinătorului, cu condiţia respectării Condiţiilor de utilizare a serviciului „Cash by Code".
- **Serviciul „SMS-notificări" -** serviciu de informare a clienţilor prin intermediul mesajelor SMS expediate la telefonul mobil cu privire la tranzacţiile efectuate cu cardul bancar şi pe contul de card. Serviciul este disponibil doar pentru numerele de telefon gestionate de Operatorii de telefonie mobilă Moldcell (ÎM Moldcell S.A.), Orange („Orange Moldova" S.A.) şi Unite („Moldtelecom" S.A.).

3. Instalarea aplicaţiei

3.1. Instalarea Aplicaţiei pentru telefoanele mobile/ dispozitivele mobile care rulează pe sistemul de operare iOS va fi efectuată de Client, din magazinul virtual oficial „App Store".

3.2. Instalarea Aplicaţiei pentru telefoanele mobile/ dispozitivele mobile care rulează pe sistemul de operare Android va fi efectuată de Client, din magazinul virtual oficial „ Google Play".

3.3. Aplicația poate fi utilizată concomitent pentru mai multe telefoane / dispozitive mobile care rulează prin sistemele de operare menționate în p.3.1 și 3.2.

4. Abonarea și autentificarea la Sistem

4.1. Abonarea la Sistem se efectuează de către Client în baza prezentelor Condiții, utilizând ”Instrucțiunea de utilizare a sistemului ”MICB Mobile Banking”” și are ca rezultat obţinerea de către Client a Login-ului şi Parolei.

4.2. Abonarea la Sistem se efectuează prin abonarea la „MICB Web Banking” şi poate fi efectuată prin următoarele modalităţi:

4.2.1. **Obţinerea Login-lui şi Parolei prin operaţiunea respectivă accesibilă la bancomatul Băncii**:

a. Clientul autentifică operaţiunea de primire a Login-lui şi Parolei prin introducerea unui Card valabil emis pe numele Clientului şi a Codului PIN în elementele de interacţiune ale bancomatului;

b. În rezultatul operaţiunii de primire a Login-lui şi Parolei Banca alocă Clientului Loginul şi Parola generate printr-un algoritm de creare a valorilor alfanumerice aleatorii şi le imprimă pe bonul bancomatului;

c. Clientul este responsabil pentru compromiterea Login-lui şi Parolei în cazul nepreluării din imprimanta bancomatului a bonului cu Login şi Parolă imprimate.

4.2.2. **Abonarea prin introducerea numărului Cardului şi Autentificării alternative de tip „SMS OTP” sau „ATM OTP”, prin intermediul paginii web a sistemului „MICB Web Banking”**:

a. Clientul efectuează abonarea prin intermediul Sistemului Web Banking pe pagina web **https://wb.micb.md**;

b. Clientul autentifică operaţiunea de primire a Login-lui şi Parolei prin introducerea numărului unui Card valabil emis pe numele Clientului şi efectuarea Autentificării alternative de tip „SMS OTP” sau „ATM OTP”;

c. În cadrul operaţiunii Clientul introduce în câmpurile respective ale interfeţei Sistemului, Login-ul şi Parola care doreşte să-i fie alocată de către Bancă. Banca îi alocă Login-ul şi Parola cu condiţia că acestea corespund cerinţelor stabilite în prezentele Condiţii de utilizare (caracterele utilizate, lungimea etc.) şi, totodată, dacă Login-ul nu este deja utilizat pentru identificarea unui alt Abonat.

4.3. **Autentificarea în sistem este posibilă prin mai multe modalități:**

a. **Cu configurarea Codului de acces** prin introducerea unui cod numeric din 5 cifre de acces la aplicație setat de către Abonat în baza mesajului „SMS OTP”. Codul de acces oferă clientului posibilitate de:

- accesare a sistemului Mobile Banking folosind codul digital scurt și convenabil în loc de numele de utilizator și parola;
- efectuare a unor operațiuni fără parola de unică folosinţă;
- generarea parolelor de unică folosință, pentru confirmarea operațiunilor în Web-Banking, E-Commerce;
- utilizare celui mai inovațional și securizat mod de autentificare (recomandat).

b. **Cu numele de utilizator şi parola:** se va utiliza numele de utilizator și parola utilizate pentru autentificarea în sistemul “MICB Web Banking”;

c. **Cu numele de utilizator și parola primită prin SMS:** în calitate de Login se va utiliza numele utilizatorului utilizat pentru autentificarea în sistemul MICB Web Banking”, iar în calitate de parolă se va utiliza codul de unică folosință transmis prin intermediul mesajului SMS (OTP SMS);

d. **Cu numele de utilizator și parolă de pe bonul tipărit la bancomat (ATM OTP):** se va utiliza numele utilizatorului si parola, care au fost imprimate pe bonul de la bancomat;

e. **Cu numărul cardului și parola primită prin SMS**: în calitate de Login se va utiliza numărul cardului, iar în calitate de parolă se va utiliza codul de unică folosință transmis prin intermediul mesajului SMS (OTP SMS);

f. **Cu numărul cardului şi parola de pe chitanţa generată de la bancomat:** în calitate de Login se va utiliza numărul cardului, iar în calitate de parolă se va utiliza unul din codurile de unică folosinţă (ATM OTP) ce au fost imprimate pe chitanţă la bancomat.

g. **Cu utilizarea amprentei digitale:** prin scanarea și identificarea amprentei digitale salvată în dispozitivul / dispozitivele Clientului. Autentificarea prin utilizarea amprentei digitale poate fi efectuată doar de pe un dispozitiv “touch id / FingerPrint”.

4.4. Clientul, prin Abonare la Sistem, confirmă faptul că a luat cunoştinţă de prezentele Condiţii de utilizare şi le acceptă.

4.5. Clientul nu are dreptul să utilizeze în procesul abonării cardul sau rechizitele unui alt card decât cel emis pe numele său.

4.6. Abonarea poate să fie efectuată doar personal de către Client şi nu poate fi efectuată de către mandatar, tutore, reprezentant legal sau orice altă persoană terţă.

4.7. Clienţii abonaţi anterior la sistemul “MICB Web Banking” implicit au acces şi la sistemul „MICB Mobile Banking”, cu utilizarea Login-lui și Parolei identice.

5. Autentificarea în Sistem prin amprenta digitală

5.1. Autentificarea în Sistem prin utilizarea amprentei digitale reprezintă o funcționalitate suplimentară oferită de Bancă pentru logarea în Sistem prin intermediul dispozitivelor “touch id / FingerPrint” ce pot efectua scanarea amprentei. În așa fel, odată ce s-a optat pentru această metodă de logare, telefonul mobil va permite Abonatului să folosească orice amprentă digitală stocată în memoria telefonului, astfel încât este prudent să fie activate măsuri suplimentare de securitate, pentru a proteja telefonul mobil de accesarea neautorizată de către alte persoane și să nu fie salvate amprente digitale ale altor persoane în memoria telefonului.

5.2. Autentificarea prin amprenta digitală poate fi utilizată ca o metodă alternativă de logare în Sistem pentru confirmarea identității Abonatului și înlocuiește alte metode de autentificare descrise în p.p. 4.3.a – 4.3.f.

5.3. Tehnologia specifică dispozitivului “touch id / FingerPrint” care scanează și identifică amprentele digitale salvate ale Abonatului nu este creată de Bancă, astfel încât Banca nu o gestionează, nu este răspunzătoare și nu oferă nici o declarație sau garanție cu privire la securitatea și funcționalitatea acestei tehnologii și de asemenea, cu privire la maniera în care producătorul dispozitivului “touch id / FingerPrint” o promovează.

5.4. Utilizarea amprentei digitale poate fi efectuată concomitent de pe mai multe telefoane / dispozitive mobile “touch id / FingerPrint”.

5.5. Activarea opțiunii de autentificare prin amprenta digitală poate fi efectuată de Abonatul care îndeplinește următoarele condiții:

a. Este un utilizator al Sistemului “MICB Mobile Banking”;

b. A instalat aplicația mobilă pe un dispozitiv echipat cu “touch id” propriu;

c. A setat în Sistem codul de acces din 5 cifre;

d. A activat la dispozitivul “touch id / FingerPrint” funcția de autentificare prin amprenta digitală și a înregistrat cel puțin o amprentă digitală personală.

e. A verificat dacă în memoria dispozitivului “touch id / FingerPrint” sunt salvate amprentele digitale personale;

5.6. Abonatul, prin autentificarea în Sistem cu utilizarea amprentei digitale confirmă faptul că a luat cunoştinţă și este de acord cu prevederile prezentelor Condiţii şi în legătură cu aceasta declară că:

a. Înțelege și acceptă faptul că orice amprentă digitală salvată în “touch id / FingerPrint” poate fi utilzată în calitate de Factor de autentificare la Sistem și permite accesul la conturile / cardurile personale ale Deținătorului;

b. Confirmă că este de acord că în scopul utilizării funcționalității “touch id”, Sistemul accesează amprentele digitale înregistrate în dispozitivul “touch id / FingerPrint” și acceptă ca Banca să acceseze și să utilizeze această informație pentru utilizarea de către Abonat a acestei funcționalități;

c. Înțelege și conștientizează importanța protejării dispozitivului / dispozitivelor sale “touch id / FingerPrint” de accesarea acestora de către persoanele terţe;

d. Recunoaște că autentificarea în Sistem prin utilizarea amprentei digitale este o metoda alternativă de autentificare și poate fi utilizată concomitent cu alte metode de autentificare;

5.7. De fiecare dată când aplicația mobilă identifică utilizarea amprentei digitale salvate în dispozitivul “touch id / FingerPrint”, se consideră că Abonatul a accesat Sistemul și a autorizat Banca să efectueze astfel de tranzacții.

5.8. Abonatul poate în orice moment dezactiva funcționalitatea de utilizare a amprentei digitale.

5.9. Banca nu garantează că funcţionalitatea “touch id / FingerPrint” va fi accesibilă de pe orice dispozitiv, precum şi nu poate garanta continuitatea accesibilităţii funcţionalităţii respective.

5.10. Banca nu este responsabilă pentru nici o pierdere suportată de Abonat in legătură cu utilizarea sau încercarea de utilizare a funcționalității “touch id” în cazul unor tranzacții neautorizate, orice acces neautorizat la dispozitivul “touch id / FingerPrint”**.**

6. Restabilirea Login-lui şi/sau Parolei

6.1. Restabilirea Login-lui şi/sau Parolei poate fi efectuată prin următoarele modalităţi:

6.1.1. **Obţinerea Login-lui şi Parolei prin operaţiunea respectivă accesibilă la bancomatul Băncii**:

a. Clientul autentifică operaţiunea de primire a Login-lui şi Parolei prin introducerea unui Card valabil emis pe numele Clientului şi a Codului PIN în elementele de interacţiune ale bancomatului;

b. În rezultatul operaţiunii de primire a Login-lui şi Parolei, Banca îi atribuie Clientului o Parolă nouă, generată printr-un algoritm de creare a valorilor alfanumerice aleatorii şi imprimă Login-ul şi Parola pe bonul bancomatului.

c. Clientul este responsabil pentru compromiterea Login-lui şi Parolei în cazul nepreluării din imprimanta bancomatului a bonului cu Login şi Parolă imprimate.

6.1.2. **Obţinerea Login-lui şi modificarea Parolei prin introducerea numărului Cardului şi Autentificării alternative de tip „SMS OTP” sau „ATM OTP”**:

a. Clientul efectuează această operaţiune prin intermediul Sistemului;

b. Clientul autentifică operaţiunea de primire a Login-lui şi Parolei prin introducerea numărului unui Card valabil emis pe numele Clientului şi efectuarea Autentificării alternative de tip „SMS OTP” sau „ATM OTP”.

c. În cadrul operaţiunii, Clientului îi este afişat în interfaţa Sistemului Login-ul său, totodată Clientul introduce în câmpurile respective ale interfeţei Sistemului Parola nouă care doreşte să-i fie alocată de către Bancă. Banca îi alocă Parola cu condiţia că aceasta corespunde cerinţelor stabilite în prezentele Condiţii de utilizare (caracterele utilizate, lungimea etc.).

7. Securitatea Sistemului

7.1. Securitatea Sistemului are ca scop:

7.1.1. securitatea Cardurilor, Conturilor Clientului şi a mijloacelor din ele, altor produse şi servicii deţinute de Client în Bancă, precum şi confidenţialitatea informaţiei despre acestea;

7.1.2. asigurarea faptului că Tranzacţiile pot fi efectuate din numele Abonatului doar de către Abonat şi nu în mod fraudulos de către o altă persoană.

7.2. Securitatea Sistemului este asigurată prin următoarele cerinţe de autentificare:

7.2.1. o persoană poate să se Aboneze la Sistem în calitate de Client sau să obţină acces la Login-ul şi Parolă doar în baza autentificării prin Card şi Cod PIN la bancomat sau în baza numărului Cardului şi Autentificării alternative în Sistem;

7.2.2. o persoană poate să obţină accesul la Sistem în calitate de Abonat doar în baza procedurii Autentificării în Sistem;

7.2.3. în cadrul Sesiunii de utilizare a Sistemului, unele Servicii sunt accesibile doar în baza Autentificării suplimentare.

7.3. Reieşind din faptul că factorul principal al securităţii Sistemului este autentificarea, securitatea Sistemului este în cea mai mare măsură influenţată de necompromiterea Factorilor de autentificare şi anume:

7.3.1. Necompromiterea Cardului, datelor cardului şi a PIN-ului. Cerinţele de securizare ale acestora sunt descrise în Regulile de utilizare a cardului.

7.3.2. Necompromiterea Parolei. Compromiterea Parolei este situaţia în care Clientul nu este ferm convins asupra faptului că aceasta nu este accesibilă persoanelor terţe.

7.3.3. Necompromiterea parolelor de unică folosinţă primite din ATM (ATM OTP). Compromiterea ATM OTP este situaţia în care Clientul nu este ferm convins asupra faptului că acestea nu sunt accesibile persoanelor terţe.

7.3.4. Necompromiterea Factorului de autentificare „SMS OTP”. Compromiterea acestui Factor este situaţia în care Clientul nu este ferm convins asupra faptului că mesajele transmise pe numărul de telefon OTP nu sunt accesibile persoanelor terţe.

7.3.5. Necompromiterea Codului de acces. Compromiterea acestui Factor este situaţia în care Clientul nu este ferm convins asupra faptului că Codul de acces nu este accesibil persoanelor terţe.

7.3.6. Necompromiterea amprentei digitale. Compromiterea acestui Factor este situația în care Clientul nu este ferm convins asupra faptului că o persoană terță nu a avut acces la dispozitivul “touch id / FingerPrint” și nu a salvat amprenta sa digitală în dispozitivul “touch id / FingerPrint”.

7.4. Clientul este responsabil pentru necompromiterea Factorilor de autentificare deţinute de el.

7.5. Cu scopul prevenirii compromiterii Parolei, Clientul trebuie:

7.5.1. să nu înscrie Parola pe un suport care permite asocierea cu Sistemul, prin natura sau poziţionarea sa;

7.5.2. să modifice regulat Parola cu ajutorul Serviciului respectiv al Sistemului;

7.5.3. 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 securitate informaţională;

7.5.4. să limiteze accesul persoanelor terțe la dispozitivul / dispozitivele “touch id / FingerPrint”.

7.6. În cazul în care Parola este compromisă, Clientul trebuie să modifice imediat Parola prin una din următoarele modalităţi:

7.6.1. Serviciul respectiv în cadrul Sesiunii de utilizare a Sistemului;

7.6.2. Operaţiunea de modificare a Parolei prin introducerea numărului Cardului şi Autentificării alternative de tip „SMS OTP” sau „ATM OTP”;

7.6.3. Obţinerea Login-lui şi Parolei (regenerate) prin operaţiunea respectivă accesibilă la bancomatul Băncii;

7.6.4. În cazul în care Clientul nu are posibilitate de a efectua acţiunile menţionate mai sus, acesta trebuie să contacteze imediat Serviciul suport carduri 24/24 al Băncii pentru a anula Parola.

7.7. **Cerinţele faţă de Parolă în Sistemul MICB Mobile Banking:**

7.7.1. Parola trebuie să conţină cel puţin 8 simboluri şi cel mult 20, să conţină cel puţin o litera latină majusculă, o literă latină minusculă şi o cifră;

7.7.2. Este interzisă utilizarea altor caractere decât litere latine majuscule/minuscule şi cifre;

7.7.3. Este interzisă stabilirea Parolei care coincide cu una din 12 Parole utilizate anterior;

7.7.4. Sistemul va suspenda Parola pentru 15 minute după fiecare 3 introduceri greşite consecutive;

7.7.5. Sistemul va impune modificarea parolei de către Abonat cel puţin o dată la 90 zile.

7.8. În cazul în care unul din Factorii de autentificare este compromis, Clientul trebuie să:

7.8.1. verifice atent Tranzacţiile efectuate din numele său pentru a depista pe cele frauduloase;

7.8.2. anunţe imediat Banca şi să comunice detaliile privind circumstanţele compromiterii şi eventualele efecte ale acesteia.

7.9. În cazul în care parola de unică folosinţă (sau lista de parole) ATM OTP este compromisă, Clientul trebuie să solicite anularea listei respective de ATM OTP prin una din următoarele modalităţi:

7.9.1. să genereze o nouă listă de ATM OTP;

7.9.2. să contacteze Serviciul suport carduri 24/24 al Băncii pentru a anula lista de parole ATM OTP.

7.10. În cazul în care Factorul „SMS OTP” este compromis, Clientul trebuie:

7.10.1. să solicite operatorului de telefonie mobilă suspendarea numărului de telefon (utilizat în calitate de numărul de telefon OTP) şi restabilirea accesului exclusiv al Clientului la acest număr de telefon;

7.10.2. să solicite Băncii, prin contactarea Serviciului suport carduri 24/24 al Băncii, suspendarea numărului de telefon OTP în sistemul informaţional al Băncii;

7.10.3. să solicite Băncii modificarea numărului de telefon utilizat în calitate de numărul de telefon OTP prin una din următoarele modalităţi:

a. modificarea numărului de telefon în cadrul Serviciului „SMS-notificări” prin intermediul bancomatului Băncii, MICB Web banking, MICB Mobile Banking sau prin depunerea cererii respective la una dintre subdiviziunile Băncii;

b. modificarea numărului de telefon mobil în afara Serviciului „SMS-notificări”, prin depunerea Chestionarului pentru client – persoană fizică la una dintre subdiviziunile Băncii.

7.11. În cazul în care Factorul “Cod de acces” este compromis, Clientul trebuie:

7.11.1. să reseteze Codul de acces din meniul Setări al aplicației “MICB Mobile Banking”.

7.12. În cazul în care Factorul “Amprenta digitală” este compromis, Clientul trebuie:

7.12.1. să șteargă toate amprentele salvate în memoria dispozitivului “touch id / FingerPrint” și să le configureze din nou;

7.13. Suspendarea / reactivarea Login-lui:

7.13.1. În cazul în care securitatea Login-lui este compromisă din motive diferite şi securitatea Login-lui nu poate fi restabilită (asigurată) prin suspendarea / anularea Factorilor de autentificare, Clientul trebuie să solicite suspendarea Login-lui, apelând Serviciul suport carduri 24/24 al Băncii;

7.13.2. În cazul suspendării Login-lui Autentificarea în Sistem şi restabilirea parolei nu vor fi accesibile;

7.13.3. Abonatul poate solicita reactivarea unui Login suspendat apelând personal Serviciul suport carduri 24/24 al Băncii, cu condiţia identificării reuşite a Abonatului de către operatorul Serviciului suport carduri 24/24 în baza datelor anterior prezentate de către Abonat Băncii;

7.13.4. Reactivarea Login-lui nu duce în sine la reactivarea Factorilor de autentificare.

7.14. Banca protejează datele transmise între Serverul Sistemului şi Telefon mobil / dispozitiv mobil prin cifrarea acestora aşa cum este definit în specificaţiile tehnice ale protocolului SSL.

7.15. Banca recomandă următoarele modalităţi de utilizare securizată a Sistemului „MICB Mobile Banking":

7.15.1. Să nu divulge informaţia confidenţială altor persoane (PIN, numărul de card, parole, conturi, datele personale);

7.15.2. Să nu lase dispozitivul / dispozitivul "touch id / FingerPrint" fără supraveghere în special după procedura de autentificare şi să asigure că ecranul dispozitivului nu este vizibil altor persoane;

7.15.3. Să seteze parola de acces la dispozitivul mobil şi opţiunea de blocare a dispozitivului după o perioadă de inactivitate;

7.15.4. Să utilizeze parole şi coduri de acces puternice, pentru a evita spargerea lor;

7.15.5. Să utilizeze diferite parole pentru fiecare serviciu (poşta electronică, conturile de acces la reţelele de socializare, etc.);

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

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

7.15.8. Să efectueze regulat actualizarea sistemului de operare, aplicaţiei MICB Mobile Banking şi altor aplicaţii instalate pe dispozitivul mobil, utilizând numai surse oficiale;

7.15.9. Pentru a fi siguri că nu descărcaţi ceva dubios, dezactivaţi în setările telefonului pe platforma Android opţiunea „Surse Necunoscute" în setările de „Securitate";

7.15.10. Să instaleze pe dispozitivul mobil aplicaţii anti-virus şi să le actualizeze regulat. De asemenea trebuie actualizată aplicaţia anti-virus la calculatoarele la care se conectează dispozitivul mobil;

7.15.11. Să nu păstreze pe dispozitivul mobil informaţie confidenţială (PIN coduri, numărul de card, parole de acces), de exemplu în mesaje SMS, E-mail-uri, mementouri, notiţe, etc.;

7.15.12. Aplicaţia MICB Mobile Banking va fi utilizată numai de către Abonatul la Sistem;

7.15.13. Să şteargă informaţia confidenţială în cazul transmiterii dispozitivului altor persoane (vinderea, reparaţia). Pentru aceasta este necesar să restabilească setările prestabilite din fabrică. Ştergerea informaţiei cu utilizarea punctelor de meniu va permite infractorului restabilirea ei;

7.15.14. Să activeze opţiunea de control la distanţă pentru ştergerea datelor la distanţă sau blocare în cazul pierderii dispozitivului;

7.15.15. Să nu execute operaţiunea de obţinere a dreptului de administrator (jail-break, rooting). Aceste operaţiuni pot scădea nivelul de securitate şi expune Sistemul unor riscuri suplimentare;

7.15.16. În cazul pierderii sau furtului dispozitivului mobil, să schimbe urgent parola de acces la sistemul de deservire bancară la distanţă, să informeze imediat Banca pentru blocarea cardurilor şi a accesului la Sistem, să sune operatorul telefoniei mobile pentru blocarea cartelei SIM;

7.15.17. În cazul schimbării numărului de telefon sau neutilizării acestuia pentru o perioadă de timp mai mare decât valabilitatea cartelei SIM, să informeze Banca. pentru deconectarea Sistemului de la numărul de telefon pentru a evita compromiterea modalităţii de Autentificare Suplimentară de tip SMS OTP;

7.15.18. Să fie vigilenţi la atacurile de tip phishing scopul cărora este obţinerea de la client a informaţiei confidenţiale. Să nu execute mesajele primite prin email sau SMS prin care se solicită divulgarea datelor confidenţiale. Banca niciodată nu transmite mesaje SMS şi email-uri pentru a solicita de la clienţi informaţie confidenţială;

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

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

7.15.21. Să termine lucrul cu aplicaţia mobilă prin accesarea butonului Exit (Ieşire);

7.15.22. Să ignoreze propunerile de instalare a unor „aplicaţii importante" sau „update-uri importante" dacă ele sunt primite de la persoane sau companii necunoscute (de exemplu prin email-uri, SMS, etc.);

7.15.23. Să evite utilizarea reţelelor wireless/Wi-Fi publice (ex. in magazin, aeroport, pe strada, in cafenea, etc.) pentru operaţiuni bancare. Aceste puncte de acces pot fi controlate de infractori şi exista riscul ca datele transmise să fie compromise. Străduiţi-vă să utilizaţi numai reţele Wi-Fi securizate în care aveţi încredere. Se recomandă să dezactivaţi opţiunea de conectare automată la Wi-Fi.

8. Serviciile financiare ale Sistemului “MICB Mobile Banking”

8.1. Serviciile financiare ale Sistemului sunt Serviciile destinate creării şi transmiterii în adresa Băncii a Documentelor electronice de plată.

8.2. Tarifele referitoare la utilizarea Serviciilor financiare ale Sistemului, precum şi limitele aplicate utilizării acestora sunt stabilite în *Tarifele şi limitele privind deservirea cardurilor bancare emise de BC „Moldindconbank” S.A. (în continuare Tarife)*.

8.3. **Serviciul „P2P MICB”** - se efectuează în conformitate cu Condiţiile de utilizare a Serviciului „P2P MICB” accesibile la orice Ghişeu al Băncii sau pe pagina web.

8.3.1. **Serviciul „Transfer pe cardul propriu” –**permite efectuarea Transferurilor între cardurile personale.

8.3.2. **Serviciul „Transfer pe card Moldindconbank” –** serviciu ce permite efectuarea Transferurilor de pe Cardul emis pe numele Abonatului pe un alt card emis de Bancă pe numele altei persoane decât Abonatul.

8.3.3. Serviciile “Transfer pe card Mastercard străin”, „Transfer pe card VISA străin” - permit efectuarea Transferului de pe Cardul emis pe numele Abonatului pe un alt card emis de altă Bancă din R. Moldova și/sau străinătate.

8.4. **Serviciul „Cash by Code”** – permite Abonatului de a genera în Sistem un cod de unică folosință în baza căruia poate fi retrasă o anumită sumă de bani în numerar direct de la bancomat fără a utiliza un card bancar.

8.5. **Serviciul „Cash-In by Code”** – permite Abonatului de a genera în Sistem un cod unic de identificare a contului de card în baza căruia poate alimenta contul său de card cu o anumită sumă de bani în numerar direct la bancomatele Cash-In fără a utiliza un card bancar.

8.6. Serviciul „Cash by Code / Cash-In by Code” se prestează în conformitate cu Condiţiile de utilizare a Serviciului „Cash by Code” accesibile la orice Ghişeu al Băncii sau **pe pagina web.**

8.7. **Serviciul „Plăţi în baza contractelor de primire a plăţilor”:**

8.7.1. Serviciul „Plăţi în baza contractelor de primire a plăţilor” (în continuare în cadrul acestui compartiment „Plăţi”) permite Clientului perfectarea plăţilor în favoarea furnizorilor de servicii şi altor beneficiari de plăţi cu care Banca are contract cu privire la încasarea plăților de la persoane fizice cu includerea clauzei prin intermediul sistemelor de deservire la distanță (în continuare „Furnizor”).

8.7.2. Utilizarea acestui Serviciu duce la perfectarea Documentului electronic prin care Abonatul solicită efectuarea plăţii în favoarea Furnizorului şi totodată informarea Furnizorului privind faptul efectuării plăţii cu transmiterea în adresa acestuia a datelor care se conţin în acest Document. Acest Document are statut de cerere.

8.7.3. Banca stabileşte unilateral lista Furnizorilor de servicii şi o poate modifica fără preaviz.

8.7.4. În calitate de Furnizor de servicii poate servi şi Banca, în cazul în care alte servicii ale Băncii sunt achitate prin Serviciul „Plăţi în baza contractelor de primire a plăţilor”. În acest caz, condiţiile prestării serviciilor achitate astfel sunt gestionate de relaţiile respective ale Clientului cu Banca.

8.7.5. Serviciul „Plăţi” este destinat cel mai des pentru a perfecta Plăţi în adresa furnizorilor conform facturilor primite de la furnizor, însă permite pentru unii furnizori şi efectuarea Plăţilor fără a avea ca bază o factură (de exemplu, alimentarea contului în cazul pachetelor preplătite de telefonie mobilă).

8.7.6. Pentru fiecare Furnizor în Sistem este definit:

a. dacă este prezentă sau nu în Sistem lista facturilor înaintate de către Furnizor şi dacă Clientul are posibilitatea de a efectua căutarea acestora;

b. câmpurile care trebuie completate în Documentul electronic şi/sau care sunt completate automat de Sistem în baza facturii selectate de Client;

c. este efectuată sau nu autorizarea fiecărei Plaţi de către Furnizorul respectiv;

d. este permisă perfectarea Documentului electronic în baza facturii, fără factură sau ambele modalităţi;

e. este solicitată sau nu Autentificarea suplimentară pentru a fi primit spre executare Documentul electronic.

8.7.7. Etapele şi modalitatea de prelucrare a Plăţii:

a. **verificarea** Documentului electronic. În acest moment:

a.1. se verifică corectitudinea completării câmpurilor Documentului, conform cerinţelor stabilite de către Bancă;

a.2. dacă este prevăzut de contractul Băncii cu Furnizorul beneficiar, se solicită autorizarea plaţii de către Furnizorul respectiv;

a.3. se verifică posibilitatea efectuării acestei Plăţi de pe cardul indicat de către Abonat (suma disponibilă, statut, limite etc.).

b. **autorizarea** Plăţii (transferului) desemnează momentul în care Banca primeşte spre executare Documentul electronic respectiv. În acest moment:

b.1. Banca blochează instantaneu suma Plăţii pe Contul Cardului de pe care se efectuează Plata, ceea ce duce la micşorarea Sumei disponibile pe acesta;

b.2. dacă este prevăzut de contractul Băncii cu Furnizorul beneficiar, Banca informează Furnizorul respectiv cu privire la Plata efectuată şi parametrii acesteia.

c. **executarea finală** a Documentului electronic. Aceasta prevede următoarele acţiuni:

c.1. Banca debitează Contul Cardului de pe care se efectuează Plata;

c.2. Banca efectuează transferul mijloacelor băneşti în adresa Furnizorului beneficiar conform prevederilor relaţiilor dintre Bancă şi acesta;

c.3. Banca anunţă Furnizorul privind datele documentului de plată conform prevederilor agreate dintre Bancă şi acesta.

8.7.8. Responsabilitatea Băncii:

a. Banca este responsabilă de executarea corectă şi la timp a prevederilor pp. 8.7.7.c.2 şi 8.7.7.c.3, totodată termenele concrete de executare a acestor acţiuni depind de prevederile contractului încheiat între Furnizor şi Bancă.

b. Banca nu este responsabilă de reacţia şi timpul reacţiei Furnizorului la executarea de către Bancă a prevederilor pp. 8.7.7.c.2 şi 8.7.7.c.3, precum şi nu este responsabilă de calitatea mărfurilor şi serviciilor oferite Clientului de către Furnizor.

8.7.9. În cazul în care Clientul are litigii cu Furnizorul şi are nevoie de confirmarea executării Documentului electronic de plată autentificată de către Bancă – document ce atestă efectuarea Plăţii în adresa Furnizorului – Clientul îl poate primi la orice subdiviziune a Băncii. Pentru aceasta, Clientul trebuie:

a. să prezinte factura, în baza căreia a fost efectuată Plata. Pentru Plăţile care nu au fost efectuate în baza facturii, să comunice angajatului Băncii datele câmpurilor care au fost completate în documentul de plată (numărul telefonului, numărul contractului cu furnizorul etc.);

b. să prezinte buletinul de identitate;

c. să comunice operatorului data achitării facturii.

Notă: Fără cunoaşterea acestor date angajatul Băncii nu va avea posibilitate să verifice faptul efectuării Plăţii. Clientul poate vizualiza toate aceste date în Sistem, în Istoria tranzacţiilor.

8.7.10. Clientul poate vizualiza în Sistem lista documentelor de plată primite spre executare.

9. Serviciile non-financiare ale Sistemului “MICB Mobile Banking”

9.1. Serviciile non-financiare ale Sistemului sunt alte Servicii decât cele destinate creării şi transmiterii în adresa Băncii a Documentelor electronice de plată.

9.2. **Serviciile informaţionale:**

9.2.1. oferă Abonatului informaţii despre conturile şi cardurile sale, tranzacţiile efectuate etc.

9.2.2. Serviciile informaţionale pot fi prezentate ca servicii separate (cum este obţinerea extrasului din cont), cât şi integrate în interfaţa Sistemului, inclusiv în alte Servicii (ca de exemplu, afişarea Sumei disponibile pe Contul Cardului pe care se efectuează un transfer sau plată).

9.2.3. Istoria tranzacţiilor. Plăţi şi transferuri:

a. Afişează lista tranzacţiilor efectuate prin intermediul Sistemului;

b. Istoria tranzacțiilor pentru plăți și transferuri conține următoarele informații:

- Numărul de referință în Sistem a tranzacției;
- Data și ora tranzacției;

- Suma tranzacției și a comisionului perceput, dacă acesta există;

9.2.4. Istoria tranzacţiilor. Extras de pe card:

a. Afişează lista tranzacţiilor efectuate cu utilizarea Cardului selectat, în Sistem şi în afara acestuia.
b. Istoria tranzacțiilor în extrasul pentru card conține următoarele informații:

- Numărul de referință în Sistem a tranzacției;
- Data și ora tranzacției;
- Suma tranzacției și a comisionului perceput, dacă acesta există;
- Locul tranzacției;

9.2.5. Rechizitele contului:

- Afişează rechizitele contului de card pentru transferuri interbancare.
- Sistemul oferă posibilitatea de a transmite rechizitele contului către o adresă de email.

9.3. **Serviciile de gestionare a cardurilor / conturilor Abonatului:**

9.3.1. Blocarea cardului:

a. Utilizarea acestui Serviciu duce la blocarea Cardului;
b. În rezultatul utilizării acestui Serviciu, clientul transmite Băncii Document electronic cu statut de cerere de blocare a Cardului;
c. În funcţie de tipul blocării solicitat, cardul poate sau nu fi deblocat prin utilizarea Serviciului „Deblocarea cardului". Clientul este informat despre aceasta prin interfaţa Sistemului.

9.3.2. Deblocarea cardului:

a. Utilizarea acestui Serviciu duce la deblocarea Cardului blocat anterior prin Serviciul „Blocarea cardului". Deblocarea Cardurilor blocate prin alte modalităţi, inclusiv de către Bancă, nu este posibilă;
b. În rezultatul utilizării acestui Serviciu, clientul transmite Băncii Document electronic cu statut de cerere de deblocare a Cardului.

9.3.3. Activarea serviciului „Protecţia cardului" (Fereastra tranzacţională):

a. Utilizarea acestui Serviciu permite Abonatului să dețină securitate avansată asupra cardurilor sale;
b. La activarea serviciului **„Protecţia cardului" (Fereastra tranzacţională)** are loc blocarea operațiunilor de retragere a numerarului din contul de card și de achitare fără numerar pe un termen nelimitat;
c. În cazul necesității utilizării cardului, fereastra tranzacțională poate fi „deschisă" pentru a permite un număr de tranzacții prestabilit de către Abonat, pentru un interval de timp determinat și un număr de tranzacții limitate (prin operațiunea "Permite operațiunile"). La expirarea termenului sau a numărului de tranzacții specificate la deschiderea "Ferestrei tranzacționale" cardul se va bloca din nou.

9.3.4. Dezactivarea serviciului „Protecţia cardului"(Fereastra tranzacţională):

a. La dezactivarea serviciului „Protecţia cardului" (Fereastra tranzacţională) cardul va fi deblocat.

- Operaţiunea de dezactivare a serviciului „Protecţia cardului" (Fereastra tranzacţională) necesită autentificare prin SMS OTP sau ATM OTP, dacă Autentificarea în Sistem a avut loc printr-o modalitate de autentificare diferită de utilizarea Codului de acces. În cazul în care pentru autentificarea în Sistem se utilizează Codul de acces, dezactivarea serviciului „Protecţia cardului" nu necesită autentificare adițională.

9.4. **Serviciul de generare a parolelor de tip „Mobile OTP":**

9.4.1. Generarea parolei de tip „Mobile OTP" se efectuează prin intermediul meniului „Generarea parolei de unică folosinţă" din interiorul Sistemului „MICB Mobile Banking";
9.4.2. Generarea parolei de tip „Mobile OTP" este posibilă doar în cazul accesării Sistemului „MICB Mobile Banking" prin Codul de acces (5 cifre);
9.4.3. Ca bază pentru generarea parolei de tip „Mobile OTP" va fi utilizat codul tranzacţiei afişat în sistemul „MICB Web Banking" sau în E-Commerce (3D Secure);
9.4.4. În rezultatul generării acestui tip de parolă, clientul transmite Băncii Document electronic cu statut de creare a parolei de unică folosinţă „Mobile OTP";
9.4.5. Parola este activă 15 minute şi poate fi utilizată doar o singură dată.

9.5. **Serviciile de gestionare a Abonamentului şi a Factorilor de autentificare:**

9.5.1. Modificarea parolei:

a. Utilizarea acestui Serviciu duce la modificarea Parolei;

b. Clientul introduce în câmpurile respective ale interfeţei Sistemului Parola nouă care doreşte să-i fie alocată în Sistem. Sistemul îi alocă Parola cu condiţia că aceasta corespunde cerinţelor stabilite în prezentele Condiţii de utilizare (caracterele utilizate, lungimea etc.).

9.6. **Serviciul de gestiune a șabloanelor și Plăților programate:**

a. **Șabloane** - utilizarea acestui serviciu permite salvarea rechizitelor unui Document electronic, în scopul generării repetate a acestuia;

b. **Plăți programate -** presupune efectuarea unei plăți cu o regularitate stabilită de către Abonat (lunar, săptămânal). Setarea plăților programate presupune că abonatul permite debitarea directă periodică din contul său de card a mijloacelor bănești în favoarea prestatorilor de servicii și/sau transferul mijloacelor bănești (P2P MICB);

9.7. **Limite tranzacționale:**

a. Utilizarea acestui Serviciu permite Abonatului să gestioneze anumite limite aferente cardului / cardurilor sale pentru diferite tipuri de operațiuni sau să interzică complet unele operațiuni;

b. Setarea limitelor tranzacționale protejează Abonatul de fraude și alte riscuri;

c. La setarea limitelor tranzacționale, are loc limitarea operațiunilor pentru anumite tranzacții.

9.8. **Serviciul “SMS-Notificări”:**

a. Utilizarea acestui Serviciu permite Abonatului să primească notificări prin SMS despre tranzacțiile efectuate pe conturile de card proprii pentru care este activat serviciul;

b. Banca oferă Clientului posibilitate de abonare /modificare /dezabonare de la Serviciu, iar odată cu obţinerea statutului de Abonat, posibilitatea de a beneficia de funcţionalitatea Serviciului „SMS-notificări”.

c. Serviciul se utilizează în conformitate cu Condițiile de Prestare a Serviciului “SMS-Notificări” și a altor mesaje de notificare.

9.9. **Serviciul “Localizarea geografică”:**

a. Utilizarea acestui Serviciu permite Abonatului să vizualizeze pe hartă în mod grafic și intuitiv locația tuturor bancomatelor / filialelor / agențiilor Băncii în referință cu locația geografică a dispozitivului pe care rulează aplicația mobilă „MICB Mobile Banking”.

10. Drepturile şi obligaţiile Părţilor

10.1. Părţile îşi asumă drepturile şi obligaţiile menţionate expres în capitolul curent, în alte capitole ale prezentelor Condiţii de utilizare, cererile depuse de către Client şi alte documente transmise de către o Parte celeilalte Părţi în legătură cu obiectul prezentelor Condiţii de utilizare.

10.2. Banca este obligată:

10.2.1. să execute Tranzacţiile în conformitate cu regimul de prestare a Serviciului respectiv definit în prezentele Condiţii de utilizare;

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

10.2.3. să asigure un grad adecvat de securitate şi siguranţă operaţională a localului, echipamentului de comunicaţii şi procesare, precum şi a soluţiei soft prin intermediul căreia se iniţiază, înregistrează, controlează şi recepţionează Tranzacţiile electronice;

10.2.4. să asigure confidenţialitatea datelor referitoare la Abonat precum şi a Tranzacţiilor efectuate de acesta prin intermediul Sistemului, în conformitate cu prevederile legislaţiei în vigoare aferente secretului comercial;

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

10.2.6. să asigure identificarea şi înscrierea corectă a Abonatului în Sistem, în baza actului de identitate al acestuia şi în baza altor documente şi măsuri care permit identificarea Abonatului în conformitate cu actele normative în vigoare şi riscurile potenţiale;

10.2.7. să asigure stocarea şi păstrarea informaţiilor referitoare la Tranzacţiile electronice efectuate prin intermediul Sistemului pentru perioadele de timp prevăzute de actele normative în vigoare, precum şi să monitorizeze corespunderea Tranzacţiilor electronice efectuate prin intermediul Sistemului condiţiilor contractuale şi normelor în vigoare;

10.2.8. să furnizeze periodic Abonatului sau la cererea expresă a acestuia informaţii referitoare la Tranzacţiile efectuate prin intermediul Sistemului sau informaţii privind situaţia contului bancar al Abonatului. Aceste informaţii vor fi prezentate în conformitate cu prevederile contractuale existente dintre Bancă şi Abonat, cu respectarea prevederilor legislaţiei în vigoare;

10.2.9. să crediteze contul bancar al Abonatului cu valoarea despăgubirilor din momentul recunoaşterii dreptului Abonatului la acestea sau de la stabilirea acestui drept de către o instanţă de judecată ori de arbitraj;

10.2.10. să asigure securitatea sistemului MICB "Mobile Banking", cu condiția respectării de către client a asigurării acțiunii de **Log out / Ieșire / Выход** după fiecare sesiune de utilizare a sistemului "MICB Mobile Banking".

10.3. Clientul este obligat:

10.3.1. să ia cunoştinţă de prezentele Condiţii de utilizare, Regulile de utilizare a cardului şi Instrucţiunii de utilizare a Sistemului "MICB Mobile Banking" înaintea abonării la Sistem şi să utilizeze Sistemul în strictă conformitate cu prevederile acestora;

10.3.2. să acceseze Sistemul numai cu ajutorul Telefonului mobil/ dispozitivului mobil care corespunde cerinţelor indicate în Instrucţiune;

10.3.3. în cazul autentificării prin utilizarea amprentei digitale, să activeze funcționalitatea de autentificare prin amprenta digitală pe dispozitivul "touch id / FingerPrint" și să înregistreze cel puțin una din amprentele personale pentru a controla accesul la dispozitivul "touch id / FingerPrint", să selecteze autentificarea în sistem prin amprenta digitală stocată în memoria dispozitivului "touch id / FingerPrint";

10.3.4. să asigure confidenţialitatea elementelor de autentificare (Login, Parolă, SMS OTP, ATM OTP şi Codul de acces, amprentă digitală), să ia măsuri rezonabile de protejare a acestora contra compromiterii şi să nu admită utilizarea acestora de către terţe persoane;

10.3.5. să asigure acțiunea de **Log out / Ieșire / Выход** după fiecare sesiune de utilizare a sistemului "MICB Mobile Banking";

10.3.6. să verifice corectitudinea documentelor electronice pregătite pentru a fi transmise spre executare, cât şi a documentelor deja executate de către Bancă;

10.3.7. să înştiinţeze Banca (prin intermediul Serviciului Suport Carduri Bancare 24/24 sau la ghişeele Băncii) imediat ce constată:

a. modificarea neautorizată a soldului contului bancar;

b. orice eroare sau neregulă apărută în urma gestionării de către Bancă a contului bancar;

c. elementele ce creează suspiciuni cu privire la posibilitatea cunoaşterii de către persoane neautorizate a factorilor de autentificare deţinute de Abonat;

d. disfuncţionalităţi ale Sistemului sau dacă parolele primite sunt incorecte;

10.3.8. să manifeste o atitudine responsabilă privind asigurarea siguranţei şi securităţii Sistemului.

10.4. Banca are dreptul:

10.4.1. să perceapă taxe şi comisioane conform *Tarifelor și Limitelor referitor la deservirea cardurilor bancare emise de BC "Moldindconbank" S.A.;*

10.4.2. să nu primească spre executare prin intermediul Sistemului Documentele electronice dacă primirea acestora nu este prevăzută în prezentele Condiţii de utilizare şi Instrucţiuni, chiar şi în cazul în care Banca primeşte / este obligată să primească asemenea documente prin alte căi (pe suport hârtie, prin telefon);

10.5. Banca nu poartă răspundere pentru cauzele de dispută ce ar putea interveni între Abonat și Beneficiarul plății ca urmare a setării plăților programate și neasigurării de către abonat a mijloacelor bănești suficiente și/sau modificării de către furnizor a structurii documentelor utilizate în cadrul plății, precum și a cauzelor în care cardul este blocat, expirat, are activat fereastra tranzacțională.

10.6. Banca nu poartă răspundere pentru daunele suportate de client ca urmare a nerespectării recomandărilor de utilizare securizată a Sistemului „MICB Mobile Banking" precum și închiderii incorecte a sesiunii de utilizare a sistemului.

11. Responsabilitatea Părţilor şi ordinea repartizării pierderilor

11.1. Clientul este responsabil de veridicitatea şi corectitudinea informaţiei transmise prin intermediul Sistemului, pentru Tranzacţiile efectuate şi Documentele electronice transmise în adresa Băncii în cadrul Sesiunii de utilizare a Sistemului, în cazul în care a avut loc Autentificarea Clientului în Sistem bazată pe Login-ul Clientului şi Factorii de autentificare deţinute de Client, inclusiv cele efectuate fraudulos de către persoanele terţe, până la suspendarea Login-lui sau Factorilor de Autentificare (Parolei, Parolei ATM OTP, Parolei SMS OTP, Codul de acces, amprenta digitală) cu utilizarea cărora a fost autentificată Tranzacţia respectivă.

11.2. Clientul este responsabil de neadmiterea compromiterii Factorilor de autentificare deţinuţi.

11.3. Banca şi Clientul recunosc puterea juridică a Tranzacţiilor efectuate în cadrul Sesiunii de utilizare a Sistemului „MICB Mobile Banking”.

11.4. Banca şi Clientul recunosc că Documentele electronice transmise de către client Băncii sunt echivalente celor depuse personal de către Client şi semnate cu semnătura olografă a acestuia.

11.5. Banca şi Clientul recunosc faptul că Documentele electronice transmise în adresa Băncii în cadrul Sesiunii de utilizare a Sistemului „MICB Mobile Banking” se echivalează cu cele perfectate de Client pe suport hârtie şi produc aceleaşi drepturi şi obligaţiuni ale Părţilor.

11.6. Banca va lua toate măsurile necesare pentru prevenirea riscurilor ce pot apărea din utilizarea frauduloasă a Sistemului „MICB Mobile Banking”. Banca este responsabilă:

11.6.1. pentru neexecutarea sau executarea necorespunzătoare a Tranzacţiilor efectuate prin intermediul Sistemului:

a. în cazul în care executarea necorespunzătoare este atribuită unei disfuncţionalităţi a Sistemului sau a unei componente a acestuia, cu condiţia că disfuncţionalitatea nu a fost cauzată intenţionat de către Abonat;

b. chiar dacă Tranzacţiile au fost iniţiate prin utilizarea mijloacelor care nu se află sub controlul Băncii, cu condiţia să se facă dovada că Tranzacţiile a fost iniţiate în conformitate cu prevederile prezentelor Condiţii de utilizare.

11.6.2. pentru Tranzacţiile electronice iniţiate după momentul notificării Băncii de către Abonat a pierderii controlului asupra Sistemului (de exemplu funcţionării defectuoase a Sistemului, compromiterea parolelor sau a altor informaţii sensibile de către persoane neautorizate etc.);

11.6.3. pentru pierderile suportate de către Abonat ca rezultat al unei fraude comise de către o persoană sau grup de persoane terţe prin exploatarea unei vulnerabilităţi a Sistemului, cu condiţia că Abonatul a respectat toate prevederile contractuale de utilizare a Sistemului.

12. Serviciul suport carduri 24/24

12.1. Banca oferă suport telefonic Abonaţilor prin intermediul Serviciului suport carduri 24/24 al Băncii.

12.2. Serviciul suport carduri 24/24 este accesibil non-stop (24 din 24 ore, 7 zile pe săptămână) la linia telefonică fierbinte, numărul de telefon: /+373/ 22 **54-89-40**.

12.3. Abonatul poate apela Serviciul suport carduri 24/24 în vederea:

12.3.1. comunicării situaţiilor de urgenţă;

12.3.2. solicitării suspendării / reactivării Login-lui, suspendării Parolei, Parolei ATM OTP şi/sau Parolei SMS OTP;

12.3.3. obţinerii consultaţiilor privind utilizarea Sistemului „MICB Mobile Banking”.

Serviciul Suport Carduri 24/24:
/+373/ 22 **548 940**

13. Dispoziţiile finale

13.1. Relaţiile dintre Bancă şi Abonat care apar în rezultatul utilizării Sistemului „MICB Mobile Banking” şi care nu sunt specificate în prezentele Condiţii de utilizare, vor fi reglementate în conformitate cu Regulile de utilizare a cardului şi legislaţia în vigoare a Republicii Moldova.

13.2. Toate neînţelegerile şi/sau litigiile apărute între Abonat şi Bancă pe marginea utilizării Sistemului „MICB Mobile Banking” 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.

13.3. Banca va informa Abonaţii 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).