



În vigoare din 23.07.2015

Aprobat de Comitetul de conducere al Băncii
la 23.07.2015, procesul verbal nr. 44

CONDIȚIILE DE UTILIZARE a sistemului „MICB Mobile-Banking”

1. Prevederi generale

1.1. Prezentele Condiții de utilizare a Sistemului „MICB Mobile-Banking”, stabilite de BC „Moldindconbank” S.A., descriu modul în care Banca oferă Clienților săi posibilitatea utilizării Sistemului „MICB Mobile-Banking”, precum și modul de utilizare a acestuia de către Abonați.

1.2. Prezentele Condiții de utilizare completează și detaliază relația contractuală existentă între Deținător și Bancă, în conformitate cu Regulile de utilizare a cardului. Regulile de utilizare a cardului sunt accesibile la orice Ghișeu al Băncii sau pe pagina web <http://www.micb.md/required-info/>.

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

2. Noțiunile utilizate

În cuprinsul Condițiilor de prestare și în orice document care derivă sau are legătura cu acestea, termenii de mai jos vor fi înțeleși după cum urmează:

- **Sistemul „MICB Mobile-Banking”, Sistem, Aplicație** – este un Sistem informațional și tranzacțional de deservire bancară la distanță a clienților – persoanelor fizice – de tipul „mobile-banking”, care utilizează tehnologia aplicațiilor mobile, fiind accesibil a fi instalat din magazinele virtuale oficiale „App Store” și „Android Play Market”.
- **Sistem de deservire bancară la distanță** – (conform Regulamentului privind utilizarea sistemelor de deservire bancară la distanță emis de Banca Națională a Moldovei) soluție informatică, pusă la dispoziție de către banca comercială clienților săi, ce permite deținătorului să aibă acces la distanță la mijloacele aflate în contul bancar al sau, în scopul obținerii de informații privind starea contului bancar și a operațiunilor realizate, efectuării de plăți în numele și din ordinul deținătorului prin intermediul unei aplicații informatice, a unei metode de autentificare electronică și al unui mijloc de comunicație. **Sistemul de deservire bancară la distanță informațional** este un sistem utilizat în scopul obținerii de informații privind starea contului bancar și a operațiunilor realizate. **Sistemul de deservire bancară la distanță tranzacțional** este un sistem utilizat în scopul efectuării de plăți în numele și din ordinul deținătorului.
- **Condiții de utilizare** – prezentul document, ce vine să detalieze modul în care Clienții Băncii se pot abona la și ulterior utiliza Sistemul „MICB Mobile-Banking”.
- **Tarife** – Tarifele și limitele BC „Moldindconbank” S.A. referitoare la deservirea cardurilor bancare, publicate pe panourile informative ale subdiviziunilor Băncii, precum și pe pagina web <http://www.micb.md/planuri-tarifare/>.
- **Card** – card de plată emis de BC „Moldindconbank” S.A. pe numele Deținătorului, în conformitate cu Contractul încheiat între Deținător și Bancă.
- **Card principal** – Card emis pe numele titularului Contului de card.
- **Card secundar** – Card emis pe un alt nume decât cel al titularului Contului de card.
- **Deținător de card** – persoana fizică pe numele căreia este emis Cardul. Cuprinde termenii „Deținătorul principal” și „Utilizatorul autorizat”.
- **Deținător principal** – Deținătorul Cardului principal care este totodată posesor al Contului de card la care este emis acest Card.
- **Utilizator autorizat** – Deținător de card, altul decât Deținătorul principal.
- **Cont de card** – contul deschis și menținut de către Deținătorul principal la Bancă, cu scopul înscrierii Tranzacțiilor cu Carduri, precum și a altor operații prevăzute de contractul respectiv.
- **Bancă** – proprietarul Sistemului: BC „Moldindconbank” S.A.
- **Client** – Deținătorul Cardului.
- **Abonat** – Clientul care este abonat la Sistem.

- **Abonament** – totalitatea relațiilor reglementate dintre Abonat și Bancă aferente Sistemului, precum și înregistrarea parametrilor și statutului acestei relații.
- **Abonare la Sistem** – procesul în urma căruia Clientul obține calitatea de Abonat în sensul prezentelor Condiții de utilizare, se stabilește Abonamentul și Banca îi alocă Clientului Loginul și Parola.
- **Telefon mobil/ dispozitiv mobil** – telefon mobil sau alt tip de echipament, care reprezintă o combinație de echipamente electronice și programe ce rulează pe acesta, utilizat de către Abonat pentru conectarea la Sistem.
- **Server „MICB Mobile-Banking”, Serverul Sistemului** – este totalitatea echipamentului electronic și programelor Băncii, pe care rulează Sistemul și cu care telefonul mobil/ dispozitivul mobil al Abonatului stabilește legătura cu scopul stabilirii Sesiunii de utilizare a Sistemului.
- **Instrucțiuni** – Instrucțiunile de utilizare a Sistemului „MICB Mobile-Banking” – document perfectat de Bancă și accesibil de pe pagina <https://wb.micb.md>, în care este descrisă modalitatea utilizării Sistemului de către Abonat. Instrucțiunile sunt parte integrantă a prezentelor Condiții de utilizare și sunt obligatorii de respectat în cadrul Abonării și 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 cardul 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 Abonatului și Serverul Sistemului, în baza Autentificării Abonatului în Sistem, pe parcursul căreia Abonatului îi sunt accesibile Serviciile Sistemului.
- **Autentificare electronică (a Abonatului) în Sistem** – Autentificarea electronică, procesul de verificare a identității Abonatului prin Login și metodele de autentificare stabilite în prezentele Condiții, cu scopul stabilirii Sesiunii de utilizare a Sistemului.
- **Serviciu** – serviciul oferit de Bancă Abonatului prin intermediul Sistemului, conform funcționalității Sistemului și produselor / serviciilor deținute de către Abonat (conturilor, cardurilor etc.), cu ajutorul căruia Abonatul poate comanda executarea unui Document electronic, inclusiv efectuarea de către Bancă a unei Tranzacții, obținerea sau modificarea unui produs sau serviciu (inclusiv și unui oferit în afara Sistemului), sau obține din partea Băncii informație.
- **Document electronic** – orice document perfectat și/sau transmis Băncii de către Abonat prin intermediul Sistemului.
- **Tranzacție electronică, Tranzacție** – operațiune efectuată în formă electronică în cadrul Sesiunii de utilizare a Sistemului în baza Documentului electronic, în cadrul utilizării unui serviciu și protejată printr-un mecanism ce permite verificarea autenticității, integrității și non-repudierii (imposibilității negării) acesteia.
- **Autentificarea suplimentară** – autentificarea **electronică a** identității Abonatului și/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 funcție de nivelul de risc al Serviciului, suma Tranzacției sau alți factori. Solicitarea sau nesolicitarea Autentificării suplimentare este efectuată la decizia Băncii. Totodată Autentificarea suplimentară poate fi utilizată în procesul Abonării la Sistem, precum și pentru restabilirea Loginului și/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 folosință în cadrul unui mesaj SMS la Numărul de telefon OTP și introducerea acestei parole de către Abonat în interfața Sistemului.
- **Număr de telefon OTP** – numărul de telefon mobil stabilit de către client în cadrul Serviciului „SMS-notificări” sau comunicat Băncii în cadrul Chestionarului clientului – persoană fizică, cu condiție 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.).
- **Autentificarea suplimentară de tip „ATM OTP”, ATM OTP** – tipul Autentificării suplimentare care prevede primirea de către Abonat a unei liste de parole de unică folosință prin intermediul bancomatului Băncii și introducerea acestei parole de către Abonat în interfața Sistemului.
- **Autentificare suplimentară de tip „Mobile OTP”** – tipul Autentificării suplimentare care prevede generarea de către Abonat a unei parole de unică folosință prin intermediul Aplicației, în baza unui cod generat în sistemul „MICB Web Banking”.
- **Factor de autentificare** – Parola, Parola ATM OTP sau SMS OTP – informația și / sau dispozitivele deținute de Client pentru asigurarea procesului de autentificare.
- **Cod de acces** - tipul Autentificării suplimentare în Sistem, care prevede introducerea unui cod numeric de acces la aplicație, setat de către Abonat în baza mesajului „SMS OTP”.

3. Instalarea aplicației

3.1. Instalarea Aplicației 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 Aplicației pentru telefoanele mobile/ dispozitivele mobile care rulează pe sistemul de operare Android va fi efectuată de Client, din magazinul virtual oficial „Android Play Market”.

4. Abonarea la Sistem

4.1. Abonarea la Sistem are ca rezultat obținerea de către Client a Loginului și Parolei.

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

4.2.1. Obținerea Loginului și Parolei prin operațiunea respectivă accesibilă la bancomatul Băncii:

- a. Clientul autentifică operațiunea de primire a Loginului și Parolei prin introducerea unui Card valabil emis pe numele Clientului și a Codului PIN în elementele de interacțiune ale bancomatului;
- b. În rezultatul operațiunii de primire a Loginului și Parolei Banca alocă Clientului Loginul și Parola generate printr-un algoritm de creare a valorilor alfanumerice aleatorii și le imprimă pe bonul bancomatului;
- c. Clientul este responsabil pentru compromiterea Loginului și Parolei în cazul nepreluării din imprimanta bancomatului a bonului cu Login și Parolă imprimate.

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

- a. Clientul efectuează abonarea prin intermediul site-ului <https://wb.micb.md>;
- b. Clientul autentifică operațiunea de primire a Loginului și Parolei prin introducerea numărului unui Card valabil emis pe numele Clientului și efectuarea Autentificării alternative de tip „SMS OTP”.
- c. În cadrul operațiunii Clientul introduce în câmpurile respective ale interfeței Sistemului Loginul și Parola care dorește să-i fie alocată de către Bancă. Banca îi alocă Loginul și Parola cu condiția că acestea corespund cerințelor stabilite în prezentele Condiții de utilizare (caracterele utilizate, lungimea etc.) și totodată dacă Loginul nu este deja utilizat pentru identificarea unui alt Abonat.

4.3. Clientul, prin Abonare la Sistem, confirmă faptul că a luat cunoștință de prezentele Condiții de utilizare și le acceptă.

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

4.5. Abonarea poate să fie efectuată doar personal de către Client și nu poate fi efectuată de către mandatar, tutore, reprezentant legal sau orice altă persoană terță.

5. Restabilirea Loginului și/sau Parolei

5.1. Restabilirea Loginului și/sau Parolei poate fi efectuată prin următoarele modalități:

5.1.1. Obținerea Loginului și Parolei prin operațiunea respectivă accesibilă la bancomatul Băncii:

- a. Clientul autentifică operațiunea de primire a Loginului și Parolei prin introducerea unui Card valabil emis pe numele Clientului și a Codului PIN în elementele de interacțiune ale bancomatului;
- b. În rezultatul operațiunii de primire a Loginului și Parolei, Banca îi atribuie Clientului o Parolă nouă, generată printr-un algoritm de creare a valorilor alfanumerice aleatorii și imprimă Loginul și Parola pe bonul bancomatului.
- c. Clientul este responsabil pentru compromiterea Loginului și Parolei în cazul nepreluării din imprimanta bancomatului a bonului cu Login și Parolă imprimate.

5.1.2. Obținerea Loginului și modificarea Parolei prin introducerea numărului Cardului și Autentificării alternative de tip „SMS OTP”:

- a. Clientul efectuează această operațiune prin intermediul Sistemului;
- b. Clientul autentifică operațiunea de primire a Loginului și Parolei prin introducerea numărului unui Card valabil emis pe numele Clientului și efectuarea Autentificării alternative de tip „SMS OTP”.
- c. În cadrul operațiunii, Clientului îi este afișat în interfața Sistemului Loginul său, totodată Clientul introduce în câmpurile respective ale interfeței Sistemului Parola nouă care dorește să-i fie alocată de către Bancă. Banca îi alocă Parola cu condiția că aceasta corespunde cerințelor stabilite în prezentele Condiții de utilizare (caracterele utilizate, lungimea etc.).

6. Securitatea Sistemului

- 6.1. Securitatea Sistemului este asigurată prin următoarele cerințe de autentificare:
- 6.1.1. o persoană poate să se Aboneze la sistem în calitate de Client sau să obțină acces la Loginul și Parolă doar în baza autentificării prin Card și Cod PIN la bancomat sau în baza numărului Cardului și Autentificării alternative în Sistem;
 - 6.1.2. o persoană poate să obțină accesul la Sistem în calitate de Abonat doar în baza procedurii Autentificării în Sistem;
 - 6.1.3. în cadrul Sesiunii de utilizare a Sistemului, unele Servicii sunt accesibile doar în baza Autentificării suplimentare.
- 6.2. Reieșind din faptul că factorul principal al securității Sistemului este autentificarea, securitatea Sistemului este în cea mai mare măsură influențată de necompromiterea Factorilor de autentificare și anume:
- 6.2.1. Necompromiterea Cardului, datelor cardului și a PIN-ului. Cerințele de securizare ale acestora sunt descrise în Regulile de utilizare a cardului;
 - 6.2.2. Necompromiterea Parolei. Compromiterea Parolei este situația în care Clientul nu este ferm convins asupra faptului că aceasta nu este accesibilă persoanelor terțe;
 - 6.2.3. Necompromiterea parolelor de unică folosință ATM OTP. Compromiterea ATM OTP este situația în care Clientul nu este ferm convins asupra faptului că acestea nu sunt accesibile persoanelor terțe;
 - 6.2.4. Necompromiterea Factorului de autentificare „SMS OTP”. Compromiterea acestui Factor este situația în care Clientul nu este ferm convins asupra faptului mesajele transmise pe numărul de telefon OTP nu sunt accesibile persoanelor terțe.
- 6.3. Clientul este responsabil pentru necompromiterea Factorilor de autentificare deținute de el.
- 6.4. Cu scopul prevenirii compromiterii Parolei, Clientul trebuie:
- 6.4.1. să nu înscrie Parola pe un suport care permite asocierea cu Sistemul, prin natura sau poziționarea sa;
 - 6.4.2. să modifice regulat Parola cu ajutorul Serviciului respectiv al Sistemului;
 - 6.4.3. să asigure protejarea Calculatorului /Telefonului mobil/ dispozitivului mobil său utilizând softul specializat (antivirus, firewall etc.), politicile de limitare a accesului la resurse și alte metode de securitate informațională.
- 6.5. În cazul în care Parola este compromisă, Clientul trebuie să modifice imediat Parola prin una din următoarele modalități:
- 6.5.1. Serviciul respectiv în cadrul Sesiunii de utilizare a Sistemului;
 - 6.5.2. Operațiunea de modificare a Parolei prin introducerea numărului Cardului și Autentificării alternative de tip „SMS OTP” sau „ATM OTP”;
 - 6.5.3. Obținerea Loginului și Parolei (regenerate) prin operațiunea respectivă accesibilă la bancomatul Băncii;
 - 6.5.4. În cazul în care Clientul nu are posibilitate de a efectua acțiunile menționate mai sus, acesta trebuie să contacteze imediat Serviciul suport al Băncii pentru a anula Parola.
- 6.6. **Cerințele față de Parolă:**
- 6.6.1. Parola trebuie să conțină cel puțin 8 simboluri și cel mult 20, să conțină cel puțin o literă latină majusculă, o literă latină minusculă și o cifră;
 - 6.6.2. Este interzisă utilizarea altor caractere decât litere latine majuscule/minuscule și cifre;
 - 6.6.3. Este interzisă stabilirea Parolei care coincide cu una din 12 Parole utilizate anterior.
 - 6.6.4. Sistemul va suspenda Parola pentru 15 minute după fiecare 3 introduceri greșite consecutive.
 - 6.6.5. Sistemul va impune modificarea parolei de către Abonat cel puțin o dată la 90 zile.
- 6.7. În cazul în care unul din Factorii de autentificare este compromis, Clientul trebuie să:
- 6.7.1. verifice atent Tranzacțiile efectuate din numele său pentru a depista pe cele frauduloase;
 - 6.7.2. anunțe imediat Banca și să comunice detaliile privind circumstanțele compromiterii și eventualele efecte ale acesteia.
- 6.8. În cazul în care parola (sau lista de parole) ATM OTP este compromisă, Clientul trebuie să solicite anularea listei respective de ATM OTP prin una din următoarele modalități:
- 6.8.1. să genereze o nouă listă de ATM OTP;
 - 6.8.2. să contacteze Serviciul suport al Băncii pentru a anula lista de parole ATM OTP.
- 6.9. În cazul în care Factorul SMS OTP este compromis, Clientul trebuie:
- 6.9.1. să solicite operatorului de telefonie mobilă suspendarea numărului de telefon (utilizat în calitate de număr de telefon OTP) și restabilirea accesului exclusiv al Clientului la acest număr de telefon;

- 6.9.2. să solicite Băncii, prin contactarea Serviciului suport al Băncii, suspendarea numărului de telefon OTP în sistemul informațional al Băncii;
- 6.9.3. să solicite Băncii modificarea numărului de telefon utilizat în calitate de număr de telefon OTP prin una din următoarele modalități:
- modificarea numărului de telefon în cadrul Serviciului „SMS-notificări” prin intermediul bancomatului Băncii sau prin depunerea cererii respective la una dintre subdiviziunile Băncii;
 - modificarea numărului de telefon mobil în afara Serviciului „SMS-notificări”, prin depunerea Chestionarului pentru client – persoană fizică la una dintre subdiviziunile Băncii.
- 6.10. Suspendarea / reactivarea Loginului:
- 6.10.1. În cazul în care securitatea Loginului este compromisă din motive diferite și securitatea Loginului nu poate fi restabilită (asigurată) prin suspendarea / anularea Factorilor de autentificare, Clientul trebuie să solicite suspendarea Loginului, apelând Serviciul suport al Băncii.
- 6.10.2. În cazul suspendării Loginului Autentificarea în Sistem și restabilirea parolei nu vor fi accesibile.
- 6.10.3. Abonatul poate solicita reactivarea unui Login suspendat apelând personal Serviciul suport al Băncii, cu condiția identificării reușite a Abonatului de către operatorul Serviciului suport în baza datelor anterior prezentate de către Abonat Băncii.
- 6.10.4. Reactivarea Loginului nu duce în sine la reactivarea Factorilor de autentificare.
- 6.11. Banca protejează datele transmise între Serverul Sistemului și Telefon mobil/ dispozitiv mobil prin cifrarea acestora așa cum este definit în specificațiile tehnice ale protocolului SSL.
- 6.12. Banca recomandă următoarele modalități de utilizare securizată a Sistemului „Mobile Banking”:
- 6.12.1. Să nu divulge informația confidențială altor persoane (PIN, numărul de card, parole, conturi, datele personale);
- 6.12.2. Să nu lase dispozitivul fără supraveghere în special după procedura de autentificare și să asigure că ecranul dispozitivului nu este vizibil altor persoane;
- 6.12.3. Să seteze parola de acces la dispozitivul mobil și opțiunea de blocare a dispozitivului după o perioadă de inactivitate;
- 6.12.4. Să utilizeze parole și coduri de acces puternice, pentru a evita spargerea lor;
- 6.12.5. Să utilizeze diferite parole pentru fiecare serviciu (poșta electronică, conturile de acces la rețelele de socializare, etc.);
- 6.12.6. Să nimicească cecurile cu parolele OTP dacă nu vor fi utilizate Să descarce 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;
- 6.12.7. Să efectueze regulat actualizarea sistemului de operare, aplicației Mobile Banking și altor aplicații instalate pe dispozitivul mobil, utilizând numai surse oficiale;
- 6.12.8. Pentru a fi siguri că nu descărcați ceva dubios, dezactivați în setările telefonului pe platforma Android opțiunea „Surse Necunoscute” în setările de „Securitate”;
- 6.12.9. Să instaleze pe dispozitivul mobil aplicații anti-virus și să le actualizeze regulat. De asemenea trebuie actualizată aplicația anti-virus la calculatoarele la care se conectează dispozitivul mobil;
- 6.12.10. Să nu păstreze pe dispozitivul mobil informație confidențială (PIN coduri, numărul de card, parole de acces), de exemplu în mesaje SMS, email-uri, mementouri, notițe, etc.;
- 6.12.11. Aplicația Mobile Banking va fi utilizată numai de Abonatul la Sistem;
- 6.12.12. Să ștergă informația confidențială în cazul transmiterii dispozitivului altor persoane (vinderea, reparația). Pentru aceasta este necesar să restabilească setările prestabilite din fabrică. Ștergerea informației cu utilizarea punctelor de meniu va permite infractorului restabilirea ei;
- 6.12.13. Să activeze opțiunea de control la distanță pentru ștergerea datelor la distanță sau blocare în cazul pierderii dispozitivului;
- 6.12.14. Să nu execute operațiunea de obținere a dreptului de administrator (jail-break, rooting). Aceste operațiuni pot scădea nivelul de securitate și expune Sistemul unor riscuri suplimentare;
- 6.12.15. În cazul pierderii sau furtului dispozitivului mobil, să schimbe urgent parola de acces la sistemul de deservire bancară la distanță, să informeze imediat Banca pentru blocarea cardurilor și a accesului la Sistem. Apoi să sune operatorul telefoniei mobile pentru blocarea cartelei SIM;
- 6.12.16. 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 modalității de Autentificare Suplimentară de tip SMS OTP;
- 6.12.17. Să fie vigilenți la atacurile de tip phishing scopul cărora este obținerea de la client a informației confidențiale. Să nu execute mesajele primite prin email sau SMS prin care se solicită divulgarea datelor

confidențiale. Banca niciodată nu transmite mesaje SMS și email-uri pentru a solicita de la clienți informație confidențială;

- 6.12.18. Să monitorizeze regulat operațiunile executate. Extrasul de cont și card primit de la Sistem, va permite depistarea la timp și semnalarea operativă a Băncii despre neregulile identificate;
- 6.12.19. În cazul nefuncționării cartelei SIM să sune imediat la operatorul telefoniei mobile pentru a se asigura că cauza nu este urmare a acțiunilor frauduloase;
- 6.12.20. Să termine lucrul cu aplicația mobilă prin accesarea butonului Exit (Ieșire);
- 6.12.21. Să ignoreze propunerile de instalare a unor „aplicații importante” sau „update-uri importante” dacă ele sunt primite de la persoane sau companii necunoscute (de exemplu prin email-uri, SMS, etc.);
- 6.12.22. Să evite utilizarea rețelelor wireless/Wi-Fi publice (ex. în magazin, aeroport, pe strada, în cafenea, etc.) pentru operațiuni bancare. Aceste puncte de acces pot fi controlate de infractori și există riscul ca datele transmise să fie compromise. Străduiți-vă să utilizați numai rețele Wi-Fi securizate în care aveți încredere. Se recomandă să dezactivați opțiunea de conectare automată la Wi-Fi.

7. Serviciile financiare ale Sistemului

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

7.2. Tarifele referitoare la utilizarea Serviciilor financiare ale Sistemului, precum și limitele aplicate utilizării acestora sunt stabilite în *Tarifele și limitele BC „Moldindconbank” S.A. referitoare la deservirea cardurilor bancare* (Tarife).

7.3. Transferuri pe carduri / conturi (Serviciile „Transfer pe cardul propriu” și „Transfer pe card Moldindconbank”):

7.3.1. Utilizarea acestor servicii permite perfectarea Documentului electronic prin care Abonatul solicită efectuarea Tranzacției de transfer de mijloace bănești de pe Cardul emis pe numele Abonatului pe un alt card. Acest Document are statut de cerere.

7.3.2. Modalitatea de prelucrare a Tranzacției:

- a. autorizarea Tranzacției (Transferului) desemnează momentul în care Banca primește spre executare Documentul electronic respectiv. În acest moment:
 - a.1. Banca blochează instantaneu suma Transferului pe Contul Cardului de pe care se efectuează Transferul, ceea ce duce la micșorarea Sumei disponibile pe acesta.
 - a.2. Banca, la discreția sa, poate majora instantaneu cu suma Transferului Suma disponibilă pe Contul Cardului pe care se efectuează Transferul, până la executarea finală a transferului.
- b. executarea finală a Transferului:
 - b.1. Transferul se execută:
 - b.1.1. pentru Documentele primite spre executare în zilele de lucru până la ora 18:00 – în ziua primirii spre executare;
 - b.1.2. pentru celelalte Documente – la discreția Băncii, în funcție de posibilitățile tehnice și operaționale, dar nu mai târziu de următoarea zi de lucru.
 - b.2. Executarea Transferului duce la debitarea Contului Cardului de pe care se efectuează Transferul și creditarea Contului Cardului pe care se efectuează Transferul.

7.3.3. Banca poate percepe comisioane pentru prelucrarea Transferului, atât de pe Contului Cardului de pe care se efectuează Transferul cât și de pe Contului Cardului pe care se efectuează Transferul, dacă acestea sunt prevăzute în Tarifele în vigoare la ziua executării Transferului.

7.3.4. Dacă valuta Transferului nu coincide cu valuta Contului Cardului, Banca va converti aceasta la cursul comercial al Băncii stabilit pentru operațiunile cu carduri pentru ziua executării Transferului.

7.3.5. Serviciul „Transfer pe cardul propriu”:

- a. Serviciul „Transfer pe cardul propriu” permite efectuarea Transferului de pe Cardul emis pe numele Abonatului pe un alt card emis de asemenea pe numele Abonatului.
- b. Serviciul „Transfer pe cardul propriu” permite efectuarea Transferului în valuta Contului Cardului de pe care se efectuează Transferul sau a Contului Cardului pe care se efectuează Transferul.
- c. Dacă valuta Transferului nu coincide cu valuta Contului Cardului, Banca va converti aceasta la cursul comercial al Băncii stabilit pentru operațiunile cu carduri pentru ziua executării Transferului.

7.3.6. Serviciul „Transfer pe card Moldindconbank”:

- a. Serviciul „Transfer pe card Moldindconbank” permite efectuarea Transferului de pe Cardul emis pe numele Abonatului pe un alt card emis de Bancă pe numele altei persoane decât Abonatul.
- b. Serviciul „Transfer pe cardul Moldindconbank” permite efectuarea Transferului doar în lei moldovenești (MDL).

8. Serviciile non-financiare ale Sistemului

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

8.2. Serviciile informaționale:

8.2.1. oferă Abonatului informații despre conturile și cardurile sale, tranzacțiile efectuate etc.

8.2.2. Serviciile informaționale pot fi prezentate ca servicii separate (cum este obținerea extrasului din cont), cât și integrate în interfața Sistemului, inclusiv în alte Servicii (ca de exemplu afișarea Sumei disponibile pe Contul Cardului pe care se efectuează un transfer sau plată).

8.2.3. Istoria tranzacțiilor. Plăți și transferuri:

a. Afișează lista tranzacțiilor efectuate prin intermediul Sistemului.

8.2.4. Istoria tranzacțiilor. Extras de pe card:

a. Afișează lista tranzacțiilor efectuate cu utilizarea Cardului selectat, în Sistem și în afara acestuia.

8.3. Serviciile de gestionare a cardurilor / conturilor Abonatului:

8.3.1. Blocarea cardului:

a. Utilizarea acestui Serviciului 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 funcție de tipul blocării solicitat, cardul poate sau nu fi deblocat prin utilizarea Serviciului „Deblocarea cardului”. Clientul este informat despre aceasta prin interfața Sistemului.

8.3.2. Deblocarea cardului:

a. Utilizarea acestui Serviciului duce la deblocarea Cardului blocat anterior prin Serviciul „Blocarea cardului”. Deblocarea Cardurilor blocate prin alte modalități, 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.

8.3.3. Fereastra tranzacțională:

a. Utilizarea acestui Serviciu duce la blocarea operațiunilor efectuate cu Cardul.

b. În rezultatul utilizării acestui Serviciu clientul transmite Băncii Document electronic cu statut de cerere de blocare a operațiunilor Cardului.

c. În setările serviciului, Clientul poate autoriza pentru o perioadă de timp efectuarea unui anumit număr de operațiuni având o sumă maximă efectuate cu Cardul.

8.4. Serviciul de generare a parolelor de tip „Mobile OTP”:

8.4.1. Generarea parolei de tip „Mobile OTP” se efectuează prin intermediul meniului „Generarea parolei de unică folosință” din interiorul Aplicației.

8.4.2. Ca bază pentru generarea parolei va fi utilizat codul tranzacției afișat în sistemul „MICB Web Banking”.

8.4.3. În rezultatul generării acestui tip de parolă, clientul transmite Băncii Document electronic cu statut de creare a parolei de unică folosință „Mobile OTP”.

8.4.4. Parola este activă 15 minute și poate fi utilizată doar o singură dată.

8.5. Serviciile de gestionare a Abonamentului și a Factorilor de autentificare:

8.5.1. Modificarea parolei:

a. Utilizarea acestui Serviciului duce la modificarea Parolei.

b. Clientul introduce în câmpurile respective ale interfeței Sistemului Parola nouă care dorește să-i fie alocată de către Bancă. Banca îi alocă Parola cu condiția că aceasta corespunde cerințelor stabilite în prezentele Condiții de utilizare (caracterele utilizate, lungimea etc.).

9. Drepturile și obligațiile Părților

9.1. Părțile își asumă drepturile și obligațiile menționate expres în capitolul curent, în alte capitole ale prezentelor Condiții de utilizare, cererile depuse de către Client și alte documente transmise de către o Parte celeilalte Părți în legătură cu obiectul prezentelor Condiții de utilizare.

9.2. Banca este obligată:

9.2.1. să execute Tranzacțiile în conformitate cu regimul de prestare a Serviciului respectiv definit în prezentele Condiții de utilizare;

- 9.2.2. să ia toate măsurile necesare pentru prevenirea riscurilor ce pot apărea în urma utilizării frauduloase a Sistemului și să asigure măsurile aplicate în vederea identificării Abonatului și asigurării confidențialității, autenticității și non-repudierii tranzacțiilor electronice;
 - 9.2.3. să asigure un grad adecvat de securitate și siguranță operațională a localului, echipamentului de comunicații și procesare, precum și a soluției soft prin intermediul căreia se inițiază, înregistrează, controlează și recepționează Tranzacțiile electronice;
 - 9.2.4. să asigure confidențialitatea datelor referitoare la Abonat precum și a Tranzacțiilor efectuate de acesta prin intermediul Sistemului, în conformitate cu prevederile legislației în vigoare aferente secretului comercial;
 - 9.2.5. să asigure Abonatul cu posibilitatea de a anunța situațiile de urgență și să ia toate măsurile necesare pentru a stopa imediat executarea tranzacțiilor frauduloase prin intermediul Sistemului din momentul în care a fost înștiințată, asigurând Abonatul cu mijloace care să poată dovedi că comunicarea a fost efectuată (data, ora înregistrării și numărul de înregistrare a comunicării);
 - 9.2.6. să asigure identificarea și înscrierea corectă a Abonatului în Sistem, în baza actului de identitate al acestuia și în baza altor documente și măsuri care permit identificarea Abonatului în conformitate cu actele normative în vigoare și riscurile potențiale;
 - 9.2.7. să instruiască Abonatul privind comportamentului optim în caz de fraudă sau suspectare de fraudă asupra sistemului de deservire bancară la distanță și, după caz, privind colaborarea cu autoritățile abilitate pentru limitarea riscurilor de fraudă;
 - 9.2.8. să asigure stocarea și păstrarea informațiilor referitoare la Tranzacțiile electronice efectuate prin intermediul Sistemului pentru perioadele de timp prevăzute de actele normative în vigoare, precum și să monitorizeze corespunderea Tranzacțiilor electronice efectuate prin intermediul Sistemului condițiilor contractuale și normelor în vigoare;
 - 9.2.9. să furnizeze periodic Abonatului sau la cererea expresă a acestuia informații referitoare la Tranzacțiile efectuate prin intermediul Sistemului sau informații privind situația contului bancar al Abonatului. Aceste informații vor fi prezentate în conformitate cu prevederile contractuale existente dintre Bancă și Abonat, cu respectarea prevederilor legislației în vigoare;
 - 9.2.10. să crediteze contul bancar al Abonatului cu valoarea despăgubirilor din momentul recunoașterii dreptului Abonatului la acestea sau de la stabilirea acestui drept de către o instanță de judecată ori de arbitraj.
- 9.3. Clientul este obligat:
- 9.3.1. să ia cunoștință de prezentele Condiții de utilizare, Regulile de utilizare a cardului și Instrucțiuni înainte abonării la Sistem și să utilizeze Sistemul în strictă conformitate cu prevederile acestora;
 - 9.3.2. să acceseze Sistemul numai cu ajutorul Calculatorului/ Telefonului mobil/ dispozitivului mobil care corespunde cerințelor indicate în Instrucțiuni;
 - 9.3.3. să asigure confidențialitatea elementelor de autentificare (Login, Parolă, SMS OTP, ATM OTP și codul de acces), să ia măsuri rezonabile de protejare a acestora contra compromiterii și să nu admită utilizarea acestora de către terțe persoane;
 - 9.3.4. să verifice corectitudinea documentelor electronice pregătite pentru a fi transmise spre executare, cât și celor deja executate de către Bancă;
 - 9.3.5. să înștiințeze Banca (prin intermediul serviciilor suport sau la ghișeele Băncii) imediat ce constată:
 - a. modificarea neautorizată a soldului contului bancar;
 - b. orice eroare sau neregulă apărute în urma gestionării de către Bancă a contului bancar;
 - c. elementele ce creează suspiciuni cu privire la posibilitatea cunoașterii de către persoane neautorizate a factorilor de autentificare deținute de Abonat;
 - d. disfuncționalități ale Sistemului sau dacă parolele de acces primite sunt incorecte;
 - 9.3.6. să manifeste o atitudine responsabilă privind asigurarea siguranței și securității Sistemului.
- 9.4. Banca are dreptul:
- 9.4.1. să perceapă taxele și comisioanele conform Tarifelor;
 - 9.4.2. să nu primească spre executare prin intermediul Sistemului Documentele electronice dacă primirea acestora nu este prevăzută în prezentele Condiții de utilizare și Instrucțiuni, chiar și în cazul în care Banca primește / este obligată să primească asemenea documente prin alte căi (pe suport hârtie, prin telefon).
- 9.5. Banca nu poartă răspundere pentru daunele suportate de client de pe urma nerespectării recomandărilor de utilizare securizată a sistemului „Mobile Banking”.

10. Responsabilitatea Părților și ordinea repartizării pierderilor

10.1. Clientul este responsabil de veridicitatea și corectitudinea informației transmise prin intermediul Sistemului, pentru Tranzacțiile efectuate și 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 Loginul Clientului și Factorii de autentificare deținute de Client, inclusiv cele efectuate fraudulos de către persoanele terțe, până la suspendarea

Loginului sau Factorilor de Autentificare (Parolei, Parolei ATM OTP, Factorului SMS OTP, Codul de acces) cu utilizarea cărora a fost autentificată Tranzacția respectivă.

10.2. Clientul este responsabil de neadmiterea compromiterii Factorilor de autentificare deținută.

10.3. Banca și Clientul recunosc puterea juridică a Tranzacțiilor efectuate în cadrul Sesiunii de utilizare a Sistemului.

10.4. Banca și Clientul recunosc că Documentele electronice transmise de către client Băncii sunt echivalente celor depuse personal de către Deținător și semnate cu semnătura olografă a acestuia.

10.5. Banca și Clientul recunosc faptul că Documentele electronice transmise în adresa Băncii în cadrul Sesiunii de utilizare a Sistemului se echivalează cu cele perfectate de Client pe suport hârtie și produc aceleași drepturi și obligațiuni ale Părților.

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

- 10.6.1. pentru neexecutarea sau executarea necorespunzătoare a Tranzacțiilor efectuate prin intermediul Sistemului:
 - a. în cazul în care executarea necorespunzătoare este atribuită unei disfuncționalități a Sistemului sau a unei componente a acestuia, cu condiția că disfuncționalitatea nu a fost cauzată intenționat de către Abonat;
 - b. chiar dacă Tranzacțiile au fost inițiate prin utilizarea mijloacelor care nu se află sub controlul Băncii, cu condiția să se facă dovada că Tranzacțiile a fost inițiate în conformitate cu prevederile prezentelor Condiții de utilizare.
- 10.6.2. pentru Tranzacțiile electronice inițiate după momentul notificării Băncii de către Abonat a pierderii controlului asupra Sistemului (de exemplu funcționării defectuoase a Sistemului, compromiterea parolelor sau a altor informații sensibile de către persoane neautorizate etc.);
- 10.6.3. pentru pierderile suportate de către Abonat ca rezultat al unei fraude comise de către o persoană sau grup de persoane terțe prin exploatarea unei vulnerabilități a Sistemului, cu condiția că Abonatul a respectat toate prevederile contractuale de utilizare a Sistemului.

11. Serviciul suport

11.1. Banca oferă suport telefonic Abonaților prin intermediul Serviciului suport al Băncii.

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

11.3. Abonatul poate apela Serviciul suport în vederea:

- 11.3.1. comunicării situațiilor de urgență;
- 11.3.2. solicitării suspendării / reactivării Loginului, suspendării Parolei, Parolei ATM OTP și/sau Factorului SMS OTP;
- 11.3.3. obținerii consultațiilor privind utilizarea Sistemului.

12. Dispoziții finale

12.1. Relațiile dintre Bancă și Abonat care apar în rezultatul utilizării Sistemului și care nu sunt specificate în prezentele Condiții de utilizare, vor fi reglementate în conformitate cu Regulile de utilizare a cardului și legislația în vigoare a Republicii Moldova.

12.2. Toate neînțelegerile și/sau litigiile apărute între Abonat și Bancă pe marginea utilizării Sistemului 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.

12.3. Banca va informa Abonații privind modificarea prezentelor Condiții de utilizare și/sau Tarifelor prin afișarea versiunii(lor) modificate a(ale) acestor documente pe pagina Web a Băncii (www.micb.md).