

**Intră în vigoare la 21.01.2019**

Aprobat de Comitetul de conducere al Băncii  
PV nr. 02 din 09.01.2019

# **Condiții de utilizare a Sistemului „MICB Mobile Banking”**

## Cuprins:

1. Dispoziții generale .....	3
2. Instalarea aplicației .....	5
3. Abonarea și autentificarea la Sistem .....	6
4. Autentificarea în Sistem prin amprenta digitală .....	7
5. Restabilirea Login-lui și/sau Parolei .....	8
6. Securitatea Sistemului .....	8
7. Serviciile financiare ale Sistemului „MICB Mobile Banking” .....	11
8. Serviciile non-financiare ale Sistemului „MICB Mobile Banking” .....	13
9. Drepturile și obligațiile Părților .....	15
10. Responsabilitatea Părților și ordinea repartizării pierderilor .....	16
11. Serviciul suport carduri 24/24 .....	17
12. Dispozițiile finale .....	17

## 1. Dispoziții generale

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

1.2. Prezentele Condiții de utilizare completează și detaliază relația contractuală existentă între Deținătorul de card și Bancă, în conformitate cu [Regulile de funcționare a contului de card și utilizare a cardului atașat](#) accesibile pe pagina web.

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.

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

1.5. Pentru informații suplimentare despre Sistemul „MICB Mobile Banking”, Deținătorul de card poate apela Serviciul suport carduri 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.

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

- **MICB Mobile Banking, Aplicație** – aplicația mobilă care oferă acces rapid și 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” și “Google Play”.
- **Sistem de deservire bancară la distanță** (în continuare Sistem) – soluție informatică, pusă la dispoziție de către Bancă clienților săi, ce permite deținătorului să aibă acces la distanță la mijloacele aflate în contul său bancar, 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, detaliază modul în care Clienții Băncii pot accesa și ulterior utiliza Sistemul „MICB Mobile Banking”.
- **Tarife** – [Tarifele și limitele referitoare la deservirea cardurilor bancare emise de BC „Moldindconbank” S.A](#) în vigoare – lista taxelor, comisioanelor și a limitelor aplicate de către Bancă la administrarea Cardurilor, plasate pe panourile informative ale subdiviziunilor Băncii, precum și pe pagina web.
- **Card** – card de plată emis de Bancă 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 numele Utilizatorului autorizat.
- **Deținător de card, Deținător** - Persoana fizică pe numele căreia este emis Cardul în conformitate cu Cererea de emitere a Cardului. Cuprinde termenii „Deținătorul principal” și „Utilizatorul autorizat”.
- **Deținător principal** - Deținătorul, posesor al Contului de card deschis în conformitate cu Cererea.
- **Utilizator autorizat** – Deținător de card, altul decât Deținătorul principal: persoana fizică pe numele căreia este emis Cardul în conformitate cu Cererea, și este nominalizată de către Deținătorul principal ca Utilizator autorizat al Contului de card.
- **Cont de card** - Contul deschis și menținut de către Deținătorul principal în cadrul Băncii, cu scopul înscrierii tranzacțiilor cu carduri, precum și a altor operațiuni prevăzute de Regulile de funcționare a contului de card și utilizare a cardului atașat, Tarifele și Cererea.
- **Bancă** – BC „Moldindconbank” S.A.
- **Client** – Deținătorul Cardului care efectuează autentificarea în sistem. Client eligibil pentru utilizarea amprentei digitale pentru autentificarea la Sistem este orice persoană fizică care deține 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 Condițiile de utilizare a Serviciului “Cash by Code”.
- **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** – 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 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.
- **Instrucțiunea** – Instrucțiunea 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. Instrucțiunea este 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 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 și 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 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 obținerea din partea Băncii a unei informații.
- **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.

## Condiții de utilizare a Sistemului „MICB Mobile Banking”

- **Număr de telefon OTP** – numărul de telefon mobil indicat de către Client în Chestionarul clientului – persoană fizică sau prin intermediul bancomatelor Băncii cu condiția 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.) 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”.
- **Autentificare suplimentară prin aplicarea Codului de acces** - tipul Autentificării suplimentare care prevede setarea Codului de acces și 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 deținut.
- **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 obținută 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 bănești de pe card pe card prin intermediul Portalului [www.transfer.md](http://www.transfer.md), bancomatelor gestionate de către Bancă, sistemelor „MICB Web Banking” și „MICB Mobile Banking” (accesibile *Deținătorilor de carduri MICB*), precum și de a alimenta cu numerar cardul în bancomatele Băncii de tip „CASH-IN”.
- **Serviciul „Cash by Code”, Serviciu** – 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 Deținătorului de card. Acest cod poate fi utilizat pentru retragerea numerarului de către Beneficiar, din inițiativa și cu participarea nemijlocită a Deținătorului, cu condiția respectării Condițiilor de utilizare a serviciului „Cash by Code”.
- **Serviciul “Cash-In by Code”** – serviciu destinat persoanelor fizice Deținătoare 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 și cu participarea nemijlocită a Deținătorului, cu condiția respectării Condițiilor de utilizare a serviciului „Cash by Code”.
- **Serviciul „SMS-notificări”** - serviciu de informare a clienților prin intermediul mesajelor SMS expediate la telefonul mobil cu privire la tranzacțiile efectuate cu cardul bancar și 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.) și Unite („Moldtelecom” S.A.).

## 2. Instalarea aplicației

- 2.1. 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”.
- 2.2. Instalarea Aplicației pentru telefoanele mobile/ dispozitivele mobile care rulează pe sistemul de operare Android va fi efectuată de Client, din magazinul virtual oficial „Google Play”.

2.3. Aplicația poate fi utilizată concomitent pentru mai multe telefoane / dispozitive mobile care rulează prin sistemele de operare menționate în pct.2.1 și 2.2.

### 3. Abonarea și autentificarea la Sistem

3.1. 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 obținerea de către Client a Login-ului și Parolei.

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

3.2.1. **Obținerea Login-ului și Parolei prin operațiunea respectivă accesibilă la bancomatul Băncii:**

- a) Clientul autentifică operațiunea de primire a Login-ului și Parolei prin introducerea unui Card valabil emis pe numele său și a Codului PIN în elementele de interacțiune ale bancomatului;
- b) În rezultatul operațiunii de primire a Login-ului 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 Login-ului și Parolei în cazul nepreluării din imprimanta bancomatului a bonului cu Login și Parolă imprimate.

3.2.2. **Abonarea prin introducerea numărului Cardului și 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 operațiunea de primire a Login-ului și Parolei prin introducerea numărului unui Card valabil emis pe numele său și efectuarea Autentificării alternative de tip „SMS OTP” sau „ATM OTP”;
- c) În cadrul operațiunii Clientul introduce în câmpurile respective ale interfeței Sistemului, Login-ul și Parola care dorește să-i fie alocată de către Bancă. Banca îi alocă Login-ul și Parola cu condiția că acestea corespund cerințelor stabilite în prezentele Condiții de utilizare (caracterele utilizate, lungimea etc.) și, totodată, dacă Login-ul nu este deja utilizat pentru identificarea unui alt Abonat.

3.3. **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 folosință;
  - generarea parolelor de unică folosință, pentru confirmarea operațiunilor în Web-Banking, E-Commerce;
  - utilizare celui mai inovativ și securizat mod de autentificare (recomandat).
- b) **Cu numele de utilizator și 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 și 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 și parola de pe chitanța 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 folosință (ATM OTP) ce au fost imprimate pe chitanță 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”.



## Condiții de utilizare a Sistemului „MICB Mobile Banking”

- 3.4. Clientul, prin Abonare la Sistem, confirmă faptul că a luat cunoștință de prezentele Condiții de utilizare și le acceptă.
- 3.5. Clientul nu are dreptul să utilizeze în procesul abonării cardul sau rechizitele unui alt card decât cel emis pe numele său.
- 3.6. Abonarea poate să fie efectuată doar personal de către Client și nu poate fi efectuată de către, reprezentantul acestuia sau orice altă persoană terță.
- 3.7. Clienții abonați anterior la sistemul “MICB Web Banking” implicit au acces și la sistemul „MICB Mobile Banking”, cu utilizarea Login-lui și Parolei identice.

#### 4. Autentificarea în Sistem prin amprenta digitală

- 4.1. 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
- 4.2. 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.
- 4.3. 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 pct. 3.3.a – 3.3.f.
- 4.4. 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.
- 4.5. Utilizarea amprentei digitale poate fi efectuată concomitent de pe mai multe telefoane / dispozitive mobile “touch id / FingerPrint”.
- 4.6. 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;
- 4.7. Abonatul, prin autentificarea în Sistem cu utilizarea amprentei digitale confirmă faptul că a luat cunoștință și este de acord cu prevederile prezentelor Condiții și în legătură cu aceasta declară că:
  - a. Înțelege și acceptă faptul că orice amprentă digitală salvată în “touch id / FingerPrint” poate fi utilizată 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 terțe;
  - 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;
- 4.8. 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.
- 4.9. Abonatul poate în orice moment dezactiva funcționalitatea de utilizare a amprentei digitale.
- 4.10. Banca nu garantează că funcționalitatea “touch id / FingerPrint” va fi accesibilă de pe orice dispozitiv, precum și nu poate garanta continuitatea accesibilității funcționalității respective.
- 4.11. Banca nu este responsabilă pentru nici o pierdere suportată de Abonat în legătură cu utilizarea sau încercarea de utilizare a funcționalității “touch id” în cazul unor tranzacții neautorizate, orice acces neautorizat la dispozitivul “touch id / FingerPrint”.

## 5. Restabilirea Login-ului și/sau Parolei

5.1. Restabilirea Login-ului și/sau Parolei poate fi efectuată prin următoarele modalități:

5.1.1. **Obținerea Login-ului și Parolei prin operațiunea respectivă accesibilă la bancomatul Băncii:**

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

5.1.2. **Obținerea Login-ului și modificarea Parolei prin introducerea numărului Cardului și Autentificării alternative de tip „SMS OTP” sau „ATM OTP”:**

- a) Clientul efectuează această operațiune prin intermediul Sistemului;
- b) Clientul autentifică operațiunea de primire a Login-ului și Parolei prin introducerea numărului unui Card valabil emis pe numele său și efectuarea Autentificării alternative de tip „SMS OTP” sau „ATM OTP”.
- c) În cadrul operațiunii, Clientului îi este afișat în interfața Sistemului Login-ul 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 are ca scop:

- 6.1.1. securitatea Cardurilor, Conturilor Clientului și a mijloacelor din ele, altor produse și servicii deținute de Client în Bancă, precum și confidențialitatea informației despre acestea;
- 6.1.2. asigurarea faptului că Tranzacțiile pot fi efectuate din numele Abonatului doar de către Abonat și nu în mod fraudulos de către o altă persoană.

6.2. Securitatea Sistemului este asigurată prin următoarele cerințe de autentificare:

- 6.2.1. o persoană poate să se Aboneze la Sistem în calitate de Client sau să obțină acces la Login-ul și Parolă doar în baza autentificării prin Card și Cod PIN la bancomat sau în baza numărului Cardului și Autentificării alternative în Sistem;
- 6.2.2. o persoană poate să obțină accesul la Sistem în calitate de Abonat doar în baza procedurii Autentificării în Sistem;
- 6.2.3. în cadrul Sesiunii de utilizare a Sistemului, unele Servicii sunt accesibile doar în baza Autentificării suplimentare.

6.3. 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:

- 6.3.1. Necompromiterea Cardului, datelor cardului și a PIN-ului. Cerințele de securizare ale acestora sunt descrise în [Regulile de funcționare a contului de card și utilizare a cardului atașat](#).
- 6.3.2. Necompromiterea Parolei. Compromiterea Parolei este situația în care Clientul nu este ferm convins asupra faptului că aceasta nu este accesibilă persoanelor terțe.
- 6.3.3. Necompromiterea parolelor de unică folosință primite din ATM (ATM OTP). Compromiterea ATM OTP este situația în care Clientul nu este ferm convins asupra faptului că acestea nu sunt accesibile persoanelor terțe.
- 6.3.4. Necompromiterea Factorului de autentificare „SMS OTP”. Compromiterea acestui Factor este situația în care Clientul nu este ferm convins asupra faptului că mesajele transmise pe numărul de telefon OTP nu sunt accesibile persoanelor terțe.
- 6.3.5. Necompromiterea Codului de acces. Compromiterea acestui Factor este situația în care Clientul nu este ferm convins asupra faptului că Codul de acces nu este accesibil persoanelor terțe.
- 6.3.6. Necompromiterea amprente 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”.

6.4. Clientul este responsabil pentru necompromiterea Factorilor de autentificare deținute de el.



## Condiții de utilizare a Sistemului „MICB Mobile Banking”

**6.5. Cu scopul prevenirii compromiterii Parolei, Clientul trebuie:**

- 6.5.1. să nu înscrie Parola pe un suport care permite asocierea cu Sistemul, prin natura sau poziționarea sa;
- 6.5.2. să modifice regulat Parola cu ajutorul Serviciului respectiv al Sistemului;
- 6.5.3. să asigure protejarea Calculatorului /Telefonului mobil/ dispozitivului mobil al său utilizând softul specializat (antivirus, firewall etc.), politicile de limitare a accesului la resurse și alte metode de securitate informațională;
- 6.5.4. să limiteze accesul persoanelor terțe la dispozitivul / dispozitivele “touch id / FingerPrint”.

**6.6. În cazul în care Parola este compromisă, Clientul trebuie să modifice imediat Parola prin una din următoarele modalități:**

- 6.6.1. Serviciul respectiv în cadrul Sesiunii de utilizare a Sistemului;
- 6.6.2. Operațiunea de modificare a Parolei prin introducerea numărului Cardului și Autentificării alternative de tip „SMS OTP” sau „ATM OTP”;
- 6.6.3. Obținerea Login-ului și Parolei (regenerate) prin operațiunea respectivă accesibilă la bancomatul Băncii;
- 6.6.4. În cazul în care Clientul nu are posibilitate de a efectua acțiunile menționate mai sus, acesta trebuie să contacteze imediat Serviciul suport carduri 24/24 al Băncii pentru a anula Parola.

**6.7. Cerințele față de Parolă în Sistemul MICB Mobile Banking:**

- 6.7.1. 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;
- 6.7.2. Este interzisă utilizarea altor caractere decât litere latine majuscule/minuscule și cifre;
- 6.7.3. Este interzisă stabilirea Parolei care coincide cu una din 12 Parole utilizate anterior de client;
- 6.7.4. Sistemul va suspenda Parola pentru 15 minute după fiecare 3 introduceri greșite consecutive;
- 6.7.5. Sistemul va impune modificarea parolei de către Abonat cel puțin o dată la 90 zile.

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

- 6.8.1. verifice atent Tranzacțiile efectuate din numele său pentru a depista pe cele frauduloase;
- 6.8.2. anunțe imediat Banca la Serviciul suport carduri 24/24 al Băncii la numărul de telefon 022 54 89 40 și să comunice detaliile privind circumstanțele compromiterii și eventualele efecte ale acesteia.

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

- 6.9.1. să genereze o nouă listă de ATM OTP;
- 6.9.2. să contacteze Serviciul suport carduri 24/24 al Băncii pentru a anula lista de parole ATM OTP.

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

- 6.10.1. să solicite operatorului de telefonie mobilă suspendarea numărului de telefon (utilizat în calitate de numărul de telefon OTP);
- 6.10.2. să solicite Băncii, prin contactarea Serviciului suport carduri 24/24 al Băncii, suspendarea numărului de telefon OTP în sistemul informațional al Băncii;
- 6.10.3. să solicite Băncii modificarea numărului de telefon utilizat în calitate de numărul de telefon OTP prin una din următoarele modalități:
  - 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 sucursalele Băncii;
  - b) modificarea numărului de telefon mobil în afara Serviciului „SMS-notificări”, prin depunerea Chestionarului pentru client – persoană fizică la una dintre sucursalele Băncii.

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

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

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

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

**6.13. Suspendarea / reactivarea Login-ului:**

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

- 6.13.2. În cazul suspendării Login-lui Autentificarea în Sistem și restabilirea parolei nu vor fi accesibile;
- 6.13.3. Abonatul poate solicita reactivarea unui Login suspendat apelând personal Serviciul suport carduri 24/24 al Băncii, cu condiția identificării reușite a Abonatului de către operatorul Serviciului suport carduri 24/24 în baza datelor anterior prezentate de către Abonat Băncii în momentul identificării la Bancă;
- 6.13.4. Reactivarea Login-lui nu duce în sine la reactivarea Factorilor de autentificare.
- 6.14.** Banca protejează datele transmise între Serverul Sistemului și Telefon mobil / dispozitiv mobil prin cifrarea acestora.
- 6.15.** Banca recomandă următoarele modalități de utilizare securizată a Sistemului „MICB Mobile Banking”:
- 6.15.1. Să nu divulge informația confidențială altor persoane (PIN, numărul de card, parole, conturi, datele personale);
- 6.15.2. Să nu lase dispozitivul / dispozitivul “touch id / FingerPrint” fără supraveghere în special după procedura de autentificare și să asigure că ecranul dispozitivului nu este vizibil altor persoane;
- 6.15.3. Să seteze parola de acces la dispozitivul mobil și opțiunea de blocare a dispozitivului după o perioadă de inactivitate;
- 6.15.4. Să utilizeze parole și coduri de acces sigure pentru a evita spargerea lor;
- 6.15.5. Să utilizeze diferite parole pentru fiecare serviciu (poșta electronică, conturile de acces la rețelele de socializare, etc.);
- 6.15.6. Să nimicească bonurile cu parolele ATM OTP dacă nu vor fi utilizate;
- 6.15.7. Să descarce aplicațiile mobile numai din magazinele oficiale AppStore și Google Play. Toate alte surse nu sunt oficiale și Banca nu poartă răspundere pentru consecințele instalării aplicațiilor descărcate din aceste surse;
- 6.15.8. Să efectueze regulat actualizarea sistemului de operare, aplicației MICB Mobile Banking și altor aplicații instalate pe dispozitivul mobil, utilizând numai surse oficiale;
- 6.15.9. Pentru a fi siguri că nu descărcă ceva dubios, să dezactiveze în setările telefonului pe platforma Android opțiunea „Surse Necunoscute” în setările de „Securitate”;
- 6.15.10. 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;
- 6.15.11. 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.;
- 6.15.12. Aplicația MICB Mobile Banking va fi utilizată numai de către Abonatul la Sistem;
- 6.15.13. 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;
- 6.15.14. Să activeze opțiunea de control la distanță pentru ștergerea datelor la distanță sau blocare în cazul pierderii dispozitivului;
- 6.15.15. 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;
- 6.15.16. 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, să sune operatorul telefoniei mobile pentru blocarea cartelei SIM;
- 6.15.17. 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 modalității de Autentificare Suplimentară de tip SMS OTP;
- 6.15.18. 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;
- 6.15.19. 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;
- 6.15.20. În cazul nefuncționării cartelei SIM să sune imediat la operatorul telefoniei mobile pentru a se asigura că cauza nu este urmare a acțiunilor frauduloase;

- 6.15.21. Să termine lucrul cu aplicația mobilă prin accesarea butonului Exit (Ieșire);
- 6.15.22. 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.);
- 6.15.23. 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 exista 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 „MICB Mobile Banking”

- 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 privind deservirea cardurilor bancare emise de BC „Moldindconbank” S.A. \(în continuare Tarife\)](#).
- 7.3. **Serviciul „P2P MICB”** - se efectuează în conformitate cu [Condițiile de utilizare a Serviciului „P2P MICB”](#) accesibile la orice Ghișeu al Băncii sau pe pagina web.
  - 7.3.1. **Serviciul „Transfer pe cardul propriu”** – permite efectuarea Transferurilor între cardurile personale.
  - 7.3.2. **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.
  - 7.3.3. **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.
- 7.4. **Serviciul „Cash by Code”** – permite Abonatului de a genera în Sistem un cod numeric cât și cod de bare în baza căruia poate fi retrasă o anumită sumă de bani în numerar direct de la bancomat fără a utiliza un card bancar.
- 7.5. **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. Codul unic este reprezentat în format grafic (cod de bare).
- 7.6. Serviciul „Cash by Code / Cash-In by Code” se prestează în conformitate cu [Condițiile de utilizare a Serviciului „Cash by Code”](#) accesibile la orice Ghișeu al Băncii sau [pe pagina web](#).
- 7.7. **Serviciul „Achitarea creditului”**- permite achitarea datoriilor pentru creditele în MDL proprii deținute la Bancă (cu excepția creditelor acordate la contul de card);
- 7.8. Utilizarea acestui Serviciu duce la perfectarea Documentului electronic prin care Abonatul solicită efectuarea transferului cu scopul achitării creditului. Acest Document are statut de cerere privind transferul mijloacelor bănești în contul curent.
- 7.9. Etapele și modalitatea de prelucrare a transferului:
  - a) **verificarea** Documentului electronic. În acest moment:
    - a.1. se verifică corectitudinea perfectării Documentului, conform cerințelor stabilite de către Bancă;
    - a.2. se verifică posibilitatea efectuării acestui transfer de pe cardul indicat de către Abonat (suma disponibilă, statut, limite etc.).
  - b) **autorizarea** transferului desemnează momentul în care Banca primește spre executare Documentul electronic respectiv. În acest moment:
    - b.1. Banca blochează instantaneu suma transferului pe Contul Cardului de pe care se efectuează transferul;
  - c) **executarea finală** a Documentului electronic. Aceasta prevede următoarele acțiuni:
    - c.1. Banca debitează Contul Cardului de pe care se efectuează transferul ceea ce duce la micșorarea Sumei disponibile pe acesta;
    - c.2. Banca efectuează transferul mijloacelor bănești pe contul curent al Abonatului legat de contractul de credit pentru care se efectuează plata;
    - c.3. Banca acceptă documentul electronic, în zilele lucrătoare, în timpul orelor de lucru 09:00-16:00. Documentul electronic autorizat de către client în zilele de odihnă sau după ora 16:00 va primi statut final în următoarea zi lucrătoare.

c.4. Achitarea datoriei conform contractului de credit din contul curent are loc conform graficului de plată prevăzut în condițiile contractelor de credit.

c.4. Achitarea anticipată a creditului se efectuează prin depunerea unei cereri scrise la sucursala contractării creditului.

**Notă:** Banca efectuează înregistrarea sumei datoriilor aferente creditului, cu condiția asigurării transferului mijloacelor bănești de către client în contul curent, până la ora 16:00 a zilei achitării conform graficului de achitare prevăzut în contractul de credit.

**Notă:** Dacă transferul se va efectua de pe un card în valută, Banca va converti suma tranzacției în valuta MDL la cursul pentru carduri în ziua efectuării operațiunii. Cursul valutar pentru operațiunile de convertire valutară sunt stabilite de către Bancă și este plasat pe site-ul Băncii: <https://www.micb.md/c/>.

#### 7.10. Serviciul „Plăți în baza contractelor de primire a plăților”:

- 7.10.1. Serviciul „Plăți în baza contractelor de primire a plăților” (în continuare în cadrul acestui compartiment „Plăți”) permite Clientului perfectarea plăților în favoarea furnizorilor de servicii și altor beneficiari de plăți 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”).
- 7.10.2. Utilizarea acestui Serviciu duce la perfectarea Documentului electronic prin care Abonatul solicită efectuarea plății în favoarea Furnizorului și totodată informarea Furnizorului privind faptul efectuării plății cu transmiterea în adresa acestuia a datelor care se conțin în acest Document. Acest Document are statut de cerere.
- 7.10.3. Banca stabilește unilateral lista Furnizorilor de servicii și o poate modifica fără preaviz.
- 7.10.4. În calitate de Furnizor de servicii poate servi și Banca, în cazul în care alte servicii ale Băncii sunt achitate prin Serviciul „Plăți în baza contractelor de primire a plăților”. În acest caz, condițiile prestării serviciilor achitate astfel sunt gestionate de relațiile respective ale Clientului cu Banca.
- 7.10.5. Serviciul „Plăți” este destinat cel mai des pentru a perfecta Plăți în adresa furnizorilor conform facturilor primite de la furnizor, însă permite pentru unii furnizori și efectuarea Plăților fără a avea ca bază o factură (de exemplu, alimentarea contului în cazul pachetelor preplătite de telefonie mobilă).
- 7.10.6. Pentru fiecare Furnizor în Sistem este definit:
- a) dacă este prezentă sau nu în Sistem lista facturilor înaintate de către Furnizor și dacă Clientul are posibilitatea de a efectua căutarea acestora;
  - b) câmpurile care trebuie completate în Documentul electronic și/sau care sunt completate automat de Sistem în baza facturii selectate de Client;
  - c) este efectuată sau nu autorizarea fiecărei Plăți de către Furnizorul respectiv;
  - d) este permisă perfectarea Documentului electronic în baza facturii, fără factură sau ambele modalități;
  - e) este solicitată sau nu Autentificarea suplimentară pentru a fi primit spre executare Documentul electronic.
- 7.10.7. Etapele și modalitatea de prelucrare a Plății:
- a) **verificarea** Documentului electronic. În acest moment:
    - 7.10.7.a.1. se verifică corectitudinea completării câmpurilor Documentului, conform cerințelor stabilite de către Bancă;
    - 7.10.7.a.2. dacă este prevăzut de contractul Băncii cu Furnizorul beneficiar, se solicită autorizarea plății de către Furnizorul respectiv;
    - 7.10.7.a.3. se verifică posibilitatea efectuării acestei Plăți de pe cardul indicat de către Abonat (suma disponibilă, statut, limite etc.).
  - b) **autorizarea** Plății (transferului) desemnează momentul în care Banca primește spre executare Documentul electronic respectiv. În acest moment:
    - 7.10.7.b.1. Banca blochează instantaneu suma Plății pe Contul Cardului de pe care se efectuează Plata, ceea ce duce la micșorarea Sumei disponibile pe acesta;
    - 7.10.7.b.2. dacă este prevăzut de contractul Băncii cu Furnizorul beneficiar, Banca informează Furnizorul respectiv cu privire la Plata efectuată și parametrii acesteia.
  - c) **executarea finală** a Documentului electronic. Aceasta prevede următoarele acțiuni:
    - 7.10.7.c.1. Banca debitează Contul Cardului de pe care se efectuează Plata;

## Condiții de utilizare a Sistemului „MICB Mobile Banking”

7.10.7.c.2. Banca efectuează transferul mijloacelor bănești în adresa Furnizorului beneficiar conform prevederilor relațiilor dintre Bancă și acesta;

7.10.7.c.3. Banca anunță Furnizorul privind datele documentului de plată conform prevederilor agreeate dintre Bancă și acesta.

## 7.10.8. Responsabilitatea Băncii:

a) Banca este responsabilă de executarea corectă și la timp a prevederilor pct. 7.10.7.c.2 și 7.10.7.c.3, totodată termenele concrete de executare a acestor acțiuni depind de prevederile contractului încheiat între Furnizor și Bancă.

b) Banca nu este responsabilă de reacția și timpul reacției Furnizorului la executarea de către Bancă a prevederilor pp. 7.10.7.c.2 și 7.10.7.c.3, precum și nu este responsabilă de calitatea mărfurilor și serviciilor oferite Clientului de către Furnizor.

7.10.9. În cazul în care Clientul are litigii cu Furnizorul și are nevoie de confirmarea executării Documentului electronic de plată autentificată de către Bancă – document ce atestă efectuarea Plății 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 Plățile care nu au fost efectuate în baza facturii, să comunice salariatului Băncii datele câmpurilor care au fost completate în documentul de plată (numărul telefonului, numărul contractului cu furnizorul etc.);

b) să prezinte actul de identitate;

c) să comunice operatorului data achitării facturii.

*Notă: Fără cunoașterea acestor date salariatul Băncii nu va avea posibilitate să verifice faptul efectuării Plății. Clientul poate vizualiza toate aceste date în Sistem, în Istoria tranzacțiilor.*

7.10.10. Clientul poate vizualiza în Sistem lista documentelor de plată transmise spre executare.

## 8. Serviciile non-financiare ale Sistemului „MICB Mobile Banking”

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;

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;

#### 8.2.4. Istoria tranzacțiilor. Extras de pe card:

a) Afișează lista tranzacțiilor efectuate cu utilizarea Cardului selectat, în Sistem și 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;

#### 8.2.5. Datele bancare ale contului:

- Sistemul oferă posibilitatea vizualizării datelor bancare ale contului de card pentru transferuri interbancare.

- Sistemul oferă posibilitatea de a transmite datele bancare ale contului către o adresă de email.

### 8.3. Serviciile de gestionare a cardurilor / conturilor Abonatului:

#### 8.3.1. 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 funcție de tipul blocării solicitat (card pierdut, furat sau altă cauză), 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 Serviciu 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. Activarea serviciului „Protecția cardului” (Fereastra tranzacțională):

- a) Utilizarea acestui Serviciu permite Abonatului să dețină securitate avansată asupra cardurilor sale;
- b) La activarea serviciului „Protecția cardului” (Fereastra tranzacțională) 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.

#### 8.3.4. Dezactivarea serviciului „Protecția cardului”(Fereastra tranzacțională):

- a) La dezactivarea serviciului „Protecția cardului” (Fereastra tranzacțională) cardul va fi deblocat.
  - Operațiunea de dezactivare a serviciului „Protecția cardului” (Fereastra tranzacțională) 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 „Protecția cardului” nu necesită autentificare adițională.

#### 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 Sistemului „MICB Mobile Banking”;
- 8.4.2. Generarea parolei de tip „Mobile OTP” este posibilă doar în cazul accesării Sistemului „MICB Mobile Banking” prin Codul de acces (5 cifre);
- 8.4.3. Ca bază pentru generarea parolei de tip „Mobile OTP” va fi utilizat codul tranzacției afișat în sistemul „MICB Web Banking” sau în E-Commerce (3D Secure);
- 8.4.4. În rezultatul generării acestui tip de parolă, Clientul transmite Băncii Document electronic cu statut de creare a parolei de unică folosință „Mobile OTP”;
- 8.4.5. 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 Serviciu duce la modificarea Parolei;
- b) Clientul introduce în câmpurile respective ale interfeței Sistemului Parola nouă care dorește să-i fie alocată în Sistem. Sistemul îi alocă Parola cu condiția că aceasta corespunde cerințelor stabilite în prezentele Condiții de utilizare (caracterele utilizate, lungimea etc.).

#### 8.6. 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](#));

#### 8.7. 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.

#### 8.8. 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 obținerea statutului de Abonat, posibilitatea de a beneficia de funcționalitatea Serviciului „SMS-notificări”.
- c) Serviciul se utilizează în conformitate cu [Condițiile de prestare a Serviciului „SMS-Notificări” și a altor mesaje de notificare.](#)

#### 8.9. Serviciul „Localizarea geografică”:

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

## 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 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;
- 9.2.8. 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;
- 9.2.9. 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;
- 9.2.10. 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”.
- 9.2.11. să asigure în caz de lipsă de activitate în sistemul “MICB Mobile Banking”, în decurs de 10 minute finisarea sesiunii sistemului.

9.3. Clientul este obligat:

- 9.3.1. să ia cunoștință de prezentele Condiții de utilizare, Regulile de funcționare a contului de card și utilizare a cardului atașat, Instrucțiunii de utilizare a Sistemului “MICB Mobile Banking” înainte abonării la Sistem și să utilizeze Sistemul în strictă conformitate cu prevederile acestora;

## Condiții de utilizare a Sistemului „MICB Mobile Banking”

- 9.3.2. să acceseze Sistemul numai cu ajutorul Telefonului mobil/ dispozitivului mobil care corespunde cerințelor indicate în Instrucțiune;
- 9.3.3. 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”;
- 9.3.4. să asigure confidențialitatea elementelor de autentificare (Login, Parolă, SMS OTP, ATM OTP și Codul de acces, amprentă digitală), să ia măsuri rezonabile de protejare a acestora contra compromiterii și să nu admită utilizarea acestora de către terțe persoane;
- 9.3.5. să asigure acțiunea de **Log out / Ieșire / Выход** după fiecare sesiune de utilizare a sistemului “MICB Mobile Banking”;
- 9.3.6. să verifice corectitudinea documentelor electronice pregătite pentru a fi transmise spre executare, cât și a documentelor deja executate de către Bancă;
- 9.3.7. să înștiințeze Banca (prin intermediul Serviciului suport carduri bancare 24/24 sau la ghișeele Băncii) imediat ce constată:
- modificarea neautorizată a soldului contului bancar;
  - orice eroare sau neregulă apărută în urma gestionării de către Bancă a contului bancar;
  - elementele ce creează suspiciuni cu privire la posibilitatea cunoașterii de către persoane neautorizate a factorilor de autentificare deținute de Abonat;
  - disfuncționalități ale Sistemului sau dacă parolele primite sunt incorecte;
- 9.3.8. să manifeste o atitudine responsabilă privind asigurarea siguranței și securității Sistemului.
- 9.4. Banca are dreptul:**
- 9.4.1. să perceapă taxe și comisioane conform [Tarifelor și Limitelor referitor la deservirea cardurilor bancare emise de BC „Moldindconbank” S.A.](#);
- 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 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.
- 9.6. 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.**

## 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 Login-ul Clientului și Factorii de autentificare deținute de Client, inclusiv cele efectuate fraudulos de către persoanele terțe, până la suspendarea Login-ului sau Factorilor de Autentificare (Parolei, Parolei ATM OTP, Parolei SMS OTP, Codului de acces, amprentei digitale) cu utilizarea cărora a fost autentificată Tranzacția respectivă.
- 10.2.** Clientul este responsabil de neadmiterea compromiterii Factorilor de autentificare deținuți.
- 10.3.** Banca și Clientul recunosc puterea juridică a Tranzacțiilor efectuate în cadrul Sesiunii de utilizare a Sistemului „MICB Mobile Banking”.
- 10.4.** Banca și Clientul recunosc că Documentele electronice transmise de către client Băncii sunt echivalente celor depuse personal de către Client 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 „MICB Mobile Banking” 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 „MICB Mobile Banking”. Banca este responsabilă:
- 10.6.1. pentru neexecutarea sau executarea necorespunzătoare a Tranzacțiilor efectuate prin intermediul Sistemului:

**Condiții de utilizare a Sistemului „MICB Mobile Banking”**

- 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 carduri 24/24

- 11.1. Banca oferă suport telefonic Abonaților prin intermediul Serviciului suport carduri 24/24 al Băncii.
- 11.2. Serviciul suport carduri 24/24 este accesibil non-stop (24 din 24 ore, 7 zile pe săptămână) la linia telefonică la numărul de telefon: /+373/ 22 **54-89-40**.
- 11.3. Abonatul poate apela Serviciul suport carduri 24/24 în vederea:
- 11.3.1. comunicării situațiilor de urgență;
  - 11.3.2. solicitării suspendării / reactivării Login-lui, suspendării Parolei, Parolei ATM OTP și/sau Parolei SMS OTP;
  - 11.3.3. obținerii consultațiilor privind utilizarea Sistemului „MICB Mobile Banking”.

## 12. Dispozițiile finale

- 12.1. Relațiile dintre Bancă și Abonat care apar în rezultatul utilizării Sistemului „MICB Mobile Banking” și care nu sunt specificate în prezentele Condiții de utilizare, vor fi reglementate în conformitate cu Regulile de funcționare a contului de card și utilizare a cardului atașat și legislația în vigoare a Republicii Moldova.
- 12.2. Toate neînțelegerile și/sau litigiile apărute între Abonat și Bancă pe marginea utilizării Sistemului „MICB Mobile Banking” 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](http://www.micb.md)).