

APROBAT

de Comitetul de conducere al Băncii
Proces-verbal nr.33 din 19.05.2026
În vigoare din 25.05.2026

Condiții de utilizare a instrumentului de plată electronic cu acces la distanță MICB Mobile Banking

Cuprins:

1. Dispoziții generale.....	3
2. Instalarea aplicației	5
3. Abonarea și autentificarea la IPAD MICB Mobile Banking.....	6
4. Autentificarea în IPAD MB prin amprenta digitală	6
5. Restabilirea Login-lui și/sau Parolei	7
6. Securitatea IPAD MICB Mobile Banking	7
7. Serviciile financiare ale IPAD MICB Mobile Banking.....	10
8. Serviciile non-financiare ale IPAD MICB Mobile Banking	18
9. Drepturile și obligațiile Părților	22
10. Responsabilitatea Părților și ordinea repartizării pierderilor	24
11. Serviciul suport carduri 24/24	24
12. Dispozițiile finale	25

1. Dispoziții generale

1.1. Prezentele Condiții de utilizare a instrumentului de plată electronic cu acces la distanță MICB Mobile Banking (în continuare Condiții de utilizare), stabilite de BC „Moldindconbank” S.A., descriu modul în care Banca oferă Clienților săi posibilitatea utilizării IPAD MICB Mobile Banking (în continuare IPAD MB), 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 [Condițiile Generale Bancare pentru persoane fizice](#) accesibile pe pagina web a Băncii.

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

1.4. Pentru informații suplimentare despre IPAD MICB Mobile Banking, Deținătorul de card poate apela Serviciul suport carduri 24/24 la numărul de telefon **/+373/ 22 71-71-71**.

1.5. 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:

- **Abonament** – totalitatea relațiilor reglementate dintre Abonat și Bancă aferente IPAD-ului, precum și înregistrarea parametrilor și statutului acestei relații.
- **Abonare la IPAD MB** – 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.
- **Abonat și/sau Utilizator**– Clientul care este abonat la IPAD MB.
- **Actualizare date** – serviciul integrat în IPAD MICB Mobile Banking prin care clienții existenți persoane fizice rezidente, confirmă informațiile personale declarate și stocate în sistemul informațional al băncii ca fiind actuale, conform prevederilor legale privind prevenirea și combaterea spălării banilor și finanțării terorismului, necesare pentru continuarea relațiilor de afaceri cu banca.
- **Alias** – este un identificator unic care permite utilizatorului serviciilor de plată să îl prezinte în locul datelor de identificare detaliate necesare pentru completarea unui ordin de plată (numărul de telefon al beneficiarului plății, înrolat în sistemul de plăți instant sau/și codul IDNP).
- **Aplicație Apple Pay** - o platformă de plată oferită de Apple Distribution International, prin intermediul căreia utilizatorul poate atașa cardurile eligibile pentru a efectua plăți la comercianți, plăți prin internet, retrage numerar la ATM-urile contactless prin intermediul dispozitivelor Apple.
- **Aplicație Google Pay** - o platformă de plată oferită de Google Ireland Limited, prin intermediul căreia utilizatorul poate atașa cardurile eligibile pentru a efectua plăți la comercianți, plăți prin internet, retrage numerar la ATM-urile contactless prin intermediul dispozitivelor cu sistem de operare Android.
- **Autentificare electronică (a Abonatului) pentru accesare IPAD MB** – 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.
- **Autentificare suplimentară cu amprenta digitală** – opțiune disponibilă doar pentru Dispozitivele echipate cu tehnologia “touch id / Finger Print” care prevede utilizarea amprentei digitale a Clientului, stocate în memoria Dispozitivului cu tehnologie “touch id / Finger Print”. Această modalitate implică scanarea și compararea amprentelor digitale cu cele salvate în dispozitivul / dispozitivele Clientului, date biometrice pe care Banca nu le prelucrează.
- **Autentificare suplimentară cu recunoaștere facială** – opțiune disponibilă doar pentru Dispozitivele cu tehnologie “Face ID” care permite utilizarea imaginii feței Clientului, stocată în memoria Dispozitivului prin care se scanează și se compară, în timp real, imaginea facială cu cea salvată în dispozitivul/dispozitivele Clientului, date biometrice pe care Banca nu le prelucrează.
- **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 E-Commerce (3D Secure);
- **Autentificare suplimentară prin aplicarea Codului de acces** - tipul Autentificării suplimentare care prevede setarea Codului de acces și aplicarea acestuia pentru accesarea ulterioară a IPAD Mobile Banking, fără a introduce Login-ul și Parola.
- **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 IPAD MB 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 IPAD MB, precum și pentru restabilirea Loginului și/sau Parolei; în acest caz Autentificarea suplimentară are denumire de „Autentificare alternativă”.
- **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 IPAD MB.
- **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 IPAD MB.
- **Autentificare strictă a clienților (SCA)**- autentificare configurată pe dispozitivul mobil al Clientului care se bazează pe utilizarea a două sau mai multe elemente din categoria cunoștințelor deținute (ceva ce doar Clientul cunoaște), a posesiei (ceva ce doar Clientul posedă) și a inerenței (ceva ce

reprezintă Clientul, la aplicarea verificării biometrice prin recunoaștere facială sau amprentă digitală). Elementele respective sunt independente, iar compromiterea unui element nu duce la compromiterea fiabilității celorlalte elemente, precum și acestea sunt concepute astfel încât să protejeze confidențialitatea datelor de autentificare.

- **Bancă** – BC „Moldindconbank” S.A.
- **Beneficiar/comerțiant** – destinatarul fondurilor ce au făcut obiectul unei operațiuni instant, realizată în baza unei metode de transfer MIA Plăți Instant;
- **Card de plată** – un suport de informație standardizat și, după caz, personalizat prin intermediul căruia deținătorul, de regulă, cu utilizarea numărului personal de identificare al său și/sau a unor alte coduri care permit identificarea sa, în funcție de tipul cardului de plată are acces la distanță la contul de plăți la care este atașat cardul de plată în vederea efectuării operațiunilor de plată.
- **Card principal** – card emis pe numele titularului Contului de card.
- **Card secundar** – card emis pe numele Utilizatorului autorizat.
- **Client** – Deținătorul Cardului sau a altor produse bancare.
- **Cod Quick Response (QR)** – reprezintă un cod de bare pătrate bidimensionale standardizate, care permit stocarea informației într-o etichetă vizuală, care poate fi citită de un dispozitiv ce dispune de elemente hardware necesare și de un software cititor;
- **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 IPAD Mobile Banking, fără a introduce Login-ul și Parola. Codul de acces se setează de către Client separat pentru fiecare Dispozitiv deținut.
- **Cont de card** – cont de plăți deschis la Bancă pe numele Deținătorului principal, cu scopul înregistrării operațiunilor de plată executate prin intermediul Cardurilor.
- **Deep link** - URL care direcționează utilizatorii direct către conținutul specific în cadrul unei aplicații, eliminând pașii suplimentari de navigare. Pe iOS, sunt gestionate cu Universal Links, iar Android folosește Intent Filters.
- **Deținător de card** - 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 Cardului principal care este totodată titular al Contului de card la care este emis acest Card.
- **Dispozitiv cu tehnologie “touch id / FingerPrint”** – dispozitiv mobil (smartphone, tabletă) dotat cu funcționalitatea “touch id”, care permite înregistrarea și utilizarea amprente digitale pentru accesarea dispozitivului.
- **Dispozitiv cu tehnologie “Face ID”**- dispozitiv mobil (smartphone, tabletă), echipat cu un sistem avansat de recunoaștere facială, care permite autentificarea și accesarea dispozitivului prin scanarea feței utilizatorului.
- **Document electronic** – orice document perfectat și/sau transmis Băncii de către Abonat prin intermediul IPAD MB.
- **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/recunoaștere facială.
- **IBAN** (International Bank Account Number) – șir de caractere care identifică în mod unic contul unui client deschis în Bancă;
- **Instituție guvernamentală** – autoritate/instituție publică subordonată Guvernului, care prestează servicii publice.
- **Instrucțiunea** – Instrucțiunea de utilizare MICB Mobile Banking – document perfectat de Bancă și accesibil de pe pagina <https://micb.md>, în care este descrisă modalitatea utilizării IPAD-ului de către Abonat. Instrucțiunea este parte integrantă a prezentelor Condiții de utilizare și sunt obligatorii de respectat în cadrul Abonării și utilizării IPAD MB.
- **Log out / ieșire / Выход** - acțiunea de finisare securizată a sesiunii de utilizare a IPAD-ului.
- **Login** – identificator alfanumeric alocat de Bancă Clientului pentru identificarea Clientului în calitate de Abonat.
- **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.).
- **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 IPAD-ului, necesar pentru Autentificarea Clientului în IPAD MB în calitate de Abonat.
- **Plătitor**- persoană fizică care este titularul unui cont de plăți, ce inițiază și autorizează un transfer din contul de plăți deținut.
- **PSP generator de QR**- participant al sistemului Instant al SAPI care generează coduri QR.
- **Push notificare**- opțiune de informare a clienților, prin intermediul notificărilor expediate la telefonul mobil conectat la internet, cu privire la tranzacțiile efectuate pe contul de card inclusiv cu utilizarea cardului de plata.
- **Server „MICB Mobile Banking”, Serverul IPAD MB** – 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 IPAD-ului.
- **Serviciu** – serviciul oferit de Bancă Abonatului prin intermediul IPAD MB, 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.

- **Serviciul „P2P by Phone”**- serviciu care oferă posibilitatea de a transfera mijloacele bănești de pe card pe card prin intermediul IPAD MICB Mobile Banking doar între deținători de carduri emise de Bancă, clienți ai Băncii persoane fizice, în baza numărului de telefon al beneficiarului (cu condiția că numărul de telefon al beneficiarului este înregistrat în sistemul informațional al Băncii și aparține unuia din operatorii GSM din Republica Moldova).
- **Serviciul „P2P MICB”** – serviciu care oferă posibilitatea de a transfera mijloacele bănești de pe card pe card prin intermediul Portalului www.transfer.md, bancomatelor gestionate de către Bancă, IPAD MICB Mobile Banking (accesibile *Deținătorilor de carduri MICB*).
- **Serviciul „SMS-notificări”** - serviciu de informare a clienților prin intermediul mesajelor SMS expediate la telefonul mobil cu privire la tranzacțiile efectuate pe contul de card inclusiv cu utilizarea cardului de plată. 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.).
- **Serviciul Me2Me** - serviciu ce permite efectuarea transferurilor între conturile proprii ale Clientului, deschise în diferite Bănci ce au fost înrolate cel puțin o dată în sistemul MIA Plăți Instant.
- **Serviciul RTP (Request To Pay)** – serviciu de mesagerie care permite beneficiarului plății prin intermediul prestatorului său de servicii de plată să solicite inițierea unui ordin de plată în MDL de la un plătitor.
- **Servicii publice** - servicii de interes public, prestate de instituții guvernamentale.
- **Sesiune de utilizare a Instrumentului de plată electronic cu acces la distanță** – sesiunea stabilită dintre echipamentul terminal al Abonatului (calculator etc.) și Serverul Sistemului, în baza Autentificării Abonatului pentru accesarea IPAD, pe parcursul căreia Abonatului sunt accesibile Serviciile IPAD-ului.
- **SEPA-(Single Euro Payments Area)** - un sistem de plăți folosit numai pentru plățile în Euro fără numerar, disponibil în țările membre UE și în alte câteva state din zona geografică europeană, în conformitate cu Registrul participanților la plățile SEPA și schemele de plată respective.
- **Tarife** – [Tarifele și limitele privind 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.
- **Telefon mobil / dispozitiv mobil** – echipament de tip smartphone sau tabletă, utilizat de către Abonat pentru conectarea la IPAD MB și utilizarea ulterioară
- a acestuia.
- **Transfer Instant P2B (Person to Business)** - serviciu ce permite transferarea mijloacelor bănești prin sistemul MIA, direct din contul plătitorului persoană fizică, către beneficiar – persoană juridică, prin utilizarea opțiunilor plată prin QR, Deep Link și solicitare de plată RTP, inițiate de beneficiar.
- **Transfer Instant P2G (Person to Government)** - serviciu ce asigură transferul fondurilor din contul plătitorului persoană fizică către instituțiile guvernamentale, prin intermediul sistemului de plăți MIA, utilizând opțiunile de plată prin QR, Deep Link și solicitări de plată RTP, inițiate de instituțiile guvernamentale.
- **Transfer Instant P2P (Person to Person)** - serviciu care oferă posibilitatea de a transfera mijloacele bănești de pe un cont de card pe alt cont (deschis în cadrul Băncii sau în alt prestator, participant la sistemul de plăți instant ”MIA”), prin intermediul instrumentului de plată electronic cu acces la distanță MICB Mobile Banking, doar pentru utilizatorii sistemului de plăți instant ”MIA”, în baza numărului de telefon al beneficiarului plății.
- **Tranzacție electronică, Tranzacție** – operațiune efectuată în formă electronică în cadrul Sesiunii de utilizare a IPAD-ului 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.
- **Utilizator al serviciilor de plată/utilizator**– persoană fizică sau juridică, inclusiv instituție guvernamentală care folosește un serviciu de plată în calitate de plătitor, de beneficiar al plății sau în ambele calități.
- **Utilizator autorizat** – Deținător de card, altul decât Deținătorul principal: persoana fizică pe numele căreia este emis Cardul în conformitate cu Cererea de emisie, și este nominalizată de către Deținătorul principal ca Utilizator autorizat al Contului de card.

În cazul în care anumite noțiuni sau acronime nu sunt definite în prezentele Condiții de utilizare, acestea vor avea înțelesul stabilit în Condițiile Generale Bancare pentru persoane fizice.

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”.

3. Abonarea și autentificarea la IPAD MICB Mobile Banking

3.1. Abonarea la IPAD se efectuează de către Client în baza acceptării prezentelor Condiții, utilizând ”Instrucțiunea de utilizare MICB Mobile Banking” și are ca rezultat obținerea de către Client a Login-ului și Parolei.

3.2. Abonarea la IPAD se efectuează prin interfața IPAD MICB Mobile Banking și poate fi efectuată prin următoarele modalități:

3.2.1. Abonarea prin introducerea numărului cardului, data expirării cardului, data nașterii și codului CVV2 în IPAD MB:

3.2.1.1. Clientul efectuează abonarea prin intermediul IPAD „MICB Mobile Banking”;

3.2.1.2. Clientul inițiază operațiunea de primire a Login-ului și a Parolei prin introducerea numărului unui Card valabil emis pe numele său, termenului de expirare a cardului, datei nașterii și codului CVC2/CVV2 și efectuarea Autentificării alternative de tip „SMS OTP” sau „ATM OTP”;

3.2.1.3. 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 IPAD MB este posibilă prin mai multe modalități:

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

- accesare a IPAD Mobile Banking, folosind codul digital scurt și convenabil în loc de numele de utilizator și parola;

3.3.1.2. **Cu numele de utilizator și parola:** se va utiliza numele de utilizator și parola utilizate pentru autentificarea care a fost setat în IPAD MICB Mobile Banking;

3.3.1.3. **Cu utilizarea amprentei digitale/recunoașterii faciale:** prin scanarea și identificarea amprentei digitale/imaginii faciale salvată în dispozitivul / dispozitivele Clientului. Autentificarea prin utilizarea amprentei digitale/recunoaștere facială poate fi efectuată doar de pe un dispozitiv “touch id / FingerPrint”/„Face ID”.

Notă: Banca își rezervă dreptul de a aplica una sau mai multe metode de autentificare pentru accesarea IPAD Mobile Banking conform pct. 3.3.

3.4. Clientul, prin Abonare la IPAD, 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 datele bancare 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 IPAD MICB Web Banking implicit au acces și la IPAD MICB Mobile Banking, cu utilizarea Login-ului și Parolei identice.

Clientul este de acord că folosirea IPAD MICB Mobile Banking este controlat și că tentative de folosire neautorizată a acestuia se urmărește în conformitate cu legislația în vigoare.

4. Autentificarea în IPAD MB prin amprenta digitală sau recunoaștere facială

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

4.2. Autentificarea prin amprenta digitală/recunoaștere facială poate fi utilizată ca o metodă alternativă de logare în IPAD pentru confirmarea identității Abonatului.

4.3. Tehnologia specifică dispozitivului “touch id / FingerPrint”/“Face ID” care scanează și identifică amprentele digitale/imaginea facială salvate ale Abonatului nu este creată de Bancă, astfel încât Banca nu o gestionează, nu este răspunzătoare și nu oferă nicio 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” /“Face ID” o promovează.

4.4. Activarea opțiunii de autentificare prin amprenta digitală sau recunoaștere facială poate fi efectuată de Abonatul care îndeplinește următoarele condiții:

- a. Este un utilizator al IPAD MICB Mobile Banking;
- b. A instalat aplicația mobilă pe un dispozitiv echipat cu “touch id”/“Face ID” propriu;
- c. A setat în IPAD codul de acces din 5 cifre;
- d. A activat la dispozitivul “touch id / FingerPrint”/“Face ID” funcția de autentificare prin amprenta digitală/recunoaștere facială și a înregistrat cel puțin o amprentă digitală/imagine facială personală;
- e. A verificat dacă în memoria dispozitivului “touch id / FingerPrint”/“Face ID” sunt salvate amprentele digitale/imaginea facială personale.

4.5. Abonatul, prin autentificarea în Sistem cu utilizarea amprentei digitale/recunoașterea facială, 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/ imagine facială salvată în dispozitivul “touch id / FingerPrint”/”Face ID” poate fi utilizată în calitate de Factor de autentificare la Sistem, permițând, astfel, accesul la conturile / cardurile personale ale Deținătorului;
 - b. Confirmă că este de acord că, în scopul utilizării funcționalității “touch id”/”face ID”, IPAD-ul accesează amprente digitale/imaginea facială înregistrate în dispozitivul “touch id / FingerPrint”/”Face ID” 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”/”Face ID” de accesarea acestora de către persoanele terțe;
 - d. Recunoaște că autentificarea în IPAD MB prin utilizarea amprentei digitale/recunoașterea facială este o metoda alternativă de autentificare și poate fi utilizată concomitent cu alte metode de autentificare;
- 4.6. De fiecare dată când aplicația mobilă identifică utilizarea amprentei digitale/recunoaștere facială salvate în dispozitivul “touch id / FingerPrint”/”Face ID”, se consideră că Abonatul a accesat Sistemul și a autorizat Banca să efectueze astfel de tranzacții.
- 4.7. Abonatul poate, în orice moment, dezactiva funcționalitatea de utilizare a amprentei digitale/recunoaștere facială.
- 4.8. Banca nu garantează că funcționalitatea “touch id / FingerPrint”/”Face ID” va fi accesibilă de pe orice dispozitiv, precum și nu poate garanta continuitatea accesibilității funcționalității respective.
- 4.9. Banca nu este responsabilă pentru nicio pierdere suportată de Abonat în legătură cu utilizarea sau încercarea de utilizare a funcționalității “touch id”/”Face ID” în cazul unor tranzacții neautorizate, orice acces neautorizat la dispozitivul “touch id / FingerPrint”/”Face ID”.

5. Restabilire Login și/sau Parolei

- 5.1. Restabilirea Login-ului și/sau Parolei poate fi efectuată prin următoarele modalități:
- 5.1.1. **Obținerea Login-ului și modificarea Parolei prin introducerea numărului Cardului, termenului de expirare a cardului, datei nașterii și codului CVC2/CVV2 și Autentificării alternative de tip „SMS OTP”**
 - 5.1.1.1. Clientul efectuează această operațiune prin intermediul sistemului Mobile Banking;
 - 5.1.1.2. Clientul autentifică operațiunea de primire a Login-ului și Parolei prin introducerea numărului unui Card valabil emis pe numele său, termenului de expirare a cardului, datei nașterii, Codului CVC2/CVV2 și efectuarea Autentificării alternative de tip „SMS OTP”.
 - 5.1.1.3. 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 IPAD MB

- 6.1. Securitatea IPAD MB 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 IPAD-ului MB este asigurată prin următoarele cerințe de autentificare și/sau confirmare tranzacții:
- 6.2.1. o persoană poate să se Aboneze la IPAD MB în calitate de Client sau să obțină acces la Login-ul și Parolă în baza numărului Cardului, termenului de expirare a cardului, datei nașterii, codului CVC2/CVV2 și Autentificării alternative în IPAD MB;
 - 6.2.2. o persoană poate să obțină accesul la IPAD MB în calitate de Abonat doar în baza procedurii Autentificării în IPAD MB;
 - 6.2.3. în cadrul Sesiunii de utilizare a IPAD-ului MB, unele Servicii sunt accesibile doar în baza Autentificării suplimentare;
- 6.3. pentru a accesa online contul de plăți sau pentru a autoriza tranzacțiile, este necesară utilizarea Autentificării Stricte a Clientului (SCA). Factorul principal al securității IPAD-ului MB este autentificarea. Securitatea IPAD-ului este garantată 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 [Condițiile Generale Bancare pentru persoane fizice](#).
 - 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 amprentei digitale. Compromiterea acestui Factor este situația în care Clientul nu este ferm convins asupra faptului că o persoană terță nu a avut acces la dispozitivul “touch id / FingerPrint” și nu a salvat amprenta sa digitală în dispozitivul “touch id / FingerPrint”.

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

6.5. Cu scopul prevenirii compromiterii Parolei, Clientul trebuie:

6.5.1. să nu înscrie Parola pe un suport care permite asocierea cu IPAD MB, prin natura sau poziționarea sa;

6.5.2. să modifice regulat Parola cu ajutorul Serviciului respectiv al IPAD-ului MB;

6.5.3. să asigure protejarea 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”/“Face ID”.

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 IPAD-ului MB ;

6.6.2. Operațiunea de modificare a Parolei prin introducerea numărului Cardului, termenului de expirare a cardului, datei nașterii, codului CVC2/CVV2 și Autentificării alternative de tip „SMS OTP”.”;

6.6.3. 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 pentru accesarea IPAD-lui 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 prin intermediul Serviciului suport carduri 24/24 al Băncii la numărul de telefon 022 71 71 71 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:

6.10.3.1. modificarea numărului de telefon în cadrul Serviciului „SMS-notificări” prin intermediul bancomatului Băncii, sau prin depunerea cererii respective la una dintre sucursalele Băncii;

6.10.3.2. 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. Cerințe și modalitatea de setare Autentificarea Strictă a Clientului (SCA)

6.13.1. Serviciul oferă posibilitatea utilizatorului de a seta codul de autentificare personalizat, pentru accesarea ulterioară a contului de plăți și confirmarea operațiunilor de plăți

6.13.2. Procesul de setare a Autentificării Stricte a Clientului (SCA) se realizează prin parcurgerea următorilor pași:

a. Din meniul principal, utilizatorul accesează secțiunea Setări și selectează opțiunea „Securitatea contului SCA” din Setările de securitate;

b. În interfața deschisă, utilizatorul alege opțiunea „Activați Autentificarea Strictă” și solicită activarea prin apăsarea butonului corespunzător;

- c. Utilizatorul va primi un cod OTP pe numărul de telefon înregistrat în sistemul băncii ce necesită a fi confirmat;.
 - d. Utilizatorului i se va solicita să seteze un cod de autentificare personalizat, din 5 cifre, pe care trebuie să-l confirme prin reintroducerea acestuia;
 - e. Pentru o siguranță suplimentară, utilizatorul poate activa și autentificarea prin date biometrice setate în dispozitiv (amprentă digitală sau recunoaștere facială), în funcție de sistemul de operare.
 - f. După parcurgerea acestor pași, utilizatorul va fi informat dacă setarea a fost realizată cu succes;
 - g. Autentificarea Strictă a Clientului este valabilă doar de pe un singur dispozitiv înregistrat;
 - h. Dacă este necesar, utilizatorul poate modifica codul de autentificare din Setări la compartimentul Securitate;
 - i. Dacă utilizatorul schimbă dispozitivul, acesta trebuie să dezactiveze SCA de pe dispozitivul anterior din Setări la compartimentul Securitate sau să contacteze Serviciul Suport.
- 6.13.3. Utilizatorul este responsabil să seteze un cod sigur, să utilizeze o combinație din 5 cifre complexă și să nu divulge codul personalizat persoanelor terțe.
- 6.13.4. Utilizatorul este responsabil să verifice setările de securitate ale contului pentru a se asigura că metodele de autentificare sunt corect configurate și actualizate.
- 6.13.5. În cazul în care utilizatorul suspectează compromiterea codului de autentificare personalizat sau a datelor biometrice, acesta trebuie să dezactiveze imediat SCA din meniul de securitate și să asigure setarea unui nou cod.
- 6.13.6. Dacă utilizatorul suspectează orice activitate neautorizată asupra contului său, trebuie să contacteze imediat Serviciul Suport pentru a bloca accesul la cont și a iniția investigația suspiciunii de acces neautorizat.
- 6.13.7. În cazul blocării accesului din cauza introducerii greșite a codului de autentificare personalizat de 5 ori consecutiv, utilizatorul trebuie să contacteze Serviciul Suport și să urmeze procedura de resetare a autentificării printr-o verificare suplimentară.
- 6.13.8. În cazul în care utilizatorul pierde accesul la dispozitivul cu MICB Mobile Banking instalat, trebuie să contacteze imediat Serviciul Suport pentru a dezactiva SCA de pe dispozitivul pierdut și să solicite asistență pentru restabilirea accesului pe un alt dispozitiv.
- 6.14. Suspendarea / reactivarea Login-lui:**
- 6.14.1. În cazul în care securitatea Login-lui este compromisă din motive diferite și securitatea Login-lui nu poate fi restabilită (asigurată) prin suspendarea / anularea Factorilor de autentificare, Clientul trebuie să solicite suspendarea Login-lui, apelând Serviciul suport carduri 24/24 al Băncii;
- 6.14.2. În cazul suspendării Login-lui Autentificarea în IPAD MB și restabilirea parolei nu vor fi accesibile;
- 6.14.3. 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;
- 6.14.4. Reactivarea Login-lui nu duce în sine la reactivarea Factorilor de autentificare.
- 6.15. Banca protejează datele transmise între Serverul Sistemului și Telefon mobil / dispozitiv mobil prin cifrarea acestora.
- 6.16. Banca recomandă următoarele modalități de utilizare securizată a Sistemului „MICB Mobile Banking”:
- 6.16.1. Să nu divulge informația confidențială altor persoane (PIN, numărul de card, parole, conturi, datele personale);
- 6.16.2. Să nu lase dispozitivul / dispozitivul “touch id / FingerPrint”/“Face ID” fără supraveghere în special după procedura de autentificare și să asigure că ecranul dispozitivului nu este vizibil altor persoane;
- 6.16.3. Să seteze parola de acces la dispozitivul mobil și opțiunea de blocare a dispozitivului după o perioadă de inactivitate;
- 6.16.4. Să utilizeze parole și coduri de acces sigure pentru a evita spargerea lor;
- 6.16.5. Să utilizeze diferite parole pentru fiecare serviciu (poșta electronică, conturile de acces la rețelele de socializare, etc.);
- 6.16.6. Să nimicească bonurile cu parolele ATM OTP dacă nu vor fi utilizate;
- 6.16.7. 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;
- 6.16.8. Să efectueze regulat actualizarea sistemului de operare, aplicației MICB Mobile Banking și altor aplicații instalate pe dispozitivul mobil, utilizând numai surse oficiale;
- 6.16.9. Pentru a fi siguri că nu descărcă ceva dubios, să dezactiveze în setările telefonului pe platforma Android opțiunea „Surse Necunoscute” în setările de „Securitate”;
- 6.16.10. 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;
- 6.16.11. 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.;

- 6.16.12. Aplicația MICB Mobile Banking va fi utilizată numai de către Abonatul la Sistem;
- 6.16.13. Să șteargă 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;
- 6.16.14. Să activeze opțiunea de control la distanță pentru ștergerea datelor la distanță sau blocare în cazul pierderii dispozitivului;
- 6.16.15. 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;
- 6.16.16. În cazul pierderii sau furtului dispozitivului mobil, să schimbe urgent parola de acces la instrumentul de plată electronic cu acces la distanță, să informeze imediat Banca pentru blocarea cardurilor și a accesului la IPAD, să sune operatorul telefoniei mobile pentru blocarea cartei SIM;
- 6.16.17. În cazul schimbării numărului de telefon sau neutilizării acestuia pentru o perioadă de timp mai mare decât valabilitatea cartei SIM, să informeze Banca pentru deconectarea IPAD-ului de la numărul de telefon pentru a evita compromiterea modalității de Autentificare Suplimentară de tip SMS OTP;
- 6.16.18. 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;
- 6.16.19. 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;
- 6.16.20. În cazul nefuncționării cartei SIM să sune imediat la operatorul telefoniei mobile pentru a se asigura că cauza nu este urmare a acțiunilor frauduloase;
- 6.16.21. Să termine lucrul cu aplicația mobilă prin accesarea butonului Exit (Ieșire);
- 6.16.22. Să ignore 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.);
- 6.16.23. 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 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 IPAD MICB Mobile Banking

- 7.1. Serviciile financiare ale IPAD MB 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. Pentru serviciile financiare și tranzacțiile supuse autorizării, se va solicita autorizarea acestora prin aplicarea Autentificării Stricte a Clientului (SCA).
- 7.4. În cazul inițierii unei tranzacții financiare care necesită Autentificarea Strictă a Clientului (SCA), însă SCA nu este setată, la etapa de autorizare, utilizatorul va fi informat că trebuie să activeze SCA pentru a putea finaliza și autoriza tranzacția.
 - 7.4.1. **Serviciul „P2P MICB”** - se efectuează în conformitate cu [Condițiile de utilizare a Serviciului „P2P MICB”](#) accesibile pe pagina web.
 - 7.4.2. **Serviciul „Transfer pe cardul propriu”** – permite efectuarea Transferurilor între cardurile personale.
 - 7.4.3. **Serviciul „Transfer pe card Moldindconbank”** – permite efectuarea Transferurilor de pe Cardul emis pe numele Abonatului pe un alt card emis de Bancă pe numele altei persoane decât Abonatul.
 - 7.4.4. **Serviciul „Transfer pe card străin”** - permite efectuarea Transferului de pe Cardul emis pe numele Abonatului pe un alt card emis de altă Bancă din R. Moldova și/sau străinătate (Visa sau MasterCard).
 - 7.4.5. **Serviciul „P2P by Phone”**- permite efectuarea Transferului de pe cardul emis pe numele Abonatului pe un alt card emis de Bancă pe numele altei persoane decât Abonatul (transferul se efectuează în baza numărului de telefon mobil al beneficiarului).
- 7.5. **Serviciul „Achitarea creditului MICB”**- permite achitarea datoriilor pentru creditele în MDL proprii deținute la Bancă (cu excepția creditelor acordate la contul de card);
- 7.6. 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.
- 7.7. 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. Documentul electronic autorizat de către client după ora 19:00 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 datoriei aferente creditului, cu condiția asigurării transferului mijloacelor bănești de către client în contul curent, până la ora 19:00 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 este stabilit de către Bancă și este plasat pe site-ul Băncii: <https://www.micb.md/c/>.

7.8. Serviciul „Plăți în baza contractelor de prestare a serviciilor bancare aferente achitării plăților în favoarea beneficiarului acestora”::

7.8.1. Serviciul „Plăți în baza contractelor de prestare a serviciilor bancare aferente achitării plăților în favoarea beneficiarului acestora” (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”).

7.8.2. 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.

7.8.3. Banca stabilește unilateral lista Furnizorilor de servicii și o poate modifica fără preaviz.

7.8.4. 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.

7.8.5. 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).

7.8.6. 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.

7.8.7. Etapele și modalitatea de prelucrare a Plății:

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

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

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

7.8.7.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:

7.8.7.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;

7.8.7.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:

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

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

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

7.8.8. Responsabilitatea Băncii:

- a. Banca este responsabilă de executarea corectă și la timp a prevederilor pct. 7.8.7.c.2 și 7.8.7.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. 7.8.7.c.2 și 7.8.7.c.3, precum și nu este responsabilă de calitatea mărfurilor și serviciilor oferite Clientului de către Furnizor.

7.8.9. 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.

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

7.9. Serviciul “Transfer către IBAN”:

7.9.1. Serviciul „Transfer către IBAN” (în continuare în cadrul acestui compartiment „Plăți”) permite Clientului perfectarea plății către contul curent al persoanei fizice și juridice în baza datelor bancare.

7.9.2. Serviciul „Transfer către IBAN” permite efectuarea transferului doar în lei moldovenești (MDL).

7.9.3. Utilizarea acestui Serviciu duce la perfectarea Documentului electronic prin care Abonatul solicită efectuarea plății către conturile curente ale persoanelor fizice și juridice deschise în Bancă sau altă bancă din Republica Moldova. Acest Document are statut de cerere.

7.9.4. Modalitatea de prelucrare a Tranzacției:

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

- a.1. se verifică corectitudinea completării câmpurilor Documentului, conform cerințelor stabilite de către Bancă;
- a.2. 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:

- b.1. banca blochează instantaneu suma transferului pe Contul Cardului de pe care se efectuează plata, ceea ce duce la micșorarea Sumei disponibile pe acesta.

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

- c.1. banca debitează Contului Cardului de pe care se efectuează transferul;
- c.2. banca efectuează transferul mijloacelor bănești pe contul curent al persoanei fizice/juridice în baza datelor bancare prezentate;

7.9.5. Responsabilitatea Băncii:

- a) Banca este responsabilă de executarea corectă și la timp a prevederilor p.7.8.4c.2., totodată termenele concrete de executare a acestor acțiuni depinde de graficul de lucru al Băncii;
- b) Banca nu este responsabilă de reacția și timpul reacției Băncii beneficiare la executarea de către Bancă a prevederilor p. 7.8.4 c.2.

7.9.6. Transferurile efectuate sunt confirmate prin aplicarea Autentificării Stricte a Clientului (SCA) .

7.10. Sistemul de plăți instant ”MIA”

7.10.1. **Sistemul de plăți instant ”MIA” (Sistem MIA)** este o soluție implementată și administrată de BNM, destinată procesării imediate a plăților instant în MDL. Aceasta permite transferuri între utilizatori persoane fizice și plăți pentru bunuri și servicii în favoarea comercianților și instituțiilor guvernamentale. Sistemul oferă o platformă care asigură mai multă siguranță și comoditate, fiind integrat direct cu aplicația „MICB Mobile Banking” pentru efectuarea plăților.

7.10.2. Activarea serviciilor incluse în sistemul de plăți instant MIA este realizată prin intermediul aplicației MICB Mobile Banking din meniul Setări acceptând ”Termenii și condițiile de utilizare al sistemului de plăți instant MIA”.

7.10.3. Contul asociat Sistemului MIA poate fi modificat prin intermediul meniului ”Setări MIA” direct din „MICB Mobile Banking”. Numărul de telefon asociat unui cod IBAN în cadrul MIA poate fi exclusiv doar numărul de telefon declarat în vederea desfășurării relațiilor contractuale cu Banca;

7.10.4. Dezactivarea serviciilor Sistemului MIA se efectuează prin intermediul meniului ”Setări MIA” din aplicația „MICB Mobile Banking”.

7.10.5. Sistemul de plăți instant MIA este reprezentat prin următoarele servicii:

7.9.5.1. **Transfer instant P2P (Person to Person)** - reprezintă transferul efectuat prin intermediul aplicației „MICB Mobile Banking”, către un număr de telefon (alias) beneficiarul căruia este înregistrat în Sistemul MIA;

- La inițierea operațiunii de plată de către plătitor, prin indicarea numărului de telefon mobil (alias) al beneficiarului plății, Banca, unde plătitorul își are deschis contul, va verifica prin serviciul de căutare CAS (Central addressing schema) al Băncii Naționale a Moldovei, dacă numărul de telefon este înregistrat în Sistemul MIA. Dacă în urma verificării, numărul de telefon a fost identificat, plătitorul va putea iniția transferul.
- Utilizatorii serviciilor Sistemului MIA pot iniția și recepționa plăți, dacă aceste opțiuni au fost setate în aplicația „MICB Mobile Banking”.
- Mijloacele bănești transferate prin Sistemul MIA vor fi înregistrate în contul de plăți al beneficiarului, care deține numărul de telefon înrolat în Sistemul MIA.
- Din moment ce plata a fost executată, aceasta nu poate fi anulată.
- Timpul maxim alocat de Sistemul MIA pentru executarea unei plăți este de 20 secunde

7.9.5.2. **Solicitare de plată de tip RTP (Request to Pay)** – reprezintă cererea de plată, prin care o persoană fizică sau persoană juridică, inclusiv instituție guvernamentală, poate solicita un transfer sau o plată pentru bunuri și servicii, inclusiv servicii publice, de la o persoană fizică în baza numărului de telefon (alias), care este înregistrat în Sistemul MIA.

- Utilizatorii serviciilor Sistemului MIA (persoane fizice) pot genera și accepta cereri de plata RTP, în favoarea altor utilizatori persoane fizice, prin intermediul sistemului, din aplicația mobilă.
- Utilizatorii serviciilor Sistemului MIA (persoane fizice) pot accepta cereri de plată de la comercianți, pentru achitarea bunurilor și serviciilor.
- Utilizatorii serviciilor Sistemului MIA (persoane fizice) pot accepta cereri de plată de la instituțiile guvernamentale, pentru achitarea serviciilor publice.
- Notificarea aferentă solicitărilor de plată se va efectua prin intermediul Push-notificărilor;
- Utilizatorul persoană fizică poate genera maxim 10 solicitări pe zi;
- Cererile pot fi acceptate sau respinse de către destinatari;
- Cerea poate fi anulată de către inițiator, dacă aceasta nu a fost acceptată de plătitor;
- Durata de existență a unei solicitări este de 24 ore;
- Istoricul solicitărilor de plată va fi păstrat în MICB Mobile banking, unde toate cererile vor putea fi gestionate (acceptate, respinse, anulate);
- Acceptarea unei solicitări este echivalată cu un transfer MIA-P2P, P2B, P2G.

7.9.5.3. **Serviciul Me2Me** -serviciu ce permite efectuarea transferurilor între cardurile/conturile proprii ale Clientului, deschise în diferite Bănci sau societăți de plată, din Republica Moldova.

- Pentru a efectua transferul este necesară activarea serviciilor Sistemului MIA în cadrul aplicațiilor bancare al prestatorului de servicii de plată unde utilizatorul are deschis cont de card sau cont curent.
- Utilizatorul poate iniția transferul prin accesarea Serviciului Me2Me, din aplicația mobilă MICB Mobile Banking și selectând instituția bancară sau societatea de plată, la care are deschis contul.
- Transferurile pot fi efectuate doar în monedă națională MDL.

7.9.5.4. **Plată cu QR**- metodă electronică de efectuare a transferurilor rapide și securizate, de plată a bunurilor și serviciilor, inclusiv servicii publice, între utilizatorii serviciilor de plată, în care tranzacția este inițiată și autorizată prin scanarea codului QR prin intermediul aplicației mobile MICB Mobile Banking.

- Pentru a accepta plățile prin MIA QR, este necesară înrolarea în sistemul MIA Plăți Instant.
- La scanarea codului QR în afara aplicației mobile, plătitorul va fi redirecționat către pagina intermediară <https://mia-qr.bnm.md> unde va putea selecta aplicația financiară MICB Mobile Banking, pentru autorizare transfer.

- 7.9.5.5. **Plată cu deep link** – metodă avansată de efectuare a transferurilor și de plată a bunurilor și serviciilor, inclusiv servicii publice, realizată prin accesarea unui link special generat de către beneficiar în adresa plătitorului, pentru inițierea și procesarea unei tranzacții în aplicația mobilă
- Plătitorul, la accesarea deep link-ului de plată, va fi redirecționat către pagina intermediară BNM <https://mia-qr.bnm.md>, de unde va putea selecta prestatorul de servicii de plată la care deține aplicație mobilă.
 - Prin intermediul aplicației mobile, utilizatorul va putea vizualiza detaliile de plată și confirma transferul sau plata pentru bunuri și servicii.

- 7.9.5.6. **Generare QR/Deep Link** - serviciu destinat pentru crearea solicitărilor de plată în cadrul sistemului de plăți MIA, prin intermediul unui cod QR/Deep link, generat direct din aplicația MICB Mobile Banking.

- Beneficiarul are opțiunea de a genera coduri QR Statice/Deep Link cu sumă liberă sau sumă fixă.
- În momentul generării codului QR, se formează automat și deep link-ul asociat.
- Codurile QR pot fi partajate pentru a fi scanate, direct de pe ecranul telefonului mobil sau pot fi expediate prin oricare canal de mesagerie accesibil.
- Codurile QR statice generate, nu au termen de expirare și pot fi utilizate pentru plăți repetate.
- Dacă în baza Codului QR nu se execută plăți în decurs de 30 zile, acesta devine inactiv.
- Utilizatorii au posibilitatea să vizualizeze lista codurilor QR generate, statutul acestora și istoricul plăților executate în baza acestora.
- Codurile QR active, pot fi anulate la necesitate, de către utilizatorul care le-a creat.

7.9.6. Modalitatea de prelucrare a unei tranzacții efectuate prin Sistemul MIA:

7.9.6.1. Pentru transferurile instant P2P:

1. Verificarea Documentului de plată electronic:

- se verifică dacă numărul de telefon indicat în ordinul de plată este înregistrat în Sistemul MIA, conform cerințelor stabilite de către Bancă;
- se verifică posibilitatea efectuării acestei plăți de pe contul indicat de către utilizatorul sistemului (suma disponibilă, statut, limite etc.) în cazul Băncii în calitate de PSP Plătitor;
- se verifică dacă au fost îndeplinite condițiile de executare a ordinului de plată pentru înregistrarea în contul beneficiarului, în cazul Băncii în calitate de PSP Beneficiar.

2. Autorizarea operațiunii de plată are loc în temeiul consimțământului plătitorului exprimat prin Autentificarea Strictă a Clientului (SCA).

3. Executarea finală a Documentului de plată electronic prevede următoarele acțiuni:

- Banca debitează Contului de plăți al plătitorului de pe care se efectuează transferul sau respinge executarea ordinului de plată și informează imediat plătitorul cu privire la aceasta;
- Banca efectuează transferul mijloacelor bănești pe contul de plăți al beneficiarului în baza alias-ului indicat.
- Banca înregistrează în contul beneficiarului suma indicată în ordinul de plată sau respinge executarea acestuia, prezentând în sistemul Instant un răspuns cu indicarea motivului pentru care nu îl acceptă.

7.9.6.2. Pentru solicitările de plată de tip RTP:

1. Verificarea solicitării RTP de către Sistemul MIA din punct de vedere tehnic :

- în cazul validării cu succes, Sistemul MIA redirecționează RTP-ul către prestatorul de servicii de plată al plătitorului pentru validare și informarea plătitorului despre RTP;
- în cazul în care RTP nu a fost validat din punct de vedere tehnic, Sistemul MIA respinge RTP-ul și transmite către prestatorul de servicii de plată al beneficiarului o informare în acest sens.

2. Acceptarea sau respingerea RTP de către plătitor:

- dacă plătitorul respinge RTP-ul, se remite un răspuns negativ la solicitarea RTP;
- dacă plătitorul acceptă RTP-ul, se inițiază ordinul de transfer Sistemului MIA spre procesare.

3. Executarea finală a RTP-ului

- Banca execută sau respinge ordinul de transfer și informează beneficiarul/comerciantul despre executarea sau respingerea RTP-ului inițiat.

7.9.6.3. Pentru transferurile Me2Me:

1. Verificarea Documentului de plată electronic:

- Se verifică dacă conturile indicate în ordinul de plată sunt înregistrate în Sistemul MIA ;
- Se verifică posibilitatea efectuării plății de pe contul MICB către contul deținut în altă bancă (suma disponibilă, statut, limite etc.).

2. Autorizarea transferului, dacă au fost validate datele în urma verificării, în corespundere cu cerințele tehnice.

3. Executarea finală a Documentului de plată electronic, prevede următoarele acțiuni:

- Banca debitează Contului de plăți al plătitorului de pe care se efectuează transferul;
- Banca efectuează transferul mijloacelor bănești de pe contul de plată al beneficiarului către contul personal deschis în altă bancă și înregistrat în Sistemul MIA.

7.9.6.4. Pentru transferurile cu QR și Deep link:

1. **Verificarea** ordinului și a detaliilor de plată în baza datelor obținute după scanarea codului QR sau accesare deep link;
2. **Acceptarea** de către Sistemul MIA a ordinului completat în baza codului QR sau Deep link;
3. **Executarea** ordinului de către bancă, în conformitate cu Regulile de funcționare a serviciului ;
4. **Informarea** utilizatorilor sistemului de plată MIA, despre executarea transferului.

7.9.6.5. Pentru Generarea Codurilor QR/Deep Link :

1. Beneficiarul plății/Comerciantul inițiază o solicitare de creare a unui cod QR prin intermediul PSP generator de QR
2. PSP generator de QR transmite solicitarea de creare QR în serviciul QR al sistemului instant, cu indicarea datelor necesare pentru completare a ordinului de plată.

7.9.6.6. Comisioanele pentru plățile executate prin sistemul de plăți instant „MIA” se aplică în corespundere cu ”Comisioane și limite aplicate pentru procesarea transferurilor prin Sistemul MIA Plăți Instant”, care sunt plasate și pot fi consultate pe pagina oficială a Băncii: www.micb.md.

7.10. Program de loialitate ”Cashback”

7.10.1 **Programul de loialitate cashback** oferă posibilitatea deținătorilor de card de a beneficia de mijloace financiare, determinate prin aplicarea unui anumit procent la valoarea tranzacțiilor care vor fi eligibile și vor corespunde criteriilor de aplicare a cashback-ului. Scopul acestui program este de a stimula tranzacțiile fără numerar la o varietate de comercianți. Categoriile de coduri de comerciant (MCC) pentru care se poate acorda cashback pot fi ajustate la discreția băncii.

7.10.2 Cashback-ul se activează direct din aplicație prin selectarea cardului și accesarea meniului ”Servicii” din care este selectată opțiunea cashback;

7.10.3 Cashback-ul poate fi conectat pentru toate conturile de card eligibile;

7.10.4 Cashback-ul se calculează imediat după efectuarea tranzacției cu unul din cardurile pentru care acesta a fost activat;

7.10.5 Cashback-ul se acumulează în contul de loialitate în valuta contului pentru care a fost conectat;

7.10.6 Utilizatorii au posibilitatea să solicite retragerea cashback-ului acumulat prin intermediul aplicației mobile a băncii IPADMICB Mobile Banking. Această facilitate oferă flexibilitate și ușurință clienților în gestionarea beneficiilor cashback-ului.

7.11 Acordarea creditelor în IPAD MICB Mobile Banking

Procesul de creditare online în aplicația mobilă a Băncii este structurat în mai multe etape esențiale, fiecare având un rol specific în asigurarea unui flux eficient și sigur pentru utilizator.

7.11.1 Identificarea Clientului Eligibil și Afișarea Ofertei

- Clientul deschide aplicația mobilă și se autentifică folosind datele de acces;
- Sistemul verifică criteriile de eligibilitate ale clientului în baza profilului;
- Dacă clientul îndeplinește criteriile stabilite de Bancă pentru solicitarea unei oferte de credit, în interfața principală a aplicației va apărea un banner informativ. Acest banner va afișa un mesaj care îi va comunica clientului că are posibilitatea de a solicita o ofertă de credit, indicând totodată și suma maximă disponibilă a creditului, conform produsului creditar pus la dispoziție de Bancă.

7.11.2 Informații despre Ofertă și Acceptarea Condițiilor

- Clientul accesează bannerul pentru a afla mai multe detalii despre oferta de credit;
- Pe această pagină, clientul găsește un link către documentul "Reguli de solicitare a creditului pentru Persoane Fizice prin intermediul aplicației mobile a Băncii". Acest document oferă detalii complete despre procesul de creditare prin intermediul aplicației mobile și este esențial pentru a asigura transparența și conformitate legală;
- Clientul confirmă acceptarea "Regulilor de solicitare a creditului pentru Persoane Fizice prin intermediul aplicației mobile a Băncii și își exprimă acordul cu privire la prelucrarea de către Bancă a datelor sale cu caracter personal în scopul formulării unei oferte de credit. Acceptul clientului este validat prin bifarea unei căsuțe de confirmare și apăsarea butonului de solicitare a ofertei, pentru continuarea procesului. În caz contrar, sistemul nu va permite accesarea pașilor următori.

7.11.3 Procesarea Cererii clientului

- Sistemul inițiază un proces automatizat. Acesta implică analiza istoricului de credit, veniturilor și altor date financiare relevante;

- În funcție de rezultatul evaluării, clientul este informat despre disponibilitatea sau indisponibilitatea ofertei de credit;
- Dacă clientul este eligibil pentru produsul creditar și decizia Băncii este una pozitivă, acestuia i se prezintă detaliile cu privire la creditul pe care îl poate solicita prin intermediul aplicației mobile: suma maximă aprobată, perioada de rambursare, rata dobânzii efective (DAE), plata lunară estimativă spre achitare, data primei plăți și alte detalii după caz;
- Clientul are posibilitatea, în limita ofertei, să modifice suma, termenul și data de achitare în corespundere cu nevoile sale financiare. După ce se alege suma și termenul creditului, solicitantul va confirma opțiunile selectate, prin tastarea butonului ”Solicitați credit” astfel fiind direcționat la următoarea etapă.
- În cazul indisponibilității ofertei de credit în aplicația mobilă, Solicitantul are dreptul să solicite și să primească detalii în legătură cu solicitarea sa de credit și decizia Băncii în legătură cu aceasta, adresându-se la oricare dintre sucursalele Băncii.

7.11.4 **Selectarea Cardului și Acceptarea Informațiilor Precontractuale**

- La următorul pas, clientul selectează cardul și contul aferent pe care dorește să fie debursată suma creditului și pe care va efectua ulterior rambursările pentru credit. Clientul vizualizează, în interfața aplicației mobile, informațiile standard privind creditul pentru consumatori precum și informația preliminară cu privire la sumele și datele (perioadele) de plată conform contractului de credit sub forma unui grafic, având posibilitatea de descărcare a acestor documente pe dispozitivul mobil al acestuia. De asemenea, pentru a continua procesul, clientul acceptă reducerea termenului de furnizare a informațiilor standard privind creditul pentru consumatori. Dacă clientul nu acceptă reducerea termenului respectiv, nu va fi posibilă continuarea procesului de obținere a creditului prin intermediul aplicației mobile a Băncii, clientul urmând să se adreseze la una din sucursalele Băncii pentru a încheia și semna contractul de credit.
- După ce clientul confirmă că a luat cunoștință de Informațiile precontractuale și graficul preliminar de rambursare și acceptă reducerea termenului de furnizare a acestora, prin bifarea căsuței corespunzătoare, Clientul va vizualiza în interfața aplicației Contractul de credit.

7.11.5 **Generarea și Încheierea Contractului de Credit**

- Contractul de credit este generat automat în aplicație pe baza datelor introduse și acceptate anterior de client;
- Clientul are posibilitatea de a citi contractul de credit în detaliu. Acesta include toate clauzele contractuale, obligațiile părților, graficul de rambursare și alte condiții relevante;
- În scopul încheierii contractului de credit, clientul își va exprima consimțământul prin una din următoarele metode:
 - prin aplicarea autentificării stricte a clientului (SCA) configurat pe dispozitivul declarat de încredere. Autentificarea se face prin codul unic personalizat de 5 cifre setat de Client sau prin autentificare cu factor biometric (amprentă digitală ori recunoaștere facială), în funcție de sistemul de operare al dispozitivului.
 - prin **Cod OTP și autentificare suplimentară cu amprentă digitală/recunoaștere facială**, tehnologie integrată în dispozitivul mobil, cu condiția ca să fie activată funcția touch id /FingerPrint sau Face ID și setată inclusiv pentru accesarea aplicației MICB Mobile Banking, în caz contrar prin **Cod OTP și apel telefonic din partea Băncii**, în cazul în care dispozitivul nu dispune de tehnologie touch id /FingerPrint sau Face ID sau dacă clientul anulează/refuză autentificarea suplimentară cu amprentă digitală/identificare facială.

7.11.6 **Finalizarea Procesului și Debursarea Creditului**

- Validarea cu succes a factorului SCA sau a codului OTP, reprezintă încheierea Contractului de credit.
- Până la debursarea creditului, clientul poate fi contactat, prin apel telefonic, de un reprezentant al Băncii, pentru identificare suplimentară. Dacă angajatul Băncii, în urma apelului telefonic, va obține informații corecte și veridice cu privire la identitatea Clientului, mijloacele bănești vor fi debursate la contul de card al Clientului.
- În situația în care angajatul Băncii va avea suspiciuni cu privire la identitatea Clientului, suma creditului nu se va debursa în contul de card al acestuia. În acest caz, pentru a obține creditul solicitat, Clientul va fi informat că poate vizita oricare sucursală a Băncii pentru a-și confirma intenția de obținere a creditului.
- Odată ce creditul este debursat, Clientul poate consulta, din meniul principal, detaliile actualizate și documentele aferente creditului.

7.11.7 Încheierea contractelor de credit acordate prin intermediul partenerilor

- Pentru cererile de credit inițiate prin intermediul partenerilor, în cazul în care acestea au fost aprobate de Bancă, Clientul Băncii, care corespunde criteriilor de eligibilitate, are posibilitatea de a încheia contractul de credit destinat achiziționării bunurilor/serviciilor de la parteneri, direct din aplicația mobilă.
- Clientul va primi o notificare privind disponibilitatea contractului spre semnare și va accesa aplicația mobilă.
- În interfața deschisă, Clientul vizualizează detaliile și informațiile aferente creditului aprobat care includ: denumirea partenerului, suma, termenul, rata lunară de plată, data primei plăți, precum și DAE (dacă creditul implică costuri).
- Clientul confirmă acceptarea Regulilor de încheiere a contractului de credit prin intermediul aplicației mobile a Băncii, a informațiilor precontractuale și a reducerii termenului de furnizare a acestora precum și a graficului preliminar de rambursare.
- În cazul în care se solicită deschiderea unui nou cont, Clientul, suplimentar, confirmă cererea de deschidere a contului și recepționarea formularului privind informarea deponenților și acceptă Tarifele și Condițiile generale bancare pentru persoane fizice.
- Acceptul Clientului este validat prin bifarea căsuțelor de confirmare.
- Clientul va vizualiza, în interfața aplicației, proiectul Contractului de credit, informația cu privire la sumele și datele (perioadele) de plată conform contractului de credit sub forma unui grafic și Cererea de deschidere a contului curent, sub forma unui fișier PDF unic. Solicitantul își va exprima consimțământul de a încheia Contractul de credit și va confirma Cererea de deschidere a contului curent, prin utilizarea instrumentelor de Autentificare Strictă a Clienților (SCA).
- Finalizarea cu succes a Autentificării stricte a clientului (SCA) reprezintă încheierea Contractului de credit și, implicit, manifestarea neechivocă a consimțământului Clientului de a intra în respectiva relație contractuală, următoarea etapă fiind debursarea mijloacelor bănești și eliberarea bunului/prestarea serviciului de către partener.
- Clientul poate ulterior consulta detaliile actualizate și actele aferente creditului contractat în MICB Mobile Banking, direct din meniul principal al aplicației, disponibile în acest format până la achitarea integrală a creditului.

7.12 Constituirea, vizualizarea și gestionarea Depozitelor în IPAD MICB Mobile Banking

Procesul de constituire și gestionare a depozitelor prin aplicația MICB Mobile Banking este structurat în mai multe etape ce asigură un flux intuitiv și comod pentru Deponent.

7.12.1. Inițierea procesului de constituire a depozitului online

- Un cont de depozit poate fi deschis doar dacă potențialul deponent deține un cont curent, inclusiv cont de card activ în aceeași valută ca cea a depozitului.
- Deponentul selectează tipul de depozit în funcție de nevoile sale financiare din cele puse la dispoziție și ulterior este redirecționat către o pagină care prezintă detaliile produselor de depozit disponibile. Aceasta va include informații despre tipul depozitului, termenul, rata dobânzii, frecvența plății dobânzii, cu sau fără capitalizare, precum și opțiunile de completare și/sau retragere,;
- În această interfață Deponentul va selecta contul curent/cardul din care vor fi transferate mijloacele bănești pentru constituirea/restituirea depozitului și contul curent/cardul pentru primirea dobânzilor;
- Deponentul va fi informat cu Condițiile Generale Bancare pentru persoane fizice, Tarifele și Informația privind garantarea depozitelor, fiindu-i puse la dispoziție toate informațiile necesare, cu posibilitatea de a dispune de timp suficient pentru a citi fiecare document. Aplicația va oferi opțiunea de a deschide fiecare document într-o fereastră separată pentru a le vizualiza și salva;
- Prin bifarea căsuțelor de acceptare, Deponentul confirmă că este de acord cu condițiile și informațiile sus menționate;
- După selectarea căsuțelor de acceptare, Deponentul va accesa opțiunea de constituire a depozitului.

7.12.2. Finalizarea și Confirmarea constituirii depozitului în aplicația mobilă

- Pentru a finaliza și autoriza constituirea depozitului, Deponentul își exprimă consimțământul prin aplicarea Autentificării Stricte a Clientului (SCA);
- După aplicarea autentificării stricte a clientului (SCA) de către utilizator, contractul de depozit se consideră încheiat și contul de depozit constituit;
- Ulterior încheierii contractului, clientul este informat că depozitul a fost deschis;
- Pe pagina principală a aplicației, deponentul va putea vizualiza lista conturilor de depozit deținute, inclusiv cele constituite la sucursala Băncii, și va avea opțiunea de a accesa detaliile fiecărui depozit, iar pentru depozitele constituite în aplicația mobilă vor fi disponibile pentru vizualizare contractele de depozit și actele aferente.

7.12.3. Completarea depozitelor în aplicația mobilă

- Deponenții care au deschis/constituit un depozit ce permite completarea, pot accesa opțiunea de completare direct din detaliile depozitului.
- La selectarea opțiunii de completare, deponentul va fi redirecționat către o pagină dedicată, unde va alege contul curent sau cardul din care se vor transfera fondurile, va introduce suma dorită pentru completare, respectând condițiile prevăzute de produs și va confirma efectuarea transferului.
- Completarea depozitelor va fi posibilă atât pentru depozitele constituite prin intermediul aplicației mobile, cât și pentru cele deschise la în sucursalele Băncii, în conformitate cu condițiile produsului.

7.12.4. Retragera parțială din depozite prin intermediul aplicației mobile

- Pentru depozitele care permit retragerea parțială a mijloacelor bănești conform Condițiilor depozitelor persoanelor fizice în vigoare, Deponentul va avea opțiunea de a selecta această funcționalitate, accesând detaliile depozitului;
- Deponentul va introduce suma dorită pentru retragere, în limitele prevăzute de produs, va selecta contul curent sau cardul pe care dorește să primească mijloacele bănești și va iniția retragerea prin tastarea butonului corespunzător;
- Retragerile parțiale din contul de depozit se autorizează prin aplicarea autentificării stricte a clientului (SCA).
- Efectuarea retragerilor parțiale, va fi posibilă atât pentru depozitele constituite prin intermediul aplicației mobile, cât și pentru cele deschise în sucursalele Băncii, în conformitate cu Condițiile depozitelor persoanelor fizice în vigoare.

7.12.5. Prelungirea și închiderea depozitului în aplicația mobilă

- Depozitele care includ opțiunea de prelungire automată, inclusiv depozitele deschise la o sucursală a Băncii, vor fi prelungite automat în ziua următoare după data scadenței, pentru o nouă perioadă, conform condițiilor în vigoare aplicabile depozitelor pentru persoane fizice la data prelungirii;
- Pentru depozitele cu prelungire automată, utilizatorul poate dezactiva/reactiva opțiunea de auto prelungire direct din aplicația mobilă, prin accesarea detaliilor depozitului și selectarea opțiunii de dezactivare/reactivare a auto prelungirii.
- În cazul dezactivării auto prelungirii, depozitul se va închide automat la data scadenței. Dezactivarea/reactivarea auto prelungirii nu este posibilă în ultima zi a termenului depozitului.
- Pentru depozitele care nu prevăd condiția de prelungire automată, în ziua următoare după data scadenței, acestea se închid automat. Soldul contului de depozit se transferă la contul de gestionare a depozitului.

7.13. Deschidere card de plată în format digital în aplicația MICB Mobile Banking

- 7.13.1 Funcționalitatea de emitere a cardului în format digital prin aplicația MICB Mobile Banking este disponibilă exclusiv clienților existenți, persoane fizice, care îndeplinesc criteriile de eligibilitate stabilite de Bancă.
- 7.13.2 Utilizatorul are posibilitatea să solicite emiterea unui card digital, ce va fi atașat unui cont nou deschis.
- 7.13.3 Cardurile digitale pot fi emise în lei moldovenești (MDL), euro (EUR) sau dolari americani (USD).
- 7.13.4 Prin accesarea funcționalității, utilizatorului îi sunt prezentate: tipul de card disponibil pentru emitere, beneficiile aferente, posibilitatea activării serviciului SMS Notificări, precum și tarifele aplicabile.
- 7.13.5 Utilizatorul consultă Condițiile Generale Bancare, Limitele și Tarifele aplicabile, informațiile privind garantarea depozitelor, iar acceptarea acestora este confirmată prin bifarea căsuței de acceptare.
- 7.13.6 Deschiderea cardului digital este autorizată prin aplicarea Autentificării Stricte a Clientului(SCA).
- 7.13.7 Odată ce cardul digital a fost emis, utilizatorul este notificat despre deschiderea cu succes a cardului.
- 7.13.8 Codul PIN aferent cardului este transmis prin SMS la numărul de telefon înregistrat în sistemul Băncii și poate fi modificat de utilizator direct din IPAD MICB Mobile Banking.
- 7.13.9 Cardul digital este activ și disponibil în IPAD MICB Mobile Banking, iar toate datele și serviciile aferente cardului sunt accesibile similar cardurilor emise fizic.
- 7.13.10 Cardul virtual (digital), poate fi înrolat în portofelele Apple Wallet, Google Wallet și Garmin pentru efectuarea plăților.
- 7.13.11 Reemiterea, închiderea cardului/contului poate fi efectuată doar în cadrul unei sucursale/agenție a Băncii, la cererea utilizatorului.

7.14. Serviciul de transfer SEPA

- 7.14.1 Pentru a iniția un transfer SEPA prin intermediul aplicației mobile, plătitorul trebuie să îndeplinească cumulativ următoarelor condiții:
- Să fie utilizator al aplicației MICB Mobile Banking;
 - Să dețină un cont de card activ în Euro;
 - Să aibă actualizate datele personale în sistemul Băncii.

- 7.14.2 Transferul SEPA poate fi executat exclusiv din contul de card în Euro. În cazul în care clientul nu deține cont în Euro, acesta poate deschide un card digital în Euro, după cum este descris în p.7.13.
- 7.14.3 Transferul poate fi efectuat doar către conturi deschise la instituții bancare din spațiul SEPA care a aderat la schema de plată SEPA;
- 7.14.4 Pentru a iniția un transfer, utilizatorul deschide pagina dedicată Plăți și transferuri din meniul rapid Plăți sau din meniul principal, selectează opțiunea **SEPA Transferuri în euro** și completează câmpul dedicat cu IBAN-ul Beneficiarului;
- 7.14.5 Sistemul verifică și validează IBAN-ul introdus, iar utilizatorul selectează tipul plății din lista predefinită.
- 7.14.6 În interfața afișată, utilizatorul completează datele beneficiarului, care includ: nume, prenume sau denumire companie (în cazul persoanelor juridice), țara de reședință, orașul și opțional tipul și numărul documentului/identificatorului beneficiarului plății.
- 7.14.7 Ulterior completării datelor beneficiarului, utilizatorul alege contul sursă în Euro, introduce suma transferului și alege destinația transferului din lista prestabilită. În cazul destinațiilor care necesită justificarea plății (ex: procurarea de bunuri și servicii), utilizatorul va indica numărul și data documentului aferent (ex: contract, factură) în câmpurile dedicate.
- 7.14.8 După completarea tuturor datelor, utilizatorul autorizează tranzacția prin aplicarea autentificării stricte a clientului (SCA).
- 7.14.9 După validarea factorului de autentificare strictă a clientului (SCA), utilizatorul va vizualiza interfața cu detaliile transferului efectuat .
- 7.14.10 Transferurile SEPA se procesează doar în zile lucrătoare, în conformitate cu graficul de acceptare a ordinelor de plată în valută străină, prevăzut în Condițiile de efectuare a transferurilor internaționale.
- 7.14.11 Comisioanele și limitele aferente transferurilor SEPA se aplică conform Tarifelor în vigoare aplicabile persoanelor fizice.

8. Serviciile non-financiare ale IPAD, MICB Mobile Banking

- 8.1. Serviciile non-financiare ale IPAD MB 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:**
- 8.2.3.1. Afișează lista tranzacțiilor efectuate prin intermediul Sistemului;
- 8.2.3.2. 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:**
- 8.2.4.1. Afișează lista tranzacțiilor efectuate cu utilizarea Cardului selectat, în Sistem și în afara acestuia.
- 8.2.4.2. 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.
- 8.2.6. **Datele bancare ale cardului:**
- Aplicația mobilă oferă posibilitatea vizualizării datelor cardului (numărul din 16 cifre, data expirării cardului și CVV2/CVC2-ul);
 - Datele cardului (numărul din 16 cifre), numele și prenumele deținătorului pot fi distribuite direct din aplicație prin intermediul posibilității de partajare, inclusiv prin aplicațiile de mesagerie și email;
- 8.3. CVV2/CVC2-ul cardului poate fi vizualizat direct din aplicație prin aplicarea Autentificării Stricte a Clientului (SCA).
- 8.4. **Serviciile de gestionare a cardurilor / conturilor Abonatului:**
- 8.4.1. **Blocarea cardului:**

8.4.1.1. Utilizarea acestui Serviciu duce la blocarea Cardului;

8.4.1.2. În rezultatul utilizării acestui Serviciu, clientul transmite Băncii Document electronic cu statut de cerere de blocare a Cardului;

8.4.1.3. În funcție de tipul blocării solicitat (card pierdut, furat sau altă cauză), cardul este blocat permanent sau temporar;

8.4.1.4. Clientul este informat despre blocarea cardului prin interfața IPAD MB.

8.4.2. **Deblocarea cardului:**

8.4.2.1. Utilizarea acestui Serviciu duce la deblocarea Cardului blocat anterior prin Serviciul „Blocarea cardului”, cu aplicarea autentificării stricte a clientului (SCA).

8.4.2.2. În rezultatul utilizării acestui Serviciu, clientul transmite Băncii Document electronic cu statut de cerere de deblocare a Cardului.

8.4.2.3. Deblocarea este posibilă doar pentru cardurile blocate temporar.

8.4.3. **Activarea serviciului „ Protecția cardului” (Fereastra tranzacțională):**

8.4.3.1. Utilizarea acestui Serviciu permite Abonatului să dețină securitate avansată asupra cardurilor sale;

8.4.3.2. 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;

8.4.3.3. 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.

8.4.4. **Dezactivarea serviciului „ Protecția cardului”(Fereastra tranzacțională):**

8.4.4.1. 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 IPAD MB a avut loc printr-o modalitate de autentificare diferită de utilizarea Codului de acces. În cazul în care pentru autentificarea în IPAD MB se utilizează Codul de acces, dezactivarea serviciului „ Protecția cardului” nu necesită autentificare adițională.

8.5. Serviciul „Modificare PIN”

Serviciul „Modificare PIN” oferă utilizatorilor posibilitatea de a schimba PIN-ul prin intermediul aplicației mobile „MICB Mobile Banking”. Modificarea PIN-ului se efectuează prin următoarea modalitate:

- Utilizatorul deschide aplicația mobilă „MICB Mobile Banking” și selectează cardul pentru care dorește să modifice PIN-ul;
- Utilizatorul selectează serviciul „Modificare PIN” și introduce noul PIN, cu respectarea cerințelor de securitate (lungimea minimă a PIN-ului și utilizarea cifrelor);
- Utilizatorul confirmă repetat noul PIN;
- Pentru asigurarea securității serviciului, utilizatorul autorizează acțiunea prin aplicarea Autentificării Stricte a Clientului (SCA). După aplicarea Autentificării Stricte a Clientului (SCA), utilizatorul va fi informat direct în aplicația mobilă că codul PIN a fost modificat cu succes. Suplimentar, utilizatorul va fi informat prin serviciul „Push notificari” sau prin serviciul „SMS notificări”, dacă are conectate aceste servicii

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

8.6.1. Generarea parolei de tip „Mobile OTP” se efectuează prin intermediul meniului „Generarea parolei de unică folosință” din interiorul IPAD MICB Mobile Banking;

8.6.2. Generarea parolei de tip „Mobile OTP” este posibilă doar în cazul accesării IPAD MICB Mobile Banking prin Codul de acces (5 cifre);

8.6.3. Ca bază pentru generarea parolei de tip „Mobile OTP” va fi utilizat codul tranzacției afișat în E-Commerce (3D Secure);

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

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

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

8.7.1. **Modificarea parolei:**

8.7.1.1. Utilizarea acestui Serviciu duce la modificarea Parolei;

8.7.1.2. 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.).

8.8. Serviciul de gestiune a șabloanelor și Plăților programate:

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

8.8.1.2. **Plăți programate** - presupune efectuarea unor plăți periodice cu o regularitate și sumă 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 transferul mijloacelor bănești (de ex: [P2P MICB.](#));

8.9. Limite tranzacționale:

- 8.9.1.1. Utilizarea acestui Serviciu permite Abonatului să gestioneze anumite limite aferente cardului / cardurilor sale pentru diferite tipuri de operațiuni sau să interzică complet unele operațiuni;
- 8.9.1.2. Setarea limitelor tranzacționale protejează Abonatul de fraude și alte riscuri;
- 8.9.1.3. La setarea limitelor tranzacționale, are loc limitarea operațiunilor pentru anumite tranzacții.

8.10. Serviciul „SMS-Notificări”:

- 8.10.1.1. Utilizarea acestui serviciu permite abonatului să primească notificări prin SMS despre tranzacțiile efectuate pe conturile de card proprii pentru care este activat serviciu;
- 8.10.1.2. Banca oferă Clientului posibilitate de dezabonare de la Serviciu „SMS-notificări”.
- 8.10.1.3. Serviciul se utilizează în conformitate cu [Condițiile de prestare a serviciului „SMS-Notificări” și a altor mesaje de notificare.](#)

8.11. Opțiunea „Push-Notificări”:

- 8.10.1. Utilizarea acestei opțiuni permite abonatului să primească pe ecranul telefonului mesaje de notificare despre tranzacțiile efectuate pe conturile de card proprii pentru care este activată această opțiune;
- 8.10.2. Banca oferă clientului posibilitatea de activare sau dezactivare a acestei opțiuni în setările aplicației.
- 8.10.3. Livrarea notificărilor Push:
- sunt livrate indiferent de faptul utilizării serviciului SMS-Notificări;
 - sunt livrate dacă este acces la rețeaua internet;
 - sunt livrate doar pentru notificarea Clientului despre tranzacțiile efectuate. Mesajele destinate protejării securității (SMS OTP), se vor expedia doar prin SMS, indiferent de setările aferente opțiunii notificărilor Push sau a serviciului SMS-Notificări;
 - notificările Push dacă din careva motive nu vor putea fi expediate clientului, sistemul va efectua repetat tentativa de expediere a acestei notificări. În cazul eșuării tuturor tentativelor, sistemul va expedia SMS-notificare doar acelor clienți care sunt abonați la serviciul SMS-Notificări în conformitate cu *“Tarifele privind deservirea cardurilor bancare emise de BC Moldindconbank S.A.”.*

8.12. Serviciul „Localizarea geografică”:

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”.

8.13. Captarea automată „SMS OTP”:

- 8.13.1.1. Utilizarea acestei opțiuni permite abonatului extragerea automată a parolei de unică folosință din mesajul SMS primit la numărul de telefon mobil fără a fi necesară introducerea manuală a acestei parole în interfața IPAD MB. Această opțiune se activează de către abonat din meniul IPAD MICB Mobile Banking.

8.14. Captarea datelor cardului prin scanarea cu telefonul mobil/dispozitivul mobil:

- 8.14.1. Utilizarea acestei opțiuni permite abonatului scanarea cu telefonul mobil/dispozitivul mobil a datelor cardului la efectuarea operațiunii de abonare la IPAD MICB Mobile Banking, la efectuarea unei tranzacții de tip P2P de pe cardul personal pe orice alt card emis de Bancă, altă bancă din Republica Moldova sau străinătate.
- 8.14.2. Pentru scanarea datelor de card se utilizează biblioteca card.io. În cazul unor imagini complexe din zona numărului de card sau în cazul în care datele de card nu sunt eboșate sau eboșate fără evidențierea culorii de pe numărul de card, atunci scanarea nu va putea fi efectuată, aceasta fiind limitarea tehnică a bibliotecii. Opțiunea de scanarea a datelor de card funcționează doar pentru cardurile care conține un număr de caractere egal cu 16.

8.13. Atașarea cardului în aplicația Apple Pay:

- 8.15.1. Utilizarea acestui serviciu permite abonatului prin intermediul aplicației MICB „Mobile Banking” atașarea cardului pe platforma de plată oferită de Apple Distribution International - Apple Pay. Acest serviciu poate fi utilizat de abonat după abonarea/autentificarea cu succes în IPAD MICB Mobile Banking.
- 8.15.2. Serviciul se utilizează în conformitate cu *Termeni și Condiții de atașare a cardurilor emise de BC „Moldindconbank” S.A. în portofele electronice.*

8.16. Atașarea cardului în aplicația Google Pay:

- 8.16.1. Utilizarea acestui serviciu permite abonatului prin intermediul aplicației MICB Mobile Banking atașarea cardului pe platforma de plată oferită de Google Ireland Limited - Google Pay. Acest serviciu poate fi utilizat de abonat după abonarea/autentificarea cu succes în IPAD MICB Mobile Banking.
- 8.16.2. Serviciul se utilizează în conformitate cu *Termeni și Condiții de atașare a cardurilor emise de BC „Moldindconbank” S.A. în portofele electronice.*

8.17. Serviciul Actualizare Date destinat clienților existenți

- 8.17.1. Serviciul de actualizare a datelor prin intermediul aplicației MICB Mobile Banking permite clientului rezident, a căror date au rămas neschimbate de la ultima actualizare în sistemul Băncii și care corespund criteriilor de eligibilitate, să confirme informațiile personale declarate în scopul actualizării.

8.17.2. Serviciul este disponibil în conformitate cu *Termeni și Condiții de actualizare a datelor online prin intermediul IPAD MICB Mobile Banking* și este structurat în câteva etape.

8.17.3. Inițierea procesului de „Actualizare Date”

8.17.3.1. La autentificarea în IPAD MICB Mobile Banking, Clientul poate accesa, din meniul principal, modulul Profil, de unde poate accesa serviciul „Actualizarea Datelor”, pentru a confirma datele înregistrate în sistemul Băncii, cu condiția ca acestea să nu fi suferit modificări pe parcursul relației de afaceri.

8.17.3.2. Clientul va confirma îndeplinirea criteriilor de eligibilitate, declarând că nu are statut de subiect FATCA, nu este o persoană expusă și asociată politic (PEP), nu este rezident fiscal într-o jurisdicție supusă raportării CRS și că este beneficiarul efectiv al operațiunilor efectuate.

8.17.3.3. Înainte de transmiterea solicitării de verificare a datelor, Clientul are obligația de a citi și de a înțelege Termenii și Condițiile privind actualizarea datelor online, precum și informațiile referitoare la politica de prelucrare a datelor cu caracter personal.

8.17.4. Verificarea eligibilității Clientului și confirmarea datelor personale

8.17.4.1. Ulterior confirmării corespunderii criteriilor de eligibilitate, sistemul inițiază procesul de comparare și verificare a datelor înregistrate în sistemul Băncii cu informațiile disponibile în Registrul de Stat al Populației.

8.17.4.2. În cazul care sistemul Băncii identifică că datele sunt diferite, procesul va fi stopat, iar Clientul va primi o notificare prin care va fi informat că actualizarea va fi posibilă de efectuat doar în cadrul sucursalei Băncii.

8.17.4.3. Dacă toate informațiile obținute din Registrul de stat al populației (nume, prenume, IDNP, data, luna și anul nașterii, serie și număr act de identitate, autoritatea emitentă, locul nașterii, data emiterii și expirării actului de identitate, cetățenia, adresa de domiciliu și de reședință) sunt identice cu cele declarate de Client în Chestionar și pe care banca le deține, sistemul Băncii va genera Clientului solicitarea de confirmare și validare a acestora. În interfața generată de aplicația Băncii, clientul va verifica și valida datele din actul de identitate, numărul de telefon, fiind exclusă posibilitatea de modificare manuală a acestora.

8.17.4.4. În cazul în care, după contrapunerea și verificarea datelor, clientul va identifica neconcordanțe, va putea selecta opțiunea că Datele nu corespund și procesul va fi stopat, iar utilizatorul va primi notificare că actualizarea va fi posibilă de a fi efectuată în cadrul sucursalei Băncii.

8.17.4.5. Ulterior validării datelor din actul de identitate, clientul va verifica și confirma adresa de domiciliu, având posibilitatea de a introduce manual adresa curentă în cazul în care aceasta diferă de adresa de domiciliu. Ulterior, acesta va confirma sau modifica informațiile legate de locul de muncă și va selecta din liste prestabilite detalii despre tipul operațiunilor efectuate, natura și volumul tranzacțiilor, sursa veniturilor.

8.17.4.6. Chestionarul se va încheia cu etapa în care utilizatorul va confirma corectitudinea datelor introduse.

8.17.5. Finalizarea confirmării datelor în scopul actualizării chestionarului

8.17.5.1. Pentru a finaliza procesul de confirmare și actualizare a datelor, utilizatorul va autoriza acțiunea prin aplicarea autentificării stricte a clientului (SCA).

8.17.5.2. După introducerea și validarea factorului de autentificare strictă a clientului (SCA), se va genera chestionarul și clientul va primi o notificare că validarea datelor în sistem este în curs de procesare;

8.17.5.3. La finalizarea verificării datelor în sistem, utilizatorul va fi notificat că procesul de actualizare a datelor a fost finalizat cu succes.

8.18. Gestionarea acordurilor de marketing și comunicare

8.18.1. Utilizatorul poate activa opțiunea de primire a ofertelor promoționale din partea Băncii prin canalele de comunicare disponibile (e-mail, SMS, canale digitale etc.) precum și opțiunea privind primirea ofertelor personalizate și crearea de profiluri din meniul aplicației, compartimentul **Setări**, secțiunea **Notificări**.

8.18.2. Fiecare opțiune poate fi activată sau retrasă individual, oricând în mod independent, din meniul aplicației, compartimentul **Setări**, secțiunea **Notificări**.

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 IPAD MB 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 IPAD MB, 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 IPAD MB 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 (după caz) 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 IPAD 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 IPAD “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, Condițiile Generale Bancare pentru persoane fizice, Instrucțiunea de utilizare MICB Mobile Banking înainte abonării la IPAD MB și să utilizeze Sistemul în strictă conformitate cu prevederile acestora;
- 9.3.2. să acceseze IPAD MB numai cu ajutorul Telefonului mobil/ dispozitivului mobil care corespunde cerințelor indicate în Instrucțiunea de utilizare „MICB Mobile Banking”;
- 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 IPAD MB 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 IPAD 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 24/24 sau la ghișeele Băncii) imediat ce constată:
- 9.3.7.1. modificarea neautorizată a soldului contului bancar;
- 9.3.7.2. orice eroare sau neregulă apărută în urma gestionării de către Bancă a contului bancar;
- 9.3.7.3. elementele ce creează suspiciuni cu privire la posibilitatea cunoașterii de către persoane neautorizate a factorilor de autentificare deținute de Abonat;
- 9.3.7.4. disfuncționalități ale Sistemului sau dacă parolele primite sunt incorecte;
- 9.3.8. să manifeste o atitudine responsabilă privind asigurarea siguranței și securității IPAD MB;
- 9.3.9. de a nu permite înregistrarea în dispozitiv, a amprentelor digitale altor persoane respectiv a altor imagini faciale în cazul Face ID, având în vedere că, accesarea MICB Mobile Banking și autorizarea tranzacțiilor s-ar putea realiza cu oricare dintre datele biometrice adăugate în dispozitiv.
- 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 de utilizare “MICB Mobile Banking”, 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:
- 9.5.1. 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;
- 9.5.2. pentru daunele suportate de client ca urmare a nerespectării recomandărilor de utilizare securizată a IPAD MICB Mobile Banking precum și închiderii incorecte a sesiunii de utilizare a sistemului;
- 9.5.3. dacă clientul este constrâns în orice mod să se autentifice în IPAD MICB Mobile Banking prin amprenta digitală sau Face ID fără consimțământul său;
- 9.5.4. dacă accesarea IPAD MICB Mobile Banking, autentificarea, autorizarea tranzacțiilor s-a realizat de către o persoană terță cu amprenta digitală sau Face ID înregistrată în dispozitivul clientului.

10. Responsabilitatea Părților și ordinea repartizării pierderilor

- 10.1. Clientul este responsabil de păstrarea securității și confidențialității Login-ului, Factorilor de autentificare și factorilor de autentificare strictă SCA și va întreprinde toate măsurile necesare pentru prevenirea accesului neautorizat și compromiterea acestora.
- 10.2. Clientul este responsabil de utilizarea corespunzătoare și securizată a dispozitivului utilizat pentru accesarea aplicației MICB Mobile Banking și de protejarea acestuia împotriva pierderii, furtului, accesului neautorizat sau compromiterii. Clientul va lua măsuri rezonabile pentru a evita instalarea de aplicații malițioase, utilizarea dispozitivelor infectate sau nesecurizate, conectarea la rețele nesigure și accesul altor persoane la dispozitiv în timpul utilizării aplicației.
- 10.3. Banca nu poartă răspundere pentru tranzacțiile, operațiunile sau documentele transmise către Bancă și autorizate prin accesarea și utilizarea IPAD MICB Mobile Banking, prin utilizarea Login-ului, a Factorilor de autentificare sau a factorilor de autentificare strictă SCA, inclusiv în cazul utilizării frauduloase de către terțe persoane, dacă compromiterea acestora s-a produs ca urmare a acțiunilor, inacțiunilor, neglijenței sau comportamentului fraudulos al Clientului. Aceasta include, fără a se limita la, divulgarea datelor de securitate, utilizarea necorespunzătoare a dispozitivului sau autorizarea tranzacțiilor sub influența unor terțe persoane cu comportament fraudulos, până la notificarea Băncii și suspendarea mijloacelor de autentificare respective.
- 10.4. Clientul este responsabil de veridicitatea și corectitudinea informației introduse în Documentele electronice primite, completate și transmise spre prelucrare Băncii.
- 10.5. Clientul este responsabil pentru suficiența mijloacelor bănești la prelucrarea operațiunilor solicitate.
- 10.6. Clientul este responsabil de abonarea la serviciile "MICB Mobile Banking", atât la cele care au fost accesate conștient, cât și la cele accesate din neatenție, cât și de toate operațiunile efectuate prin intermediul acestora.
- 10.7. Banca nu este responsabilă pentru neexecutarea operațiunilor solicitate de Client și pierderile care pot apărea din motivul lipsei sau insuficienței mijloacelor bănești pe contul de card sau blocării cardului de plată, indiferent din ce motiv acesta a fost blocat.
- 10.8. Banca nu este responsabilă pentru imposibilitatea accesării/utilizării sistemului de plăți instant MIA care sunt cauzate de defecțiunile tehnice a platformei Băncii Naționale a Moldovei sau a participanților sistemului.
- 10.9. Banca și Clientul recunosc puterea juridică a Tranzacțiilor efectuate în cadrul Sesiunii de utilizare a IPAD MICB Mobile Banking.
- 10.10. 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.
- 10.11. Banca și Clientul recunosc faptul că Documentele electronice transmise în adresa Băncii în cadrul Sesiunii de utilizare a IPAD MICB Mobile Banking se echivalează cu cele perfectate de Client pe suport hârtie și produc aceleași drepturi și obligațiuni ale Părților.
- 10.12. Banca va lua toate măsurile necesare pentru prevenirea riscurilor ce pot apărea din utilizarea frauduloasă a IPAD MICB Mobile Banking. Banca este responsabilă:
 - 10.12.1. pentru neexecutarea sau executarea necorespunzătoare a Tranzacțiilor efectuate prin intermediul IPAD MB:
 - 10.12.1.1. în cazul în care executarea necorespunzătoare este atribuită unei disfuncționalități a IPAD MB sau a unei componente a acestuia, cu condiția că disfuncționalitatea nu a fost cauzată intenționat de către Abonat;
 - 10.12.1.2. 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.
 - 10.12.2. pentru Tranzacțiile electronice inițiate după momentul notificării Băncii de către Abonat a pierderii controlului asupra IPAD MB (de exemplu funcționării defectuoase a Sistemului, compromiterea parolelor sau a altor informații sensibile de către persoane neautorizate etc.);
 - 10.12.3. 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 IPAD MB, cu condiția că Abonatul a respectat toate prevederile contractuale de utilizare a IPAD MB.

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 (24/24 ore, 7 zile pe săptămână) la linia telefonică la numărul de telefon: /+373/ 22 71-71-71.
- 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, a tokenului SCA, obținerii consultațiilor privind utilizarea IPAD MICB Mobile Banking.

12. Dispozițiile finale

- 12.1. Relațiile dintre Bancă și Abonat care apar în rezultatul utilizării IPAD MICB Mobile Banking și care nu sunt specificate în prezentele Condiții de utilizare, vor fi reglementate în conformitate cu Condițiile Generale Bancare pentru persoane fizice și legislația în vigoare a Republicii Moldova.
- 12.2. Toate neînțelegerile și/sau litigiile apărute între Abonat și Bancă pe marginea utilizării IPAD 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).
- 12.4. Prezentele Condiții de utilizare a IPAD „MICB Mobile Banking” intră în vigoare la data de 26.05.2026
- 12.5. Din data intrării în vigoare a prezentelor Condiții se abrogă Condițiile de utilizare a Instrumentului de plată electronic cu acces la distanță „MICB Mobile Banking”, aprobate de către Comitetul de conducere al Băncii la 10.03.2026 proces verbal nr.15)