Termeni și Condiții specifice pentru utilizarea serviciului 3D Secure

I. Definiții:

În cuprinsul prezentelor Termeni și Condiții specifice pentru utilizarea serviciului 3D Secure prin cardurile emise de OTP Bank (denumite în continuare "Condiții specifice"), termenii menționați mai jos vor fi utilizați având următorul înteles:

Serviciul 3D Secure – este un standard de autentificare dezvoltat de Organizațiile Internaționale de Carduri VISA și Mastercard și acceptat la nivel global, care permite efectuarea tranzacțiilor cu cardul pe internet (E-Commerce) în condiții de strictă securitate, asigurând protecția deținătorilor în momentul autentificării. Sistemul de comerț electronic securizat este implementat pe site-urile comercianților sub denumirea „Mastercard Identity Check" pentru cardurile de tip Mastercard și „Verified by VISA" pentru cardurile VISA, și se pot identifica prin intermediul siglelor. Autentificarea tranzacțiilor prin serviciul 3D Secure se poate realiza prin: introducerea datelor biometrice (amprentă/recunoaștere facială), introducerea parolei dinamice transmisa prin SMS pe numărul de telefon mobil comunicat Băncii sau prin introducerea parolei statice insotita de parola dinamica transmisa prin SMS pe numărul de telefon mobil comunicat Băncii.
Aplicația SmartBank (denumită în continuare Aplicația sau SmartBank) – parte a serviciului OTPdirekt prin care Deținătorul/Utilizatorul Autorizat, își poate accesa conturile deținute la Bancă, poate efectua o serie de operațiuni bancare sau prin ecranul specific poate autentifica prin biometrie plățile efectuate pe Internet cu cardurile emise de OTP Bank Romania. Aplicația SmartBank este funcțională pe dispozitive cu sisteme de operare Android sau iOS.
Autentificare biometrică– informație de siguranța constând în una din următoarele metode de autentificare:

- *scanarea amprentei digitale* a Deținătorului/Utilizatorului Autorizat de către dispozitivul utilizat, citirea acesteia realizându-se de către tehnologia specifică dispozitivului. Această funcționalitate este disponibilă numai pentru modelele de dispozitive care permit și au încorporată tehnologia specifică scanării amprentei digitale;
- *recunoașterea facială* a Deținătorului/Utilizatorului Autorizat de către dispozitivul utilizat, citirea acesteia realizându-se de către tehnologia specifică dispozitivului. Această funcționalitate este disponibilă numai pentru modelele de dispozitive care permit și au încorporată tehnologia specifică scanării trăsăturilor faciale.

Banca – este reprezentată de OTP BANK ROMANIA S.A (denumită în continuare Banca sau OTP Bank), așa cum este identificată în Condițiile Generale de Afaceri / Condițiile Generale de Afaceri Persoane Juridice și Categorii Asimilate și cu dispozițiile condițiilor contractuale de emitere carduri specifice fiecărei categorii / tip de produs (card de debit, card de credit).
Romcard – furnizor extern care oferă servicii de autentificare 3D Secure în cadrul procesului de efectuare plăți online prin intermediul cardurilor OTP Bank România.
Card – card de debit/card de credit, emis de OTP Bank România prin intermediul căruia se pot efecuta tranzacții pe Internet (E-Commerce).
Condiții specifice – prezentul document contractual conținând condițiile specifice de utilizare a serviciului 3D Secure pentru cardurile emise de OTP Bank.
Deținător – titularul contului de Card, care a solicitat Băncii emiterea unui Card principal prin semnarea Cererii-Contract de Emitere pe numele căruia Banca a emis Cardul Principal.
Utilizator Autorizat – este acea persoană fizică pentru care Deținătorul a solicitat și Banca a dispus emiterea unui Card suplimentar cu acces la contul de card al Deținătorului.

Notificare de tip "push" – presupune trimiterea de mesaje de tip pop-up pe dispozitivele ce dețin instalată aplicația SmartBank cu scopul de a informa asupra faptului că este necesară aprobarea tranzacțiilor online efectuate de către Deținator/Utilizator Autorizat prin biometrie.
Parolă dinamică – este o parolă unică primită de către Deținător/Utilizator Autorizat prin SMS pe numărul de telefon mobil comunicat Băncii prin intermediul căreia se pot autentifica tranzacțiile online efectuate cu cardul prin serviciul 3D Secure.
Parola statică – este o parolă formată dintr-o informație cunoscută și la îndemana Deținătorului/Utilizatorului Autorizat fiind parte din procesul de autentificare a tranzacțiilor online efectuate cu cardul prin serviciul 3D Secure.

II. Aplicarea condițiilor specifice

1. Prezentele Condiții specifice reglementează aspectele particulare privind utilizarea serviciului 3D Secure pentru efectuarea tranzacțiilor online cu cardurile emise de OTP Bank, prin intermediul autentificării biometrice prin aplicația SmartBank sau prin SMS transmis pe numărul de telefon mobil declarat Băncii.
2. Pentru Cardurile utilizate pentru tranzacțiile online autentificate prin serviciul 3D Secure, prezentele Condiții specifice se completează cu dispozițiile Condițiilor Generale de Afaceri ale Bancii și Condițiilor Contractuale de emitere Carduri.
3. Prezentele Condiții specifice nu reglementează achiziția de servicii/produse sau plata și livrarea acestora, efectuată de Deținator/Utilizator Autorizat cu comercianții online.
   Acești comercianți sunt terți față de Bancă și își reglementează prin propriile condiții contractuale furnizarea serviciilor/vânzarea produselor. Deținătorul/Utilizatorul Autorizat se va supune condițiilor contractuale stabilite de acești comercianți atunci când contractează servicii/produse de la ei, când le vizitează site-urile sau când le oferă acestora informații despre persoana sa. Banca nu răspunde pentru legalitatea furnizării/prestării acestor produse/servicii și nici pentru securitatea, precizia, legalitatea sau orice alt aspect privind respectivele produse/servicii oferite de acești terți. Deținătorul/Utilizatorul Autorizat este responsabil să citească, să înțelegă și să accepte prevederile contractelor puse la dispoziție de acești terți înainte de a utiliza cardurile emise de Bancă pe site-urile acestora.
4. Banca nu este răspunzătoare și nu oferă suport sau asistență pentru hardware, software sau alte produse sau servicii ale terților, cum ar fi spre exemplu dispozitivul pe care este instalată aplicația SmartBank. Orice întrebari sau probleme în legatură cu dispozitivul, se vor adresa respectivului furnizor/terț.
5. Funcțiile si funcționalitatea aplicației SmartBank pot fi îmbunătățite sau actualizate fără vreo notificare prealabilă.
6. Condițiile specifice sunt comunicate Deținătorului/ Utilizatorului Autorizat în cadrul procesului de activare a funcției de autentificare tranzacții online prin utilizarea metodelor biometrice (scanare amprentă, recunoaștere facială), prin aplicația SmartBank și pot fi consultate pe site-ul Bancii https://www.otpbank.ro. Banca poate modifica oricând prezentele Condiții specifice, urmând să le facă publice pe site-ul Băncii https://www.otpbank.ro. Utilizarea aplicației după data intrării în vigoare a modificărilor va fi considerată acceptare a noilor Condiții specifice.

III. Descrierea și utilizarea serviciului 3D Secure

1. Serviciul 3D Secure este o tehnologie dezvoltată de Organizațiile Internaționale de Carduri VISA și Mastercard care reprezintă un standard de securitate a tranzacțiilor e-commerce, reduce substantial fraudele pe Internet și asigură un mediu securizat derularii acestui tip de tranzacții. În funcție de organizația de plăți sub care este emis cardul, Serviciul este identificabil pe site-ul comercianților care sunt înrolați, sub denumirile: Mastercard Identity Check" pentru cardurile de tip Mastercard și „Verified by VISA" pentru cardurile VISA.

2. Serviciul 3D Secure este oferit gratuit de către Banca și toate cardurile emise de OTP Bank sunt înrolate automat în sistemul 3D Secure. Deținătorii/Utilizatorii Autorizati de carduri emise de OTP Bank care efectuează tranzacții pe site-uri înrolate 3D Secure (care afisează logo Verified by Visa/VISA /Mastercard Identity Check), pot autentifica tranzacțiile online astfel:

- **autentificare biometrică în aplicația SmartBank**, descarcată și instalată din App Store sau Google Play, în funcție de dispozitivul utilizat. La prima utilizare a aplicației Deținătorul/Utilizatorul Autorizat va activa funcția de autentificare tranzacții online prin utilizarea metodelor biometrice (scanare amprentă, recunoaștere facială), urmând pașii descriși în aplicație. Va fi necesar să se introducă ultimele 10 (zece) cifre din numărul cardului utilizat și ultimele 6 (șase) cifre din CNP, ulterior va primi pe telefonul mobil, printr-un mesaj SMS, un cod unic pentru a confirma activarea în aplicație. Totodată, Aplicația va solicita setarea unui cod alternativ pentru a se utiliza în cazurile în care metoda de autentificare biometrică nu este recunoscută pentru aprobarea tranzacțiilor online din diverse motive (de ex.: probleme temporare ale dispozitivului de recunoaștere amprentă/ recunoaștere facială, condiții de iluminare scazută etc.). Ulterior activării, indiferent pe ce dispozitiv este inițiată tranzacția online, respectiv pe desktop, pe tabletă, pe laptop sau pe telefonul mobil, pentru autentificarea tranzacției prin intermediul aplicației SmartBank, Deținătorul/Utilizatorul Autorizat va primi pe dispozitivul pe care este descărcată aplicația, o notificare de tip "push", care îl va direcționa către ecranul cu datele tranzacției (suma, valuta, denumirea comerciantului) pentru autentificarea biometrică si aprobarea tranzacției. În cazul în care Deținătorul/Utilizatorul Autorizat nu recunoaste tranzacția, aceasta se poate respinge din cadrul aceluiași ecran al Aplicației.
  Daca Deținătorul/Utilizatorul Autorizat nu are descărcată aplicația SmartBank sau nu are opțiunea de autentificare prin biometrie activă, poate fi direcționat din pagina de plată pentru descărcarea aplicației/activarea opțiunii de autentificare prin biometrie.
  Pentru siguranța tranzacțiilor online, aplicația SmartBank poate fi utilizată doar dacă este securizată prin metodele de autentificare puse la dispoziție de către dispozitivul utilizat. Referitor la autentificarea biometrică (amprentă digitala și recunoașterea facială), aceste verificări se bazeaza pe tehnologia dispozitivului utilizat, iar Banca nu are acces și nu controlează datele biometrice stocate pe dispozitiv. Banca doar valideaza realizarea de catre dispozitiv a autentificării prin metode biometrice, fară a prelucra, efectiv, în niciun fel, datele biometrice.

- **autentificare cu parola dinamică prin SMS -** pentru fiecare tranzacție online cu cardul, Deținătorul/Utilizatorul Autorizat va introduce în pagina de plată, în ecranul indicat pentru aprobarea tranzacției, o parola dinamica unica primita prin SMS pe numărul de telefon mobil comunicat Băncii.

- **autentificare în doi pași – parola statică + parola dinamică (**va fi disponibilă Deținătorului/Utilizatorului Autorizat din momentul primirii unei informări din partea Băncii, pe unul dintre canalele: e-mail, SMS, website, Internet Banking/SmartBank **) -** la prima tranzacție online efectuată cu cardul, Deținătorul/Utilizatorul Autorizat va introduce în pagina de plată o parolă statică, formata din ultimele 6 (șase) cifre din CNP, ulterior va primi prin SMS pe numărul de telefon mobil comunicat Băncii, o parolă dinamică unică, pe care de asemenea o va introduce în pagina de plată, în ecranul indicat pentru aprobarea tranzacției. Parola statică mai sus comunicată, se va modifica la prima utilizare, în sensul că Deținătorului/Utilizatorului Autorizat i se va solicita să își seteze o parolă statică de 6 (șase) cifre, cunoscută doar de către acesta. Astfel,

pentru următoarele tranzactii online efectuate prin intermediul cardului, Deținătorul/Utilizatorul Autorizat va utiliza parola statică setată de către acesta și parolă dinamică unică primita prin SMS. În cazul în care Deținătorul/Utilizatorul Autorizat nu mai cunoaște parola statică setata, este necesar să solicite resetarea acesteia către Romcard, la numărul de telefon 021.202.6999.

3. Pentru utilizarea serviciului 3D Secure, Deținătorul/Utilizatorul Autorizat trebuie să dețină un număr de telefon mobil actualizat în sistemul Băncii, iar site-ul pe care se efectuează tranzacțiile trebuie să respecte la rândul său standardul de securitate 3D Secure, respectiv să afișeze logo-ul "Visa /Verified by Visa" sau “Mastercard Identity Check”.
Deținătorii/Utilizatorii Autorizati cardului pot solicita actualizarea numărului de telefon mobil în unitățile teritoriale OTP Bank sau prin apelarea serviciului Call Center, la numărul de telefon (+4) 021 308 00 89.
4. În cazul în care Deținătorul/Utilizatorul Autorizat efectuează tranzacții pe site-uri care nu sunt înrolate în serviciul 3D Secure, prin Verified by Visa / Mastercard Identity Check, Banca nu va fi responsabilă de eventualele prejudicii cauzate.

IV. Obligațiile și răspunderea Deținătorului/Utilizatorului

1. Deținătorul/Utilizatorul Autorizat are obligația de a activa serviciul 3D Secure cu funcția de autentificare biometrică (scanare amprentă, recunoaștere facială), prin aplicația SmartBank, doar de pe dispozitive ce îi apartin în mod legal, acestea nefiind utilizate si de catre alte persoane. După activarea funcției de autentificare biometrică, va securiza dispozitivul cu aceeași atenție pe care trebuie să o utilizeze pentru păstrarea în siguranță a cardului utilizat, pentru a evita utilizarea neautorizată a aplicatiei.
2. Deținătorul/Utilizatorul Autorizat are obligația de a anunta Banca pentru blocarea imediata a cardului daca are suspiciuni privind compromiterea confidențialității datelor sale personale (datele cardului, codurile/parolele unice de validare a tranzacțiilor online și utilizarea acestora pe Internet). Banca nu va fi responsabilă pentru plățile efectuate prin intermediul cardului până la momentul informării sale cu privire la apariția unuia dintre evenimentele anterior enumerate.
3. Deținătorul/Utilizatorul Autorizat are obligația de a păstra în siguranță datele sale de autentificare în Aplicația SmartBank și/sau pentru dispozitivul său. Banca nu poate interveni și nu poate fi făcută responsabilă pentru plățile online autorizate prin intermediul Aplicației SmartBank de către alte persoane, fie cu acordul Deținătorului/Utilizatorului Autorizat, fie ca urmare a neîndeplinirii de către acesta a obligațiilor ce-i revin conform prevederilor contractuale din prezentele Condiții Specifice.
4. Deținătorul/Utilizatorul Autorizat are obligația să actualizeze sistemul de operare conform recomandarilor producătorului dispozitivului și să utilizeze doar versiunile oficiale ale sistemului de operare furnizat de acesta. Totodată, să nu impiedice protecțiile de securitate a sistemelor de operare recomandate de producătorul dispozitivului. În cazul în care Deținătorul/Utilizatorul Autorizat nu respectă aceste recomandări, Banca nu este răspunzătoare pentru niciun fel de prejudicii cauzate dispozitivului utilizat, incluzând dar fără a se limita la orice risc de securitate cauzat de viruşi, erori, falsificare, întrerupere, defecțiune, întârziere în operaţiuni sau transmisiuni, cădere a reţelei sau orice altă defecţiune tehnică produsă.
5. Deținătorul/Utilizatorul Autorizat va instala Aplicația Smart Bank doar din magazinele oficiale - Google Play și App Store, publicate de Banca și nu va instala alte aplicații din surse neoficiale care ar putea compromite securitatea Aplicației.
6. Aplicația SmartBank nu va fi funcțională în cazul în care metodele de securizare ale dispozitivului utilizat sunt dezactivate, însă aplicația SmartBank nu controlează aceste metode de securizare și nu raspunde pentru eventualele pierderi cauzate ca urmare a dezactivării lor de către Deținător/Utilizator Autorizat sau de modul în care furnizorul dispozitivului utilizează respectivele metode de securizare.

V. Întreruperea funcționării sau modificarea Aplicației SmartBank

1. Utilizarea Aplicației SmartBank de către Deținător/Utilizator Autorizat poate înceta în următoarele situații:
    - la solicitarea Deținătorului/Utilizatorului Autorizat prin dezinstalarea aplicației de pe dispozitivul utilizat, cu efect imediat. Dezinstalarea aplicației nu înseamnă încetarea relației de afaceri între Deținător/Utilizator Autorizat și Bancă;
    - la solicitarea Băncii în cazul în care se constată că Deținătorul/Utilizatorul Autorizat nu respectă prezentele Condiții specifice sau orice alte reguli care pot aduce prejudicii de orice natură Băncii, cu efect imediat și fără notificarea prealabilă a Deținătorului/Utilizatorului Autorizat;
    - atunci când încetează relația de afaceri între Deținător/Utilizator Autorizat și Bancă conform prevederilor contractuale agreate în momentul deschiderii relației de afaceri.
2. Aplicația SmartBank se poate suspenda sau modifica, din orice motiv, inclusiv când necesită lucrări de remediere sau întreţinere.Totodată, Aplicația poate fi retrasă, cu anunțarea prealabila a Deținătorilor/Utilizatorilor Autorizati pe site-ul Bancii https://www.otpbank.ro, cu 30 de zile înainte.
3. Prezentele Condiții Specifice pot fi modificate oricând, după publicarea acestora pe site-ul Băncii https://www.otpbank.ro, în conformitate cu prevederile art. II pct. 6.

VI. Prelucrarea datelor cu caracter personal

În vederea utilizării serviciului 3D Secure, așa cum este acesta descris în prezentele Condiții Specifice, OTP Bank Romania prelucrează date cu caracter personal obținute în cadrul relației de afaceri cu Deținătorul și/sau Utilizatorul Autorizat în temeiul executării contractului încheiat cu OTP Bank România.
Totodată, utilizarea Aplicației SmartBank presupune parcurgerea cu succes a procesului decizional automat de activare a autentificării biometrice în cadrul serviciului 3D Secure și având în vedere prelucrarea datelor cu caracter personal efectuată în acest context, Deținătorul și/sau Utilizatorul Autorizat poate, prin apelarea Call Center-ului Băncii, să solicite și să obțină detalii suplimentare, să își exprime punctul de vedere, să conteste decizia și să solicite intervenție umana pentru re-analizarea rezoluției primite ca urmare a procesului decizional automat.
Banca respectă caracterul privat al datelor cu caracter personal prelucrate și se angajează să îl protejeze în strictă conformitate cu prevederile legale aplicabile. In acest sens, Banca deține, conform legii, calitatea de operator de date cu caracter personal și prelucrează datele cu caracter personal în conformitate cu Regulamentul (UE) 2016/679 și celelalte prevederi legale aplicabile cu privire la protecția persoanelor privind prelucrarea datelor cu caracter personal și libera circulație a acestor date, în vederea utilizarii serviciului 3D Secure pentru tranzactiile online efectuate cu cardurile emise de OTP Bank Romania SA. De asemenea, Banca poate efectua orice verificări, poate să solicite și să obțină informații de la orice instituție competentă, registru public, arhiva, bază de date electronică sau terț abilitat, deținător de astfel de informații, conform competențelor lor legale. Informații legate de prelucrarea și protecția datelor cu caracter personal de către OTP Bank Romania S.A., (scopuri, destinatarii datelor, drepturile de care beneficiaza persoana vizată conform legii: dreptul de fi informat, de a avea acces la acestea, dreptul la rectificarea sau ștergerea acestora („dreptul de a fi uitat”) sau la restricționarea prelucrării sau a opoziției la prelucrari, precum și dreptul la portabilitatea datelor, dreptul de a depune plângere în fața Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automata, inclusiv crearea de profiluri și dreptul de retragere a consimțamântul în orice moment, fară a fi prejudiciat in vreun fel etc.) se regăsesc în Notificarea privind protecția datelor cu caracter personal, document pus la dispoziție de către Bancă la initierea relatiei de afaceri între Deținător/Utilizator Autorizat și Bancă.
De asemenea, informații în legatură cu prelucrarea datelor cu caracter personal de către OTP Bank România S.A., în general (inclusiv privind procesele decizionale automate) se regăsesc în secțiunea dedicată din cadrul

Condițiilor Generale de Afaceri ale Băncii sau din cadrul site-ului Băncii https://www.otpbank.ro, secțiunea Confidențialitate.

VII. Date de contact

Pentru solicitările legate de utilizarea serviciului 3D Secure puteți contacta serviciul Call Center, de luni până vineri, între 8:30 - 21:00 la numerele de telefon:

- 0800 88 22 88 (apelabil gratuit din orice reţea fixă sau mobilă)
- (+4) 021 308 57 10 (apelabil internațional, tarif normal)
- (+4) 021 308 00 89 (apelabil internațional, tarif normal)