TUCA ZBARCEA
ASOCIATII

NOILE PROPUNERI DE REGLEMENTĂRI EUROPENE – PSD3 ȘI PSR

MĂSURILE DE PROTECȚIE ÎMPOTRIVA FRAUDELOR ȘI DE PROTECȚIE A UTILIZATORILOR

Data: 22 MARTIE 2024

Autor: Gabriela Anton, partener Țuca Zbârcea & Asociații

Noile propuneri de reglementări europene în materia serviciilor de plată și accesul la date financiare

- Pe 28 iunie 2023, Comisia Europeană a publicat un pachet de propuneri legislative menit să modernizeze și să armonizeze cadrul actual aplicabil serviciilor de plată. Noul pachet legislativ este văzut de Comisie ca o evoluție mai degrabă decât ca o revoluție, necesar pentru a ține pasul cu digitalizarea accelerată a acestui sector.
- De la introducerea Directivei Europene privind Serviciile de Plată (Directiva UE 2015/2366 - PSD2) în 2015, serviciile financiare au fost una din categoriile cu cea mai rapidă rată de adoptare a tehnologiilor digitale.
- Conform declarațiilor Comisiei, propunerile au ca prioritate interesele și încrederea consumatorilor, concurența și securitatea. Acest pachet este văzut și ca un pas important pentru a armoniza Piața Unica Europeană pentru plăți și pentru a reduce divergențele în implementarea națională a regulilor europene.

PSD3, PSR ȘI FIDA

- Prin acest pachet, Comisia propune ca actuala reglementare PSD2 să fie divizată în două acte:
  - Un regulament privind serviciile de plată în cadrul pieței interne – PSR, care va uniformiza aplicarea serviciilor de plată în cadrul Uniunii Europene, atât pe plan național cât și transfrontalier. PSR preia din actuala directivă PSD2 cadrul legal de reglementare a prestării de servicii de plată, incorporând și anumite cerințe din standardele tehnice de reglementare, ghidurile și opiniile emise de Autoritatea Bancară Europeană.
  - O nouă directivă privind serviciile de plată și serviciile de monedă electronica în cadrul pieței interne - PSD3. Noua directivă PSD3 va incorpora instituțiile emitente de monedă electronică (EMI) ca o formă a instituțiilor de plată (PI) fuzionând directiva privind serviciile de plată și directiva privind privind instituțiile emitente de monedă electronică într-un cadru legal unitar.
  - De asemenea, Comisia a venit cu o propunere de Regulament privind un cadru pentru accesul la date financiare, menit să transforme conceptul de open banking în open finance.
  - Aceasta reglementare va stabili drepturi și obligații cu privire la accesul la datele clienților în sectorul financiar, în prezent aplicabil doar la nivelul conturilor de plată, prin intermediul prestatorilor de servicii de informare cu privire la conturi, reglementat de PSD2.

Principalele obiective

- **Combaterea și atenuarea fraudei în materie de plăți**, prin facilitarea schimbului de informații legate de fraudă între prestatorii de servicii de plată (PSP), consolidarea regulilor de autentificare a clienților, extinderea drepturilor la rambursare ale consumatorilor, care cad victimă fraudei, și impunerea verificărilor cu privire la codul IBAN al beneficiarului plăților și numele contului;
- **Îmbunătățirea accesului** prestatorilor nebancari la sistemele de plăți din UE (cu garanții adecvate), prin conferirea drepturilor acestor prestatori la un cont bancar, pentru contracararea fenomenului de descărcare de risc (a se vedea și Opinia EBA din 2012 si Ghidul EBA/GL/2023/04 privind politicile și controalele pentru gestionarea eficace a riscurilor de spălare a banilor și de finanțare a terorismului (SB/FT) atunci când se oferă acces la servicii financiare);
- **Îmbunătățirea funcționării serviciilor** de tip open banking și **introducerea de noi servicii precum introducerea serviciilor de numerar în magazine**, permițându-le comercianților cu amănuntul să furnizeze servicii în numerar clienților fără a solicita o achiziție și clarificând regulile aplicabile operatorilor de bancomate independenți;
- **Armonizarea** implementării acestor reglementări la nivelul statelor membre de autoritățile naționale.

Măsurile propuse pentru combaterea și atenuarea fraudei în materie de plăți

- Numărul cazurilor de „inginerie socială” în care consumatorii sunt induși în eroare în ceea ce privește autorizarea unei operațiuni de plată către un autor al fraudei a crescut semnificativ în ultimii ani. Prin PSR sunt vizate în particular cazurile de „***spoofing***”, în care autorii fraudelor pretind că sunt angajați ai prestatorului de servicii de plată al unui client și utilizează în mod abuziv numele, adresa de e-mail sau numărul de telefon al prestatorului de servicii de plată pentru a câștiga încrederea clienților și pentru a-i determina să întreprindă anumite acțiuni.
- În aceste situații, autorii fraudelor pot prelua controlul asupra întregului proces de consimțământ și autentificare, inclusiv asupra realizării autentificării stricte a clienților, ceea ce face dificilă calificarea unei operațiuni drept autorizată sau neautorizată.
- PSD2 a limitat rambursările doar la operațiunile neautorizate și nu are instrumentele necesare pentru a adresa acest nou tip de fraude. Măsurile de prevenție precum autentificarea strictă a clienților s-au dovedit insuficiente pentru a preveni astfel de fraude.

Măsurile propuse pentru combaterea și atenuarea fraudei în materie de plăți

- Obligarea prestatorilor să ofere gratuit servicii de verificare a corespondenței dintre codul unic de identificare (IBAN) și numele beneficiarului plății pentru orice operațiune de transfer (inclusiv pentru plăți instant).
- Stabilirea unui cadru legal care să permită prestatorilor să facă schimb de informații cu privire la fraude prin platforme IT dedicate, care să asigure acestor schimburi legitimitate din perspectiva GDPR.
- Consolidarea capacităților de monitorizare a tranzacțiilor.
- Obligarea prestatorilor să deruleze periodic programe și campanii de conștientizare cu privire la tendințele și riscurile în materie de fraudă care să se adreseze clienților și angajaților prestatorilor de servicii de plată, cu scopul de a ajuta clienții să înțeleagă că sunt victime ale unei tentative de fraudă.
- Acordarea dreptului clientului la despăgubire în anumite situații specifice.
- Îmbunătățirea regulilor privind autentificarea strictă a clienților.

Răspunderea pentru frauda prin uzurparea identității

- Prestatorii de servicii de plată ar putea fi considerați la rândul lor victime ale cazurilor de „spoofing”, deoarece a avut loc o uzurpare a informațiilor acestora. Cu toate acestea, prestatorii de servicii de plată dispun de mai multe mijloace decât consumatorii pentru a pune capăt acestor cazuri de fraudă, inclusiv și prin mijloace tehnice elaborate împreună cu furnizorii de servicii de comunicații electronice (cum ar fi operatorii de rețele de telefonie mobilă, platformele de internet etc.).
- Prestatorii de servicii de comunicații electronice vor trebui să coopereze cu prestatorii de servicii de plată pentru a preveni noi cazuri ale acestui tip de fraudă, inclusiv prin instituirea de măsuri organizatorice și tehnice adecvate pentru a proteja securitatea și confidențialitatea comunicațiilor în conformitate cu Directiva 2002/58/CE, inclusiv în ceea ce privește identificarea apelantului și a adresei de e-mail.
- Totuși, orice acțiune introdusă de un prestator de servicii de plată împotriva altor prestatori, cum ar fi prestatorii de servicii de comunicații electronice, pentru prejudicii financiare cauzate în contextul acestui tip de fraudă, va trebui formulată în conformitate cu dreptul intern.

Răspunderea pentru frauda prin uzurparea identității

- Un consumator de bună-credință care a fost victima unei astfel de fraude de tip „spoofing” va avea dreptul la rambursarea întregii sume aferente operațiunii de plată frauduloase de către prestatorul de servicii de plată în cauză, cu excepția cazului în care plătitorul a acționat în mod fraudulos sau a dat dovadă de „*neglijență gravă*”.
- Termenul de soluționare este de zece zile lucrătoare, când prestatorul fie rambursează suma clientului, fie contestă solicitarea invocând frauda sau neglijența gravă din partea acestuia. Probele și gradul de presupusă neglijență ar trebui evaluate, în general, în conformitate cu dreptul intern. Cu toate acestea, se consideră că o „neglijență gravă” ar trebui să implice comportamente care prezintă un grad semnificativ de imprudență, precum păstrarea credențialelor pentru autorizare într-un format ușor de detectat de terți.
- De îndată ce consumatorul ia cunoștință de faptul că a fost victima unei astfel de fraude de tip „*spoofing*”, acesta ar trebui să raporteze incidentul, fără întârzieri nejustificate, poliției (de preferat prin proceduri de depunere a plângerilor online, în cazul în care acestea sunt puse la dispoziție de poliție) și prestatorului său de servicii de plată, furnizând toate probele necesare.
- Prin aceste condiții procedurale, s-a dorit evitarea unui drept automat la rambursare pentru client, pentru a nu crea hazard moral și o reducere a vigilenței clientului.

Serviciul de verificare IBAN și a numelui beneficiarului

- Pentru a contribui la reducerea fraudei și a erorilor, consumatorii vor beneficia în mod gratuit de un serviciu de verificare a discrepanțelor între codul unic de identificare al beneficiarului plății (IBAN) și numele beneficiarului plății furnizate de plătitor. Regulamentul UE 886/2024 privind transferurile credit instant în euro prevede deja un serviciu de verificare a corespondenței dintre codul unic de identificare și numele beneficiarului plății care urmează să fie oferit utilizatorilor de transferuri de credit instant în euro. Noul serviciu reglementat prin PSR se va aplica celorlalte tipuri de transfer care nu intră sub incidența noului regulament.
- Prestatorul de servicii de plată al plătitorului va trebuit să notifice clientul în cel mult câteva secunde din momentul în care acesta a introdus informațiile privind beneficiarul plății în cazul în care se detectează astfel de discrepanțe, înainte ca plătitorul să autorizeze operațiunea.
- În cazul în care prestatorul nu notifică utilizatorul cu privire la aceste discrepante, are obligația de a rambursa acestuia contravaloarea transferului în termen de 10 zile lucrătoare.

Serviciul de verificare IBAN și a numelui beneficiarului

- Gradul de discrepanță poate fi parțial, influențat și de situații precum prezența diacriticelor sau diferențele dintre denumirile comerciale și cele juridice în cazul persoanelor juridice. Prestatorii de servicii de plată vor indica gradul unei astfel de discrepanțe prin indicarea în notificare a faptului că nu există „nicio corespondență” sau că există „o corespondență apropiată”. Prestatorii de servicii de plată vor informa utilizatorii cu privire la posibilele consecințe ale alegerii lor de a ignora discrepanța notificată și de a executa operațiunea.
- Clienții pot decide autorizarea unei operațiuni de plată în pofida faptului că serviciul de verificare a corespondenței a detectat o discrepanță și a notificat utilizatorul în acest sens. Utilizatorii pot renunța la utilizarea unui astfel de serviciu în orice moment pe durata relației lor contractuale cu prestatorul de servicii de plată și pot reveni ulterior la utilizarea acestuia.
- Se pot pune la dispoziția plătitorilor anumite soluții care să le permită să emită un ordin de plată fără a introduce ei înșiși codul unic de identificare. În schimb, astfel de elemente sunt oferite de furnizorul soluției de inițiere respective. În astfel de cazuri, nu este necesar un serviciu care să verifice corespondența dintre codul unic de identificare și numele beneficiarului plății, deoarece riscul de fraudă sau de erori se reduce semnificativ.

Clarificări cu privire la aplicarea ASC

- Cazurile de excludere de la aplicarea ASC, dezvoltate de ABE prin Q&A au fost reglementate pentru a evita aplicarea acestora în mod diferit sau abuziv:
  - Pentru operațiunile inițiate de comercianți (MIT), autentificarea strictă a clienților se aplică doar la stabilirea mandatului inițial.
  - Ordinele prin corespondență sau prin telefon (MO-TO) se refera numai la inițierea operațiunilor de plată (și nu executarea acestora), implicând totuși cerințe de securitate și verificări care să permită autentificarea.
- Înscrierea instrumentelor de plată, în special a cardurilor de plată, în portofelele electronice, crearea unui token sau procesul de înlocuire a acestuia poate da naștere unui risc de fraudă legată de plată sau altor abuzuri când se realizează prin intermediul unui canal la distanță și ar trebui, prin urmare, să necesite aplicarea ASC în momentul emiterii sau al înlocuirii tokenului. Astfel, prestatorul de servicii de plată ar trebui să verifice de la distanță dacă utilizatorul este utilizatorul de drept al instrumentului de plată și să asocieze utilizatorul și versiunea digitalizată a instrumentului de plată cu dispozitivul respectiv.

Clarificări cu privire la aplicarea ASC

- Articolul 85 (12) din PSR clarifică că elementele ASC nu trebuie în mod necesar să aparțină unor categorii diferite (i.e. cunoștințe, inerență sau posesie) atât timp cât independența lor este pe deplin menținută. Această prevedere va ajuta la rezolvarea unor probleme de onboarding a unor noi instrumente de plată și crearea elementelor SCA, ceea ce va ajuta la o experiență îmbunătățită pentru utilizator.
- **Răspunderea prestatorilor de servicii tehnice** – Conform noilor propuneri, prestatorii de servicii tehnice și operatorii schemelor de plată care prestează servicii fie beneficiarului plății fie pretatorilor de servicii de plată sunt la rândul lor răspunzători pentru orice prejudiciu financiar cauzat acestora pentru incapacitatea, în cadrul relației lor contractuale, de a furniza serviciile necesare pentru a permite autentificarea strictă a clienților. Deși nereglementat, acest tip de furnizori au un rol semnificativ, e.g. prin furnizarea protocoalelor de comunicare utilizate de instituțiile de plată pentru aplicarea ASC.

Schimbul de informații cu privire la fraude

- Pentru a detecta mai bine operațiunile de plată frauduloase și pentru a-și proteja clienții, în scopul monitorizării operațiunilor, prestatorii de servicii de plată vor putea utiliza datele privind fraudele în domeniul plăților partajate de alți prestatori de servicii de plată pe o bază multilaterală, cum ar fi platformele informatice specifice bazate pe acorduri privind schimbul de informații.
- În acest mod, prestatorii de servicii de plată pot utiliza colectiv informațiile privind codurile unice de identificare, tehnicile de manipulare și alte circumstanțe asociate transferurilor de credit frauduloase identificate individual de fiecare prestator de servicii de plată. Datele privind fraudele în domeniul plăților, partajate în cadrul unui acord multilateral ar trebui să fie utilizate numai în scopul îmbunătățirii monitorizării operațiunilor și nu ar trebui să constituie motive pentru retragerea serviciilor bancare fără o investigație detaliată.
- PSR va constitui o bază legală prin prisma GDPR, care va permite acest schimb de informații, pe baza unui acord multilateral și a unei platforme IT dedicate. Înainte de a încheia un acord privind schimbul de informații, prestatorii de servicii de plată vor trebui să efectueze o evaluare a impactului asupra protecției datelor și după caz, să consulte autoritatea relevantă pentru protecția datelor.

Răspunderea pentru tranzacții neautorizate

- Noile reguli obligă prestatorul de servicii de plată să ramburseze plătitorului valoarea operațiunii de plată neautorizate imediat sau cel târziu la sfârșitul zilei lucrătoare următoare, cu excepția cazului în care este suspectată o fraudă (pentru care se aplică termenul de zece zile lucrătoare).
- O schimbare notabilă în sarcina probei este introdusă și prin modificarea cerinței ca prestatorului să îi revină sarcina de a demonstra că *operațiunea a fost autorizată, înregistrată corect, înscrisă în conturi și nu a fost afectată de o deficiență în executarea serviciilor*.
- Formularea actuală din PSD 2 si Legea 209/2019 obliga prestatorii să dovedească autentificarea, ceea ce reprezintă mai degrabă un aspect tehnic ce poate fi furnizat în baza înregistrărilor date de sistemele utilizate, spre deosebire de autorizare conform propunerii din PSR.

Răspunderea pentru tranzacții neautorizate

- Această modificare vine în contextul în care și definiția autorizării a fost modificată, fiind înlocuită formularea anterioară care se referea la *exprimarea consimțământului plătitorului pentru executarea operațiunii* de plată. În noua formulare, exprimarea consimțământului este înlocuită de „*acordarea permisiunii pentru executarea operațiunii*”.
- În contextul în care PSR menționează că înlocuirea noțiunii de consimțământ cu permisiune s-a efectuat pentru a evita interpretarea acesteia exclusiv drept „consimțământ” sau „consimțământ explicit”, astfel cum sunt definiți acești termeni în GDPR, este neclar cu ce se va asimila noțiunea de permisiune în celelalte cazuri.
- În orice caz, o sarcina impusă prestatorului de a dovedi consimțământul clientului ar fi extrem de dificilă în practică în măsura în care acesta ar trebui să prezume intenția sau starea psihică a clientului său.

Calendarul de implementare

- Adoptarea finală a acestui pachet legislativ este estimată a avea loc în cursul anului 2025.
- Statele membre vor fi obligate să transpună PSD3 în termen de 18 luni de la publicarea în Jurnalul Oficial al Uniunii Europene.
- Conform noului regim introdus de PSD3, autorizațiile deja acordate instituțiilor de plată și instituțiilor emitente de monedă electronica vor rămâne în vigoare pentru o perioadă suplimentară de 24 de luni de la intrarea în vigoare a PSD3.
- Cu toate acestea, instituțiile deja autorizate vor trebui să depună o nouă cerere de autorizare la autoritățile naționale competente (i.e. Banca Națională a României) în termen de 18 luni de la intrarea în vigoare a PSD3.
- Prin urmare, este foarte important ca instituțiile deja autorizate să identifice în timp util și să analizeze compatibilitatea propriilor sisteme și măsurile necesare pentru adoptarea noilor cerințe de reglementare ce vor fi impuse prin PSD3, pentru a continua să funcționeze.

TUCA ZBARCEA
ASOCIATII

Mulțumesc!

Gabriela ANTON, Partner
gabriela.anton@tuca.ro

4-8 Nicolae Titulescu ave
America House, West Wing, 8th floor
Sector 1, 011141, Bucharest, Romania
T: (40-21) 204 88 90
F: (40-21) 204 88 99
E: office@tuca.ro
www.tuca.ro