DEPARTAMENTUL DE STUDII PARLAMENTARE ŞI POLITICI UE
DIRECŢIA STUDII ŞI DOCUMENTARE LEGISLATIVĂ

MĂSURI PENTRU ÎMBUNĂTĂȚIREA PROTECȚIEI CONSUMATORILOR ÎMPOTRIVA FRAUDEI BANCARE ÎN UNIUNEA EUROPEANĂ – ASPECTE COMPARATIVE

studiu documentar

aprilie 2026

Lucrările elaborate în cadrul Direcției studii și documentare legislativă au caracter documentar și nu reprezintă punctul de vedere al Camerei Deputaților.
Documentele legislative oficiale au fost consultate în limba de origine, iar traducerea informațiilor relevante selectate nu reprezintă o traducere oficială, fiind furnizată ca un mijloc de înțelegere a unui document original, scris în altă limbă.
Baza de date cuprinzând totalitatea studiilor elaborate de Direcția studii și documentare legislativă poate fi accesată prin intermediul paginii de Intranet a Camerei Deputaților la adresa:
http://www.cdep.ro/pls/dic/site2015.page?den=dsdl-home1

Documentare și sinteză: Violeta Cincă
Consilier parlamentar - Direcția studii și documentare legislativă
Palatul Parlamentului, str. Izvor nr.2-4, sect.5, București
Tel: 021.316.03.65; 021.414.13.50/ 51, Interior 1350/1349, camera 5070
E-mail: doc@cdep.ro

CUPRINS

_Toc226539273

INTRODUCERE

În perioada 2023–2026, Uniunea Europeană a trecut la un model de „protecție unificată”. Deși fiecare țară are propriile particularități juridice, trei reglementări majore la nivel european au standardizat responsabilitățile băncilor în toate cele 27 de state membre. Această tranziție se bazează pe trei piloni legislativi principali: Regulamentul privind plățile instantanee (IPR), Regulamentul privind serviciile de plată (PSR/PSD3) și noile cerințe în materie de combatere a spălării banilor (AML).

Schimbarea esențială constă în faptul că sarcina asigurării securității a trecut de la consumator la bancă. Dacă sistemele băncii nu detectează o înșelătorie sofisticată, banca este acum mult mai susceptibilă să fie trasă la răspundere pentru pierderile suferite.

Regulamentul privind plățile instantanee (IPR) prevede că toate băncile din zona euro care oferă transferuri bancare standard trebuie să ofere și transferuri instantanee fără costuri suplimentare. Pentru a asigura un echilibru între rapiditatea acestor plăți și securitate, regulamentul introduce o nouă responsabilitate esențială:

Verificarea beneficiarului (VoP): băncile trebuie să ofere un serviciu care să verifice dacă codul IBAN al beneficiarului corespunde cu numele acestuia înainte de autorizarea tranzacției.

Dacă o bancă nu efectuează această verificare sau furnizează o confirmare incorectă de „concordanță”, banca este strict răspunzătoare pentru pierderea financiară. Dacă banca avertizează cu privire la o neconcordanță, iar clientul continuă, răspunderea revine clientului.

Cei trei piloni ai protecției UE (2024–2026)

A. Regulamentul privind plățile instantanee (IPR)

Termenul limită de implementare: octombrie 2025 (zona euro); iulie 2027 (în afara zonei euro).

Verificarea obligatorie a beneficiarului (VoP) - Băncile trebuie să verifice dacă numele beneficiarului corespunde codului IBAN înainte de a efectua transferul de bani.

Dacă banca nu efectuează această verificare sau oferă o confirmare falsă de „concordanță”, aceasta este strict răspunzătoare pentru pierdere.

În prezent, această măsură este activă în toate statele din zona euro (de exemplu, Franța, Germania, Spania, Italia).

B. Regulamentul privind serviciile de plată (PSR) și PSD3

Acordul politic a fost atins la sfârșitul anului 2025, iar aplicarea deplină se va face în decursul anului 2026.

Băncile trebuie să ramburseze sumele victimelor „spoofingului" sau ale fraudei prin uzurparea identității (de exemplu, un escroc care simulează un apel de la bancă).

Banca trebuie să dovedească „neglijența gravă" a clientului pentru a evita rambursarea. În era deepfake-urilor bazate pe IA și a phishingului de înaltă calitate, „neglijența gravă" este acum definită mult mai strict în favoarea consumatorului.

C. Monitorizare obligatorie în timp real

Băncile trebuie să implementeze analize comportamentale bazate pe IA.

Se așteaptă ca băncile să blocheze tranzacțiile care se abat de la obiceiurile tipice de cheltuieli ale unui client (de exemplu, locație, oră sau sume neobișnuit de mari) și să ofere o linie de asistență umană — nu doar un chatbot — pentru alerte de fraudă.

ASPECTE COMPARATIVE

AUSTRIA

Consumatorii din Austria beneficiază de protecție financiară împotriva fraudei prin intermediul unor cadre juridice solide, precum Legea privind protecția consumatorilor (KSchG) și reglementările PSD2/SCA. Măsurile de protecție includ autentificarea obligatorie în doi pași (SCA) pentru plăți, o supraveghere strictă din partea FMA (Autoritatea pentru piețele financiare), dreptul de a contesta tranzacțiile neautorizate, precum și servicii de consiliere specializate și gratuite.

Cel mai important mecanism împotriva fraudelor bancare rezultă din trecerea de la a doua la a treia Directivă privind serviciile de plată. În timp ce PSD2 a instituit autentificarea puternică a clientului (SCA), noul Regulament privind serviciile de plată (PSR) și PSD3 (aprobat la sfârșitul anului 2025) introduc o răspundere mult mai strictă:

Răspunderea pentru frauda prin uzurparea identității: băncile sunt acum obligate, în general, să ramburseze sumele de bani clienților care cad victime ale „spoofingului" (caz în care un fraudator se dă drept angajat al băncii). Dacă clientul autorizează o plată în urma acestei înșelăciuni, banca este răspunzătoare, cu excepția cazului în care poate dovedi „neglijență gravă".

Corelarea IBAN/nume: începând cu anii 2025–2026, băncile austriece trebuie să implementeze verificările obligatorii pentru a se asigura că numele beneficiarului corespunde cu IBAN-ul. Dacă banca nu semnalează o neconcordanță și are loc o fraudă, banca poartă întreaga răspundere.

Blocarea tranzacțiilor: băncile destinatarilor au acum competența (și se așteaptă din ce în ce mai mult acest lucru) de a bloca tranzacțiile suspecte primite, extinzând responsabilitatea dincolo de banca plătitorului.

Autoritatea austriacă pentru piețele financiare (FMA) a beneficiat de o extindere semnificativă a mandatului său pentru a asigura „integritatea financiară". Autoritatea austriacă pentru piețele financiare (FMA) preia, începând cu 1 ianuarie 2026, responsabilitatea pentru monitorizarea și aplicarea sancțiunilor financiare în sectorul financiar austriac de la Banca Națională a Austriei (OeNB). Astfel, s-a finalizat ultima etapă a reformei adoptate în 2024. FMA devine autoritatea centrală pentru monitorizarea respectării sancțiunilor financiare și își consolidează rolul de instanță de supraveghere globală pentru integritatea pieței financiare.

Hotărârile recente ale Curții Supreme din Austria (OGH) au stabilit un standard extrem de ridicat pentru ceea ce constituie „neglijență gravă" din partea unui consumator.

Schimbarea abordării în cazul phishingului. În trecut, băncile susțineau faptul că introducerea unui cod TAN (număr de tranzacție) pe un site fals constituia neglijență gravă. Tendințele recente sugerează că dacă un site de phishing este suficient de „înșelător" sau imită perfect interfața băncii, banca nu poate scăpa ușor de răspundere.

Sarcina de a dovedi că clientul a acționat cu intenție sau cu neglijență gravă revine în continuare băncii. O simplă neglijență „obișnuită" (de exemplu, un moment de neatenție) nu mai este suficientă pentru ca o bancă să refuze o rambursare.

VKI (Asociația pentru Informarea Consumatorilor) și Camera Muncii (AK) au adoptat o atitudine mai agresivă în „procesele-model" împotriva băncilor.

Clauze ilegale: VKI a contestat cu succes termenii și condițiile mai multor bănci care încercau să transfere răspunderea pentru tranzacțiile „neautorizate" asupra utilizatorului prin intermediul unor clauze vagi.

Instanțele au recunoscut din ce în ce mai mult o „obligație specială de diligență" (secțiunea 1299 ABGB, Codul civil) pentru bănci, în calitate de experți. Aceasta înseamnă că dacă sistemul de securitate al unei bănci ar fi putut detecta un model de fraudă (de exemplu, transferuri multiple rapide către o țară cu risc ridicat), dar nu a făcut-o, banca este considerată răspunzătoare pentru această neglijență.

BELGIA

În ultimii trei ani (2023–2025), măsurile menite să sporească responsabilitatea băncilor belgiene în protejarea clienților împotriva fraudei au trecut de la o abordare pur reactivă la una de prevenire proactivă, ca urmare a creșterii numărului de escrocherii de tip phishing și „spoofing” (suplinirea identității). Printre măsurile cheie se numără verificarea obligatorie a codului IBAN, monitorizarea îmbunătățită a tranzacțiilor cu ajutorul inteligenței artificiale (IA) și o răspundere mai strictă a băncilor în anumite scenarii de fraudă.

Pe 9 octombrie 2025 a avut loc o schimbare în reglementarea bancară, atunci când Belgia – în conformitate cu Regulamentul UE 2024/886 – a impus tuturor băncilor verificarea obligatorie a numelui asociat codului IBAN (atunci când un client inițiază un transfer, banca trebuie să verifice automat dacă numele destinatarului corespunde cu IBAN-ul). Dacă o bancă nu furnizează această avertizare și un client trimite bani unui fraudator (situație frecventă în cazul „fraudei cu facturi”), banca este acum mult mai expusă la cereri de despăgubire.

Sistemul „galben/roșu”. Sistemele furnizează acum avertismente de tipul „Potrivire apropiată” sau „Nicio potrivire”. Dacă un client ignoră un avertisment de tipul „Nicio potrivire”, banca poate invoca în continuare neglijența, dar lipsa unui avertisment constituie acum o eroare bancară definitivă.

Pentru a combate frauda în domeniul facturilor – care costă belgienii milioane de euro anual –, guvernul a impus facturarea electronică prin rețeaua Peppol pentru toate tranzacțiile B2B începând cu 1 ianuarie 2026.

Integrarea în sistemul bancar: băncile belgiene și-au integrat platformele de plată cu Peppol și se așteaptă ca băncile să semnaleze acum facturile „în afara rețelei” ca fiind de risc ridicat. Prin renunțarea la fișierele PDF trimise prin e-mail (care pot fi ușor interceptate și modificate), responsabilitatea structurală pentru livrarea sigură s-a mutat către infrastructura financiară, mai degrabă decât către vigilența utilizatorului final.

Febelfin (Federația Sectorului Financiar Belgian) a raportat că până în 2025, băncile au reușit să blocheze sau să recupereze 75% din tranzacțiile frauduloase înainte ca acestea să părăsească sistemul.

În martie 2026, Banca Națională a Belgiei (NBB) a anunțat o politică mai strictă de „denunțare publică”. Băncile cu sisteme de combatere a spălării banilor (AML) și de detectare a fraudelor, constant deficitare, sunt acum identificate public, creând un stimulent reputațional pentru creșterea bugetelor de securitate.

FINLANDA

În Finlanda, tendința către o responsabilitate sporită a băncilor s-a accelerat semnificativ între anii 2023 și 2026. Această tranziție este determinată atât de recomandările Autorității de Supraveghere Financiară din Finlanda (FIN-FSA), cât și de punerea în aplicare a reglementărilor UE - precum Regulamentul privind plățile instantanee (IPR) și viitorul Regulament privind serviciile de plată (PSR/PSD3). Tendința principală este trecerea de la principiul „clientul trebuie să fie atent” la cel al „banca trebuie să prevină și să ramburseze”, în special în cazul înșelătoriilor sofisticate în care clienții sunt induși în eroare să autorizeze ei înșiși plățile.

Fraudele bancare au stârnit numeroase discuții în Finlanda. De exemplu, potrivit raportului anual al Biroului Ombudsmanului Financiar din Finlanda, numărul solicitărilor din partea clienților legate de sectorul bancar a crescut în ultimii ani, în principal din cauza creșterii numărului de cazuri de escrocherii și de *phishing*. În 2020 au existat nu mai puțin de 200 de cazuri de acest tip, iar în 2023 au fost peste 500. Pentru a proteja clienții împotriva fraudelor, numeroși actori instituționali precum poliția și Autoritatea de Supraveghere Financiară din Finlanda au primit mai multe avertismente și recomandări cu privire la această problemă.

Un sondaj realizat în rândul băncilor de către Autoritatea de Supraveghere Financiară (FIN-FSA) în 2023 arăta că, acestea au identificat și implementat în mare parte și în mod corespunzător aspectele cheie ale securității plăților online. Cu toate acestea, ancheta FIN-FSA a relevat că există încă posibilități de îmbunătățire a securității tranzacțiilor bancare. FIN-FSA este autoritatea responsabilă cu supravegherea sectoarelor financiar și de asigurări din Finlanda, inclusiv a băncilor. FIN-FSA a dat instrucțiuni privind dezvoltarea restricțiilor de securitate pentru serviciile bancare online și plățile mobile, precum și privind monitorizarea și blocarea mai eficientă a tranzacțiilor frauduloase. FIN-FSA a recomandat băncilor să își îmbunătățească sistemele de monitorizare a plăților, astfel încât să poată bloca cu mai multă precizie plățile care diferă semnificativ de istoricul de plăți anterior al clientului, de exemplu, în funcție de destinatar sau de valoarea plății. În aceste cazuri, poate fi necesar să se solicite o confirmare suplimentară a plății din partea clientului, într-o manieră suficient de informativă.

Verificarea obligatorie a beneficiarului (octombrie 2025)

O etapă importantă atinsă în octombrie 2025 în cadrul Regulamentului UE privind plățile instantanee impune tuturor băncilor finlandeze să ofere un serviciu de „*verificare a beneficiarului”*.

Înainte de finalizarea unei plăți, banca trebuie să verifice automat dacă numele destinatarului corespunde codului IBAN (numărul de cont) furnizat.

Dacă banca nu efectuează această verificare sau oferă o confirmare incorectă de „concordanță”, aceasta este răspunzătoare pentru pierderile rezultate din fraudă. Aceasta vizează frauda de tip „Plată autorizată de tip push” (APP), în care victimele cred că plătesc unei întreprinderi sau unei autorități legitime.

Noi recomandări privind limitele de securitate (2024–2025)

În urma unei analize tematice din 2024, FIN-FSA a emis noi recomandări stricte pentru instituțiile de credit:

Băncile trebuie să permită clienților să stabilească limite în euro pe tranzacție și limite zilnice pentru toate transferurile de credit.

FIN-FSA recomandă acum băncilor să stabilească automat aceste limite pentru clienții de retail care nu le-au stabilit ei înșiși, pe baza profilului de risc al clientului.

Băncile sunt îndemnate să implementeze perioade de așteptare (de exemplu, 24 de ore) atunci când un client instalează o nouă aplicație de identificare sau adaugă un dispozitiv nou, înainte de a putea efectua plăți de valoare mare.

Monitorizarea comportamentală în timp real

FIN-FSA a intensificat presiunea asupra băncilor pentru ca acestea să utilizeze inteligența artificială și biometria comportamentală în vederea prevenirii fraudelor în momentul în care acestea au loc.

Băncile ar trebui să blocheze sau să semnaleze plățile care diferă semnificativ de istoricul unui client (de exemplu, ora, locația sau destinatarul neobișnuit).

Dacă sistemul unei bănci suspectează o fraudă, se așteaptă ca aceasta să întrerupă tranzacția și să solicite o confirmare separată și explicită din partea clientului — depășind standardul „Autentificarea puternică a clientului” (SCA).

În decembrie 2025, băncile finlandeze (conduse de OP) și principalii operatori de telecomunicații au lansat un nou model de cooperare în domeniul combaterii fraudei.

Acest model permite băncilor să partajeze date cu operatorii de telecomunicații pentru a bloca traficul către site-urile frauduloase în câteva minute, nu în câteva zile. Astfel, sectorul financiar are responsabilitatea de a acționa ca un „scut digital” activ, nu doar ca un simplu procesator pasiv de plăți.

FRANȚA

Băncile franceze au adoptat măsuri semnificative pentru combaterea spălării banilor (măsuri menite să sporească transparența și să asigure integritatea sistemului financiar). Aceste inițiative reflectă un angajament mai amplu de a preveni activitățile financiare ilicite și de a reduce riscul ca sistemul bancar al țării să fie utilizat în scopuri criminale. Aceste noi măsuri includ controale mai stricte asupra transferurilor de sume mari, retragerilor de numerar și conturilor Livret A, printre altele.

Abordarea Franței a evoluat de la simpla reacție la activitățile criminale la prevenirea proactivă a acestora, instituțiile financiare jucând un rol central. Deși aceste măsuri pot cauza unele inconveniențe pentru clienți, ele reprezintă un pas important în lupta globală împotriva spălării banilor.

Începând cu 29 aprilie 2025, unele bănci franceze vor suspenda transferurile care depășesc 1.000 de euro pentru o perioadă de până la 72 de ore, în cazul în care se detectează anomalii. Această măsură face parte dintr-o strategie mai amplă de identificare a tranzacțiilor suspecte și de prevenire a circulației necontrolate a fondurilor prin sistem.

Pe lângă monitorizarea transferurilor, mai multe bănci au introdus restricții privind retragerile de numerar care depășesc 800 de euro. Această nouă regulă a intrat în vigoare la 1 mai 2025 și impune clienților să justifice scopul oricărei retrageri de numerar care depășește această sumă. Deși tranzacțiile în numerar sunt adesea utilizate în scopuri legitime, ele constituie totodată un instrument frecvent folosit de cei care spală bani, întrucât sunt mai greu de urmărit în comparație cu tranzacțiile digitale. Prin impunerea acestei cerințe, Franța urmărește să descurajeze utilizarea numerarului în scopul spălării banilor și al evaziunii fiscale.

O altă schimbare importantă vizează monitorizarea conturilor de economii Livret A. Aceste conturi, care oferă scutiri fiscale cetățenilor francezi, reprezintă un instrument popular de economisire, dar pot fi folosite și pentru spălarea banilor dacă nu sunt monitorizate cu atenție. Începând cu 2 mai 2025, anumite bănci vor începe să blocheze transferurile din conturile Livret A dacă detectează orice activitate suspectă. Aceasta include transferurile care par neobișnuite ca sumă, frecvență sau destinație sau cele care implică persoane fizice sau organizații legate de țări cu risc ridicat.

Regula privind „spoofing-ul” (noul standard de răspundere)

Cea mai importantă schimbare vizează spoofing-ul (fraudatorii care se dau drept angajați ai băncii). Anterior, băncile refuzau adesea să ramburseze victimelor sumele de bani cu care au fost păgubite, invocând faptul că clientul a dat dovadă de „neglijență gravă” prin validarea unei tranzacții la telefon.

Conform Legii 1058 din 2025, dacă o persoană este victima unui furt de identitate comis de cineva care se dă drept angajat al băncii, banca trebuie să ramburseze tranzacția neautorizată.

„Verificarea beneficiarului" obligatorie (corelarea IBAN-nume)

În conformitate cu Regulamentul UE 2024/886, Franța a introdus corelarea IBAN-nume ca măsură de protecție obligatorie pentru transferurile de credit:

- Înainte de executarea unui transfer, banca trebuie să verifice dacă numele beneficiarului furnizat de client corespunde cu cel al titularului real al contului IBAN de destinație;
- Dacă există o discrepanță, banca trebuie să alerteze clientul și să îi permită să anuleze tranzacția;
- Dacă banca nu efectuează această verificare și transferul se dovedește a fi fraudulos, banca este considerată responsabilă financiar pentru pierdere.

Pentru a preveni apariția „conturilor-*mule*" (conturi utilizate pentru a canaliza bani furați), Legea 1058 din 2025 a instituit un registru centralizat gestionat de Banque de France. Băncile sunt obligate să raporteze și să actualizeze informațiile referitoare la conturile identificate ca fiind utilizate în scopuri frauduloase.

Deși răspunderea băncilor pentru fraude individuale rămâne legată de tranzacția specifică, acestea se confruntă acum cu un risc de reglementare și cu o potențială răspundere în cazul în care nu raportează sau nu iau măsuri în urma informațiilor referitoare la aceste conturi semnalate.

GERMANIA

În Germania, cadrul juridic privind frauda bancară cunoaște, în perioada recentă, o schimbare semnificativă. Deși plafonul standard de răspundere de 50 de euro este în vigoare de ani de zile, noile măsuri prevăzute pentru anii 2025 și 2026 se îndreaptă către un model de tip „*Prevenirea pe primul plan*", impunând băncilor sarcini financiare și operaționale mult mai riguroase.

Conform reglementărilor la nivel european (PSR/PSD3), cadrul de răspundere se extinde pentru a acoperi fraudele legate de plățile „push" autorizate (APP).

Noile reguli vor considera banca responsabilă dacă aceasta nu a reușit să detecteze că propriul numele sau numărul de telefon erau falsificate de către fraudator.

Pentru prima dată, răspunderea va fi împărțită în proporție de 50/50 între banca expeditoare și banca destinatară. Acest lucru obligă „banca escrocului” să fie mult mai agresivă în înghețarea conturilor suspecte, deoarece acum are un interes financiar în pierdere.

Până la sfârșitul anului 2025 și pe parcursul anului 2026, băncile germane au obligația să implementeze un serviciu de verificare a corespondenței numelor pentru toate transferurile bancare.

Înainte de a apăsa butonul „Trimite”, banca trebuie să verifice instantaneu dacă codul IBAN corespunde cu numele destinatarului introdus.

În cazul în care banca nu efectuează această verificare sau confirmă „corespondența” pentru un cont fraudulos, aceasta devine strict răspunzătoare pentru orice pierdere rezultată.

Noul Regulament privind serviciile de plată (PSR), care intră în vigoare ca lege direct aplicabilă pe întreg teritoriul Germaniei, impune băncilor să depășească măsurile de securitate statice.

Băncile sunt acum obligate să monitorizeze tranzacțiile în timp real pentru a depista „comportamente de utilizare anomale”. Dacă o bancă procesează o tranzacție care este „obiectiv suspectă” pe baza modelelor tipice de cheltuieli fără a o semnaliza sau a solicita o verificare suplimentară, banca poate fi considerată direct răspunzătoare pentru daunele cauzate.

Autoritatea de reglementare financiară din Germania, BaFin, a stabilit oficial ca prioritate „reziliența operațională” pentru perioada 2026–2029.

BaFin efectuează mai multe auditări „aprofundate” asupra sistemelor informatice ale băncilor pentru a se asigura că acestea pot rezista la atacuri sofisticate de phishing bazate pe inteligență artificială.

Se observă și o tendință de aplicare a unor sancțiuni mult mai severe. La sfârșitul anului 2025/începutul anului 2026, BaFin a aplicat amenzi record (de exemplu, 45 de milioane de euro unei mari bănci internaționale) în special pentru deficiențe în controalele de combatere a spălării banilor și de prevenire a fraudei.

Instanțele germane (inclusiv Curtea Federală de Justiție, BGH) au stabilit recent un standard foarte ridicat în ceea ce privește definiția „neglijenței grave”.

Simpla cădere în capcana unui e-mail de phishing cu aspect profesional nu mai este considerată automat neglijență gravă.

Judecătorii hotărăsc frecvent că, dacă banca nu poate dovedi că, clientul a dat dovadă de „neglijență extremă” (ignorând mai multe avertismente explicite), banca trebuie să ramburseze fondurile furate.

POLONIA

În Polonia, principalul act normativ care definește obligațiile băncilor este Legea bancară, adoptată în 1997 și modificată ulterior. Printre cele mai importante responsabilități se numără:

- obligația de a păstra confidențialitatea datelor clienților,
- obligația de a furniza informații,
- obligația de a preveni spălarea banilor,
- obligația de a asista clienții în utilizarea produselor și serviciilor oferite,
- obligația de a menține stabilitatea financiară,
- obligația de a respecta standardele etice,
- obligația de a preveni îndatorarea excesivă a clienților,
- obligația de a participa la sistemul de garantare a depozitelor.

Sectorul bancar din Polonia este reglementat de o serie de acte juridice care vizează, în plus, protejarea consumatorilor și asigurarea stabilității financiare. Printre cele mai importante reglementări se numără:

- Legea privind creditul de consum – care reglementează principiile acordării creditului de consum prin introducerea unor mecanisme menite să asigure transparența și inteligibilitatea ofertelor de credit pentru consumatori,
- Legea privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal (în conformitate cu RGPD) – care protejează datele cu caracter personal ale clienților,
- Legea privind serviciile de plată – care asigură protecția în ceea ce privește serviciile de plată, inclusiv securitatea tranzacțiilor și răspunderea pentru operațiunile neautorizate,
- Legea privind tranzacționarea instrumentelor financiare – care asigură protecția investitorilor, inclusiv a persoanelor fizice,
- Legea privind supravegherea pieței financiare – care stabilește reglementările care guvernează supravegherea instituțiilor financiare.

Organismele publice responsabile de supravegherea băncilor și de sprijinirea clienților în protejarea drepturilor lor includ:

- Autoritatea de Supraveghere Financiară din Polonia (Komisja Nadzoru Finansowego – KNF) ,

- Președintele Oficiului pentru Concurență și Protecția Consumatorilor (Prezes Urzędu Ochrony Konkurencji i Konsumentów – Prezes UOKIK) ,
- Președintele Oficiului pentru Protecția Datelor cu Caracter Personal (Prezes Urzędu Ochrony Danych Osobowych – Prezes UODO),
- Ombudsmanul Financiar (Rzecznik Finansowy – RF),
- Inspectorul General pentru Informații Financiare (Główny Inspektor Informacji Finansowej – GIIF).

Majoritatea modificărilor legislative recente din legislația națională (începând cu anul 2022) au fost legate de adaptări menite să asigure conformitatea cu reglementările UE, precum Actul privind reziliența operațională digitală (DORA) sau modificările aduse Directivei privind serviciile de plată (PSD2).

Ca răspuns la dezvoltarea serviciilor electronice și la riscurile crescânde în materie de securitate cibernetică, băncile au implementat o serie de măsuri de protecție a clienților impuse atât de reglementările UE, cât și de cele naționale, precum:

- educarea clienților prin campanii frecvente și sesiuni de instruire pentru a-i ajuta să înțeleagă diferite tipuri de fraude bancare și pentru a le spori capacitatea de a recunoaște activitățile suspecte,

- implementarea de măsuri de informare prin intermediul platformei online și al aplicației mobile a băncii, inclusiv avertismente cu privire la tipurile comune de fraudă,

- utilizarea metodelor de verificare a identității pe mai multe niveluri – precum autentificarea prin SMS, autentificarea în doi pași sau autentificarea biometrică – pentru a preveni accesul neautorizat la conturile clienților,

- monitorizarea tranzacțiilor clienților în timp real pentru a detecta activități suspecte, precum transferuri neobișnuite sau operațiuni neautorizate,

- trimiterea de notificări cu privire la fiecare tranzacție efectuată în contul unui client, permițând astfel supravegherea financiară în timp real,

- emiterea de alerte privind activitățile suspecte din conturi, cum ar fi încercările de schimbare a parolelor sau încercările eșuate de conectare,

- utilizarea de filtre anti-phishing și anti-vishing în comunicările cu clienții pentru a bloca încercările de phishing și vishing (adică uzurparea identității băncii pentru a obține în mod fraudulos datele de conectare, atât verbal, cât și vizual),

- criptarea datelor clienților atât în timpul transmiterii, cât și în timpul stocării, pentru a le proteja împotriva accesului neautorizat,

- actualizarea periodică a software-ului pentru a preveni potențialele vulnerabilități de securitate,

- implementarea unui sistem robust de gestionare a accesului pentru a controla cine poate utiliza sistemele băncii și permisiunile care sunt acordate,

- utilizarea sistemelor de monitorizare comportamentală care detectează activități neobișnuite ale utilizatorilor fără a necesita pași suplimentari de autentificare a clienților,

- cooperarea cu agențiile de aplicare a legii responsabile de investigarea fraudelor bancare.

Aceste măsuri au fost, de asemenea, incluse și dezvoltate în detaliu în Recomandările (KNF, 2015) și Orientările (Prezes UOKIK, 2024) emise de instituțiile de supraveghere care își desfășoară activitatea în Polonia.

PORTUGALIA

Desfășurarea activității financiare în Portugalia este rezervată entităților autorizate de Banco de Portugal, banca centrală a Republicii Portugheze. Aceasta înseamnă că desfășurarea acestei activități este permisă numai entităților care au făcut obiectul unui proces de autorizare sau de recunoaștere (în cazul instituțiilor financiare autorizate în alte state membre ale Uniunii Europene) de către Banco de Portugal. În cadrul acestui proces, Banco de Portugal verifică respectarea unei serii de cerințe care asigură solvabilitatea și capacitatea de a desfășura activități financiare atât a entității, cât și a membrilor principalelor sale organe sociale. Desfășurarea activității financiare de către o entitate neautorizată poate constitui o infracțiune și reprezintă o încălcare gravă, pedepsită cu amendă, printre alte sancțiuni, în conformitate cu Decretul-lege nr. 298/92 din 31 decembrie 1992 privind cadrul juridic al instituțiilor de credit și al societăților financiare.

Banco de Portugal prezintă actele normative relevante (norme naționale, europene și standarde de reglementare ale Banco de Portugal) care reglementează, direct sau indirect, combaterea spălării banilor și a finanțării terorismului (ML/TF). În ceea ce privește chestiunea din solicitarea dumneavoastră, putem evidenția următoarele acte legislative:

- Legea nr. 83/2017 din 18 august 2017, care instituie măsuri de combatere a spălării banilor și a finanțării terorismului, transpunând parțial Directivele 2015/849/UE a Parlamentului European și a Consiliului din 20 mai 2015 și 2016/2258/UE a Consiliului din 6 decembrie 2016, modifică Decretul-lege nr. 48/95 din 15 martie 1995 (Codul penal) și Decretul-lege nr. 110/2018 din 10 decembrie 2018 (Codul proprietății industriale), coroborate cu Circulara nr. CC/2024/00000052 (Recomandări sau orientări generice | Proceduri de

actualizare a elementelor de identificare în temeiul Legii nr. 83/2017 din 18 august, menționată mai sus);

- Legea nr. 46/2018 din 13 august 2018 de stabilire a cadrului juridic privind securitatea spațiului cibernetic, de transpunere a Directivei (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsurile pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în întreaga Uniune;
- Decretul-lege nr. 91/2018 din 12 noiembrie 2018 privind cadrul juridic pentru serviciile de plată și moneda electronică (RJSPME), care introduce în legislația portugheză Directiva europeană 2015/ 2366/UE privind accesul la activitatea instituțiilor de plată și la prestarea serviciilor de plată, precum și privind accesul la activitatea instituțiilor de monedă electronică și la prestarea serviciilor de emitere de monedă electronică;
- Circulara Banco de Portugal n. CC/2020/00000044, din 7 iulie 2020, prin care se recomandă un set de bune practici aplicabile comercializării produselor și serviciilor bancare de retail (și anume depozite bancare, produse de credit, servicii de plată și monedă electronică) prin canale digitale (online sau mobile);
- Avizul Banco de Portugal nr. 3/2021, din 13 aprilie 2021, care reglementează procesul de înregistrare la Banco de Portugal a entităților care intenționează să desfășoare, pe teritoriul portughez, activități cu active virtuale supuse înregistrării, precum și modificările ulterioare ale elementelor care trebuie înregistrate;
- Decretul-lege nr. 65/2021 din 30 iulie 2021 privind Regulamentul privind cadrul juridic pentru securitatea spațiului cibernetic, referitor la măsurile de asigurare a unui nivel comun ridicat de securitate a rețelelor și a informațiilor în întreaga Uniune și privind punerea în aplicare a reglementărilor europene privind certificarea în materie de securitate cibernetică, pentru:
    - stabilirea măsurilor menite să asigure un nivel comun ridicat de securitate a rețelelor și a informațiilor în întreaga Uniune Europeană;
    - stabilirea cerințelor de securitate a rețelelor și a sistemelor informatice aplicabile administrațiilor publice, operatorilor de infrastructuri critice și operatorilor de servicii esențiale, precum și definirea cerințelor privind notificarea incidentelor de securitate cibernetică aplicabile acestor entități și furnizorilor de servicii digitale;
    - înființarea Centrului Național de Securitate Cibernetică în calitate de Autoritate Națională de Securitate Cibernetică, permițând

implementarea unui cadru național de certificare în domeniul securității cibernetice;
- stabilirea regimului de sancțiuni aplicabil în materie de certificare a securității cibernetice;

- Legea nr. 79/2021 din 24 noiembrie 2021 de transpunere a Directivei (UE) 2019/713 a Parlamentului European și a Consiliului din 17 aprilie 2019 privind combaterea fraudei și a contrafacerii mijloacelor de plată fără numerar;
- Hotărârea Consiliului de Miniștri nr. 106/2022, din 2 noiembrie, de aprobare a Strategiei Naționale de Apărare Cibernetică;
- Avizul Banco de Portugal nr. 1/2023, din 24 ianuarie 2023, de stabilire a aspectelor necesare pentru asigurarea respectării obligațiilor de prevenire a spălării banilor și a finanțării terorismului, în cadrul activității entităților care desfășoară activități cu active virtuale;
- Legea nr. 81/2023 din 28 decembrie, de transpunere a Directivei (UE) 2020/284 a Consiliului, în ceea ce privește introducerea anumitor cerințe pentru prestatorii de servicii de plată;
- Avizul Banco de Portugal nr. 4/2024, din 19 noiembrie 2024, care stabilește obligația de a identifica beneficiarul final în tranzacțiile care utilizează referințe de plată și debitare directă, modificat prin Avizul Banco de Portugal nr. 1/2025; și
- Instrumentul Banco de Portugal nr. 8/2024, din 6 iunie 2024, care stabilește cerințele pentru entitățile supuse supravegherii băncii de a raporta periodic informații către *Banco de Portugal* în domeniul prevenirii spălării banilor și finanțării terorismului.

SPANIA

Printre măsurile introduse în ultimii ani se numără cele implementate de Legea nr. 4/2022 din 25 februarie privind protecția consumatorilor și a utilizatorilor împotriva situațiilor de vulnerabilitate socială și economică. Această lege prevede elaborarea unui plan de măsuri care include, printre altele, atingerea unor niveluri maxime de securitate pentru a proteja utilizatorii serviciilor bancare împotriva furturilor, înșelăciunilor și fraudelor online.

Tot în anul 2022, a fost adoptată Circulara 3/2022 din 30 martie a Băncii Spaniei de modificare a Circularei 2/2016 din 2 februarie adresată instituțiilor de credit privind supravegherea și solvabilitatea, care finalizează adaptarea sistemului juridic spaniol la Directiva 2013/36/UE și la Regulamentul (UE) nr. 575/2013; Circulara 2/2014 din 31

ianuarie adresată instituțiilor de credit privind exercitarea diverselor opțiuni de reglementare prevăzute în Regulamentul (UE) nr. 575/2013 al Parlamentului European și al Consiliului din iunie 2013 privind cerințele prudențiale pentru instituțiile de credit și firmele de investiții și de modificare a Regulamentului (UE) nr. 675/2013 al Parlamentului European și al Consiliului din iunie 2013 privind cerințele prudențiale pentru instituțiile de credit și firmele de investiții și de modificare a Regulamentului (UE) nr. 675/2013 al Parlamentului European și al Consiliului din iunie 2013 privind cerințele prudențiale pentru instituțiile de credit și firmele de investiții și de modificare a Regulamentului (UE) nr. 675/2013. nr. 575/2013 al Parlamentului European și al Consiliului din 26 iunie 2013 privind cerințele prudențiale pentru instituțiile de credit și firmele de investiții și de modificare a Regulamentului (UE) nr. 648/2012 și Circulara 5/2012 din 27 iunie 2012 adresată instituțiilor de credit și furnizorilor de servicii de plată privind transparența serviciilor bancare și creditarea responsabilă.

Această normă a introdus modificări la o circulară anterioară, pentru a permite Băncii Spaniei să adopte norme privind elaborarea și punerea în aplicare a Ordinului EHA/2899/2011 din 28 octombrie privind transparența și protecția clienților serviciilor bancare.

O altă măsură demnă de menționat este Circulara 4/2021, din 25 noiembrie, a Băncii Spaniei adresată instituțiilor de credit și altor instituții supravegheate, privind modelele de declarații confidențiale privind conduita pe piață, transparența și protecția clienților, precum și privind registrul reclamațiilor.

Pe de altă parte, în domeniul judiciar, instanțele spaniole acordă o importanță din ce în ce mai mare rolului și responsabilității băncilor în schemele de fraudă împotriva clienților lor. Pentru un exemplu recent, puteți consulta următorul articol de presă, care conține hotărârea și este disponibil în limba spaniolă: Advertencia judicial a los bancos ante el auge de las estafas: «Los clientes son las víctimas y las entidades deben responder» | El Correo.

ȚĂRILE DE JOS

În prezent, există o serie de acte normative care prevăd că băncile trebuie să raporteze tranzacțiile neobișnuite ca atare. Tranzacțiile sunt considerate neobișnuite atunci când există suspiciuni că ar fi legate de fraudă sau escrocherie. Acest lucru este prevăzut la articolul 16 din Legea privind prevenirea spălării banilor și finanțării terorismului (Wet ter voorkoming van witwassen en financieren van terrorisme).

Începând cu 2025/2026, Autoritatea olandeză pentru piețele financiare (AFM) și-a intensificat supravegherea asupra modului în care băncile utilizează inteligența artificială și algoritmii pentru a detecta fraudele.

Băncile sunt acum obligate să își cartografieze aplicațiile de AI și să se asigure că acestea sunt „controlabile și explicabile”. Acest lucru înseamnă că băncile nu pot pur și simplu să susțină că nu au observat un model fraudulos; ele trebuie să demonstreze că sistemele lor de monitorizare sunt suficient de robuste pentru a detecta comportamente neobișnuite (cum ar fi un transfer brusc de valoare mare din contul unui client în vârstă înaintată la ora 3:00 dimineața).

Legea privind reziliența operațională digitală (DORA), aplicabilă începând cu 2025, obligă băncile să mențină standarde mai ridicate pentru gestionarea riscurilor ICT, asigurându-se că sistemele de detectare a fraudelor nu dau greș în perioadele de vârf sau în cazul atacurilor cibernetice.

Sub îndrumarea Asociației Bancare Olandeze (NVB) și ca răspuns la presiunile parlamentare, băncile au înăsprit barierele tehnice pentru a preveni fraudele de mare valoare legate de „plățile push autorizate” (APP).

Dacă un client dorește să-și mărească limita zilnică de transfer, majoritatea băncilor olandeze impun acum o perioadă de așteptare obligatorie de 4 ore înainte ca noua limită să devină activă. Această „perioadă de reflecție” este concepută pentru a contracara presiunea psihologică exercitată de escroci în timpul fraudelor prin falsificarea identității telefonice în timp real sau prin „help desk”.

O schimbare semnificativă a avut loc odată cu punerea în aplicare a Regulamentului UE 2024/886. Deși băncile olandeze dispuneau deja de un sistem de „verificare a numelui” (IBAN-Naam Controle), acesta a devenit acum o cerință legală obligatorie pentru toate transferurile instant și SEPA.

Băncile trebuie să verifice dacă numele furnizat de expeditor corespunde cu cel al titularului contului IBAN. În cazul unei neconcordanțe, banca are obligația legală de a emite un avertisment înainte de finalizarea tranzacției.

Dacă o bancă nu furnizează acest serviciu de verificare și un client este victima unei fraude, banca poate fi trasă la răspundere pentru pierderea suferită.

Deși nu este o lege nouă, acordul voluntar de despăgubire încheiat între marile bănci olandeze (ING, Rabobank, ABN AMRO, Volksbank) și guvern a devenit standardul de facto.

În trecut, băncile au folosit „neglijența gravă” ca motiv pentru a refuza rambursările. Cu toate acestea, hotărârile recente ale instanțelor olandeze și orientările AFM au ridicat pragul pentru ceea ce constituie neglijență. Cu excepția cazului în care un client a fost

incredibil de imprudent (de exemplu, divulgând codul PIN și cardul bancar fizic), se așteaptă din ce în ce mai mult ca băncile să ramburseze sumele de bani cu care au fost înșelate victimele „spoofingului” sofisticat (în care escrocii se dau drept funcționari bancari).

Asociația Bancară Olandeză (NVB) a lansat inițiativa „NextGen Gatekeepers” în 2025. Aceasta obligă băncile să nu se mai limiteze doar la analizarea propriilor date.

Băncile partajează acum date specifice într-un mod mai activ cu companiile de telecomunicații și cu poliția pentru a bloca linkurile frauduloase din SMS-uri (smishing) înainte ca acestea să ajungă la telefonul clientului.

Guvernul olandez promovează un model de „responsabilitate în lanț” în care băncile, în calitate de gardieni finali, suportă povara financiară dacă permit efectuarea unei tranzacții frauduloase atunci când sunt disponibile semnale din alte sectoare de analiză (cum ar fi indiciile că un număr de telefon este cunoscut ca fiind fraudulos).

WEBOGRAFIE

AUSTRIA

https://www.fma.gv.at/en/from-1-january-2026-the-fma-is-the-new-supervisory-authority-for-monitoring-and-imposing-financial-sanctions/#:~:text=The%20FMA%20becomes%20the%20central,instance%20for%20financial%20market%20integrity.

https://www.bmf.gv.at/en/topics/combating-fraud.html

BELGIA

https://www.brusselstimes.com/1785663/money-transfers-eu-banks-now-required-to-check-names-and-ibans-match

https://www.nbb.be/doc/ts/publications/fmi-and-paymentservices/2025/fmi-2025_payments.pdf

https://www.ing.be/en/business/news/secure-business/invoice-fraud-easy-to-detect#:~:text=From%201%20January%202026%2C%20electronic,in%20PDF%20or%20Word%20format.

https://gasa.org/

https://gasa.org/events/summit/gass-europe-2026

FINLANDA

https://www.finanssiala.fi/en/news/banks-and-operators-new-anti-fraud-model-enables-faster-response-times/#:~:text=Under%20the%20leadership%20of%20OP,collection%20and%20rapid%20information%20sharing.

https://www.finanssivalvonta.fi/en/publications-and-press-releases/supervision-releases/2025/follow-up-assessment-of-online-payment-security--recommendations-for-credit-institutions/#:~:text=Based%20on%20a%20thematic%20review,limits%20on%20their%20credit%20transfers.

https://www.finanssiala.fi/en/columns/is-eu-legislation-fighting-or-fostering-fraud/#:~:text=This%20verification%20requirement%20was%20first,instant%20payments%20from%20October%202025.

https://www.finanssivalvonta.fi/en/publications-and-press-releases/Press-release/2025/fin-fsa-recommends-measures-for-banks-to-take-to-improve-online-payment-security--eus-instant-payments-regulation-speeds-up-payments-but-also-increases-risks/#:~:text=The%20FIN%2DFSA%20has%20published,further%20development%20of%20fraud%20monitoring.

https://www.op.fi/en/op-financial-group/about-us/op-in-brief

https://www.europarl.europa.eu/news/en/press-room/20251121IPR31540/payment-services-deal-more-protection-from-online-fraud-and-hidden-fees#:~:text=To%20protect%20customers%20from%20impersonation,police%20and%20informs%20their%20PSP.

https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202408.ro.pdf

https://www.ecb.europa.eu/press/pr/date/2024/html/ecb.pr240801~f21cc4a009.ro.html

https://www.consilium.europa.eu/en/press/press-releases/2024/05/30/anti-money-laundering-council-adopts-package-of-rules/

FRANȚA

https://acpr.banque-france.fr/system/files/2025-12/20251217_ACPR_report_on_rebound_accounts_EN.pdf

https://www.banque-france.fr/en/governors-interventions/our-compass-preventing-retail-payments-fraud-adapt-technical-defenses-and-extend-scope-and-reach

https://fincrimecentral.com/france-banks-money-laundering-measures-2025/

https://lebot-avocat.com/en/law-2025-1058-november-2025-fight-against-banking-fraud/#:~:text=By%20strengthening%20prevention%20mechanisms%20and,authentication%20procedures%20to%20deflect%20responsibility.

GERMANIA

https://www.bafin.de/EN/Verbraucher/Finanzbetrug/finanzbetrug_node_en.html;jsessionid=686C6727BB72A61766099A776388BC52.internet002

https://www.acams.org/en/news/german-regulator-fines-jpmorgan-record-e45-million-over-late-str-filings

https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Massnahmen/60b_KWG_84_WpIG_und_57_GwG/neu/meldung_2025_11_06_jp_morgan_se_en.html

https://www.bafin.de/EN/DieBaFin/BaFin-Ziele/Ziele_2026_2029/Ziele2026_2029_en.html

https://www.landesrecht-bw.de/bsbw/document/NJRE001628864

POLONIA

https://rf.gov.pl/en/online-safety-beware-of-cybercriminals/

https://criminallawpoland.com/specialization/scams/

https://uodo.gov.pl/en/553/1990

PORTUGALIA

https://www.bportugal.pt/en/page/unauthorised-activity

https://www.cncs.gov.pt/en/proteja-se-contra-a-fraude-nas-operacoes-bancarias-e-pagamentos-online

https://www.apb.pt/en/banking-customer/online-security

https://clientebancario.bportugal.pt/en/consumer-disputes

SPANIA

https://www.bde.es/wbe/es/areas-actuacion/normativa/regulacion-sistema-financiero/old_regulacion-estatal-sistema-financiero/transparencia___da6512ff3c61281.html

https://clientebancario.bde.es/pcb/es/menu-horizontal/podemosayudarte/normativa/

https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=322_Codigo_de_Lucha_contra_el_Fraude_y_la_Corrupcion&tipo=C&modo=2

ȚĂRILE DE JOS

https://www.afm.nl/en/sector/actueel/2026/jan/pb-agenda-2026#:~:text=The%20AFM%20asks%20institutions%20to,making%20logic%2C%20and%20actively%20report

https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

https://privacy-web.nl/en/nieuws/ing-compenseert-slachtoffers-van-spoofing/

https://www.betaalvereniging.nl/en/knowledge-base/iban-and-bic/iban-name-check/#:~:text=Legally%20required&text=This%20must%20therefore%20also%20work,come%20from%20different%20SEPA%20countries.

https://www.nvb.nl/media/czxdynla/nextgen-poortwachters-position-paper.pdf