



Deputat în Parlamentul Republicii Moldova

Domnului CARP Lilian,

**Președintele Comisiei de anchetă pentru examinarea
fenomenului escrocheriilor telefonice, financiare, digitale și
pentru evaluarea eficienței măsurilor de prevenire și
combateră a acestora**

PROPUNERI SUPLIMENTARE

la Raportul Comisiei de anchetă privind examinarea fenomenului escrocheriilor
telefonice, financiare și digitale

Prezentele propuneri sunt formulate în baza analizei materialelor investigative disponibile privind activitatea rețelelor infracționale care operează platforme frauduloase de investiții, precum și a tiparelor operaționale identificate în cadrul destructurării acestor grupări. Informațiile obținute relevă elemente structurale ale fenomenului care nu sunt suficient abordate în Raportul de bază și care necesită intervenții legislative specifice.

1. Reglementarea activității de intermediere publicitară (affiliate marketing) în domeniul serviciilor financiare

Analiza rețelelor destructurate demonstrează că platformele frauduloase de investiții utilizează sistematic rețele de intermediari publicitari (denumiți „afiliați”) care, contra unui comision per client atras, direcționează cetățenii către platformele respective prin publicitate pe rețelele sociale, motoarele de căutare și alte canale digitale. Acești intermediari operează fără nicio formă de licențiere sau responsabilitate juridică, deși contribuția lor la captarea victimelor este determinantă.

Se propune:

- a) Completarea Legii nr. 171/2012 privind piața de capital cu un capitol distinct privind intermedierea publicitară în domeniul serviciilor financiare, care să instituie obligativitatea înregistrării și licențierii persoanelor care desfășoară activitate de atragere a clienților pentru prestatorii de servicii financiare și de investiții;
- b) Instituirea răspunderii solidare a intermediarului publicitar cu prestatorul de servicii de investiții pentru prejudiciul cauzat clienților atrași, atunci când intermediarul nu a verificat existența autorizației prestatorului;
- c) Obligarea platformelor de publicitate online (rețele sociale, motoare de căutare) să solicite dovada autorizației CNPF înainte de acceptarea publicității pentru servicii financiare destinate cetățenilor Republicii Moldova.

2. Combaterea operării simultane sub identități multiple (multi-brand)

Investigațiile relevă că o singură infrastructură informatică și operațională poate deservi simultan zeci de „mărci” diferite de platforme de investiții, fiecare prezentându-se ca o entitate juridică distinctă. Această practică permite grupărilor infracționale să continue activitatea sub un alt nume imediat după blocarea uneia dintre mărci, făcând ineficiente măsurile punctuale de blocare.

Se propune:

- a) Completarea Legii privind prevenirea și combaterea spălării banilor și finanțării terorismului nr. 308/2017 cu obligația pentru prestatorii de servicii de plată de a identifica și raporta către SPCSB situațiile în care mai mulți comercianți aparent distincți utilizează aceeași infrastructură de procesare, aceleași conturi de decontare sau aceiași beneficiari efectivi;
- b) Acordarea competenței CNPF de a solicita blocarea simultană a tuturor platformelor afiliate tehnic sau operațional unei entități identificate ca frauduloasă, nu doar a celei care face obiectul plângerii individuale;
- c) Modificarea Codului penal, art. 190 (Escrocheria), prin adăugarea unei circumstanțe agravante pentru săvârșirea faptei prin utilizarea simultană a mai multor identități comerciale fictive în scopul eludării măsurilor de blocare.

3. Reglementarea persoanelor implicate în mișcarea fondurilor ilicite („catâri financiari”)

Datele din investigații indică existența unor persoane fizice care, în mod organizat, facilitează transferul fondurilor sustrase prin utilizarea conturilor personale, a cardurilor bancare și a portofelelor electronice. Aceste persoane — cunoscute în terminologia internațională drept „money mules” — acționează fie din ignoranță, fie în cunoștință de cauză, constituind o verigă esențială în lanțul de spălare a banilor.

Volumul financiar gestionat de aceste persoane poate atinge sume de ordinul milioanelei per individ.

Se propune:

- a) Completarea Codului penal cu un articol distinct (propunere: art. 243¹) privind facilitarea transferului de fonduri provenite din infracțiuni, care să incrimineze separat punerea la dispoziție a conturilor, cardurilor sau portofelelor electronice personale în scopul tranzitării fondurilor aparținând terților, în condițiile în care persoana cunoaște sau trebuie să cunoască originea ilicită a acestora;
- b) Instituirea prezumției de cunoaștere a originii ilicite atunci când volumul tranzacțiilor tranzitate prin contul persoanei depășește semnificativ veniturile declarate sau când tranzacțiile prezintă tipare specifice (transferuri rapide succesive, multiple surse către o singură destinație);
- c) Completarea Legii nr. 308/2017 cu obligația instituțiilor financiare de a aplica măsuri sporite de verificare și de a raporta automat către SPCSB conturile persoanelor fizice prin care tranzitează lunar sume ce depășesc echivalentul a 50.000 MDL din surse multiple neidentificate.

4. Obligații specifice pentru furnizorii de servicii de active virtuale (VASP)

Materialele examinate confirmă utilizarea intensivă a criptomonedelor — în special a stablecoin-urilor de tip USDT pe rețeaua Tron (TRC-20) — ca instrument principal de colectare a fondurilor de la victime și de disimulare ulterioară a traseului financiar. Platformele frauduloase oferă victimelor instrucțiuni detaliate pentru achiziționarea și transferul de criptomonede, ceea ce demonstrează integrarea profundă a activelor virtuale în schema infracțională.

Se propune:

- a) Adoptarea urgentă a cadrului legislativ primar privind reglementarea furnizorilor de servicii de active virtuale (VASP) în conformitate cu Recomandările FATF (în special Recomandarea 15 și Nota Interpretativă aferentă), cu stabilirea autorității de supraveghere (BNM sau CNPF);
- b) Instituirea obligației pentru VASP de a aplica regula transferurilor (travel rule) și de a raporta către SPCSB toate tranzacțiile cu active virtuale care depășesc echivalentul a 1.000 EUR sau care prezintă indicatori de risc (destinații în jurisdicții necooperante, conversii rapide, fragmentare deliberată);
- c) Completarea Codului de procedură penală cu dispoziții specifice privind sechestrarea și confiscarea activelor virtuale, inclusiv procedura de obținere a cheilor private, cooperarea cu bursele de criptomonede și mecanismul de conservare a probelor digitale pe blockchain;

- d) Încheierea de acorduri de cooperare cu principalele burse de criptomonede (Binance, OKX, Bybit) pentru asigurarea răspunsului rapid la solicitările autorităților moldovenești privind înghețarea fondurilor.

5. Mecanism de protecție a victimelor împotriva re-victimizării

Practica investigativă internațională demonstrează că listele de victime ale platformelor frauduloase sunt comercializate către alte grupări infracționale, care contactează ulterior aceleași persoane oferindu-le „servicii de recuperare” a banilor pierduți (așa-numitele „recovery scams”). Victima este astfel supusă unui al doilea ciclu de fraudare, adesea cu prejudicii comparabile primei înșelăciuni.

Se propune:

- a) Instituirea unui mecanism de alertare proactivă, prin care instituțiile financiare și operatorii telecom, la sesizarea organelor de drept, să notifice victimele identificate despre riscul de re-contactare frauduloasă și despre canalele oficiale de raportare;
- b) Incriminarea expresă a comercializării sau transmiterii bazelor de date conținând informații despre victimele infracțiunilor financiare, ca infracțiune distinctă (propunere: completarea art. 259 Cod penal — violarea dreptului la corespondență — sau introducerea unui articol separat);
- c) Obligarea prestatorilor de servicii financiare de a aplica un regim de monitorizare sporită asupra conturilor aparținând persoanelor identificate anterior ca victime ale fraudelor, pe o perioadă de 12 luni, cu alertare automată la detectarea unor tipare de tranzacții similare.

6. Perioada obligatorie de reflecție pentru transferurile de valoare ridicată

Tiparele identificate în cadrul platformelor investigate arată o progresie controlată a sumelor depuse de victime: depozite inițiale mici (50-200 USD), urmate de sume tot mai mari pe măsură ce „agentul” câștigă încrederea victimei. Prejudiciul final per victimă poate atinge zeci de mii de dolari. Introducerea unei perioade obligatorii de reflecție pentru transferurile atipice ar putea întrerupe acest ciclu de escaladare.

Se propune:

- a) Modificarea Legii nr. 114/2012 privind serviciile de plată și moneda electronică prin introducerea obligației pentru prestatorii de servicii de plată de a aplica o perioadă de reflecție de minimum 24 de ore pentru transferurile care depășesc de 3 ori media lunară a tranzacțiilor clientului sau care sunt destinate unor beneficiari noi situați în jurisdicții cu risc ridicat;

- b) În perioada de reflecție, prestatorul va contacta clientul prin canalul de comunicare verificat (apel telefonic, nu SMS) pentru confirmarea intenției de transfer și pentru informarea acestuia despre riscurile asociate;
- c) Excluderea de la aplicarea perioadei de reflecție a transferurilor între conturile aceluiasi titular, a plăților recurente și a transferurilor către beneficiari verificați anterior.

7. Registrul platformelor neautorizate și blocarea accesului

În prezent, nu există un mecanism centralizat prin care cetățenii să poată verifica dacă o platformă de investiții este autorizată, iar blocarea resurselor frauduloase se face punctual și cu întârziere. Deoarece rețelele investigate operează simultan sub zeci de denumiri comerciale și domenii internet, este necesară o abordare sistematică.

Se propune:

- a) Crearea și publicarea de către CNPF a unui Registru Național al Platformelor Neautorizate, actualizat săptămânal, care să conțină denumirile comerciale, domeniile internet și aplicațiile mobile asociate entităților neautorizate identificate;
- b) Obligarea furnizorilor de servicii de acces la internet (ISP) de a implementa mecanisme tehnice de avertizare (pagină de avertizare prealabilă accesului) pentru domeniile incluse în Registru, conform modelului implementat deja de mai multe state membre UE;
- c) Integrarea Registrului cu sistemele anti-fraud ale instituțiilor financiare, astfel încât transferurile destinate entităților din Registru să fie automat semnalate și supuse verificării suplimentare.

8. Responsabilizarea prestatorilor de servicii de plată care procesează fondurile platformelor frauduloase

Investigațiile demonstrează că platformele frauduloase utilizează zeci de procesatori de plăți și canale de colectare a fondurilor (portofele electronice, procesatori de carduri, servicii de transfer). Unii dintre acești prestatori nu efectuează verificările minime de due diligence asupra comercianților pe care îi deservesc sau ignoră semnalele evidente de fraudă (rate anormal de ridicate de dispute, volume disproporționate față de activitatea declarată).

Se propune:

- a) Completarea cadrului de reglementare al BNM cu obligația pentru prestatorii de servicii de plată de a efectua verificări periodice ale comercianților acceptați, inclusiv monitorizarea ratei de dispute (chargebacks) și a reclamațiilor, cu obligația de a rezilia relația comercială la depășirea pragurilor stabilite;

- b) Introducerea răspunderii administrative și financiare a prestatorului de servicii de plată care continuă procesarea tranzacțiilor pentru un comerciant după primirea unei notificări din partea autorităților competente privind caracterul fraudulos al activității acestuia;
- c) Obligarea restituirii integrale a sumelor procesate către victimele identificate, în cazul în care prestatorul nu poate demonstra efectuarea verificărilor rezonabile (inversarea sarcinii probei privind due diligence-ul).

9. Baza de date națională a indicatorilor de fraudă

Lipsa unui sistem centralizat de partajare a indicatorilor de fraudă (numere de telefon, conturi bancare, domenii internet, adrese de criptomonede, adrese IP) între toate instituțiile implicate generează întârzieri în reacție și permite utilizarea repetată a acelorași instrumente de către infractori.

Se propune:

- a) Crearea, sub coordonarea Centrului Național Antifraudă propus, a unei baze de date operaționale care să conțină: numerele de telefon utilizate în apeluri frauduloase, IBAN-urile și conturile implicate în transferuri suspecte, domeniile internet și adresele IP ale platformelor frauduloase, adresele de criptomonede utilizate pentru colectarea fondurilor;
- b) Asigurarea accesului în timp real pentru toți participanții la HUB (bănci, operatori telecom, organe de drept), cu protocoale diferențiate de acces în funcție de nivelul de clasificare a informațiilor;
- c) Obligarea tuturor instituțiilor financiare de a interoga automat baza de date la procesarea transferurilor și de a aplica măsuri de verificare sporită atunci când beneficiarul figurează în baza de date.

10. Protecția angajaților și colaboratorilor care denunță activitatea infracțională a call-centrelor

Rețelele infracționale de tip call-centru angajează, de regulă, un număr semnificativ de persoane — operatori, manageri, personal tehnic — dintre care unele pot fi dispuse să coopereze cu organele de drept. În absența unui cadru clar de protecție, aceste persoane nu au stimulente suficiente pentru a denunța activitatea infracțională.

Se propune:

- a) Extinderea sferei de aplicare a Legii nr. 122/2018 privind avertizorii de integritate pentru a acoperi explicit persoanele care denunță activitatea infracțională a entităților de tip call-centru, platforme de investiții sau alte structuri implicate în fraude financiare;
- b) Introducerea posibilității de reducere substanțială a pedepsei (până la exonerare în cazul cooperării depline) pentru angajații call-centrelor care, înainte de inițierea

urmăririi penale sau în faza incipientă a acesteia, oferă informații determinante pentru identificarea organizatorilor, beneficiarilor și a infrastructurii utilizate;

- c) Alocarea resurselor necesare pentru programele de protecție a martorilor în cazurile transfrontaliere de fraudă organizată.

11. Modificări legislative specifice necesare

Implementarea propunerilor de mai sus necesită modificarea sau completarea următoarelor acte normative:

Actul normativ	Modificarea propusă
Codul penal (nr. 985/2002)	Art. 190 — adăugarea circumstanțelor agravante privind multi-brand și comunicații electronice Art. nou 243 ¹ — facilitarea transferului de fonduri ilicite (money mules) Art. 259 sau articol nou — comercializarea datelor victimelor
Codul de procedură penală (nr. 122/2003)	Capitol nou privind sechestrarea și confiscarea activelor virtuale, procedura de conservare a probelor pe blockchain
Legea privind piața de capital (nr. 171/2012)	Capitol nou privind intermedierea publicitară în domeniul serviciilor financiare, licențierea afiliaților
Legea privind serviciile de plată (nr. 114/2012)	Articol nou privind perioada obligatorie de reflecție pentru transferurile atipice
Legea privind prevenirea spălării banilor (nr. 308/2017)	Completare privind raportarea operațiunilor multi-brand, praguri de raportare pentru conturile de tranzit, obligații VASP
Legea privind avertizorii de	Extinderea sferei de aplicare pentru denunțătorii din call-centre și platforme frauduloase

integritate (nr. 122/2018)	
Legea comunicațiilor electronice (nr. 72/2025)	Completare privind obligația ISP de implementare a mecanismelor de avertizare pentru domeniile din Registrul platformelor neautorizate

PUNCT FOCAL NAȚIONAL ANTI-FRAUDĂ

Principalele atribuții și componența

1. Crearea Punctului Focal Național Anti-Fraudă, care să funcționeze permanent, în regim online și în timp real, ca centru unic de coordonare a combaterii fraudelor telefonice și online.

2. Componența obligatorie:

- Ministerul Afacerilor Interne (MAI);
- Serviciul de Informații și Securitate (SIS);
- Procuratura Generală și PCCOCS;
- Inspectoratul General al Poliției (IGP);
- Serviciul Prevenirea și Combaterea Spălării Banilor (SPCSB);
- Agenția pentru Securitate Cibernetică (ASC);
- Banca Națională a Moldovei (BNM);
- instituțiile financiar-bancare;
- operatorii de telefonie mobilă și internet;
- Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației (ANRCETI);
- alte instituții competente, în funcție de necesități.

3. Coordonarea în timp real a schimbului de informații între toate instituțiile participante, inclusiv privind tentativele de fraudă, conturile suspecte, cartelele SIM, numerele telefonice, infrastructura digitală și fluxurile financiare.

4. Blocarea imediată a numerelor utilizate pentru spoofing, a platformelor frauduloase, a conturilor bancare și a altor instrumente folosite în activități infracționale, în limitele competențelor legale.
5. Implementarea obligatorie, de către toți operatorii de telefonie, a sistemelor tehnice și software de autentificare a originii apelurilor și de blocare a spoofing-ului, conform standardelor internaționale.
6. Introducerea unui mecanism unic de alertare rapidă a populației, prin SMS, aplicații mobile, notificări bancare și alte canale oficiale, în limbile română și rusă.
7. Monitorizarea permanentă a noilor tipologii de fraudă și elaborarea de recomandări operative pentru toate instituțiile participante.
8. Coordonarea operațiunilor cibernetice defensive și, în condițiile legii, a măsurilor ofensive împotriva infrastructurii utilizate de grupările criminale organizate.
9. Elaborarea rapoartelor publice periodice privind numărul victimelor, prejudiciile reale, fondurile recuperate, cauzele penale și eficiența măsurilor întreprinse.
10. Prezentarea periodică în Parlament a rezultatelor activității Punctului Focal Național Anti-Fraudă și a propunerilor legislative necesare pentru combaterea eficientă a fraudelor telefonice și online.

Prezentele propuneri suplimentare vizează acoperirea lacunelor identificate în procesul de analiză a materialelor investigative și sunt orientate către eliminarea condițiilor structurale care permit funcționarea neîntreruptă a rețelelor infracționale. Fără abordarea sistemică a tuturor verigilor lanțului — de la recrutarea victimelor prin intermediari publicitari, până la disimularea finală a fondurilor prin active virtuale — eficiența măsurilor de combatere va rămâne limitată, iar prejudiciul continuu al cetățenilor se va menține pe o traiectorie ascendentă.

Cu respect,

Renato USATÎI