

PROGRAMUL
CU PRIVIRE LA PREVENIREA COMBATAREA SPĂLĂRII BANILOR SI
FINANȚĂRII TERORISMULUI APLICAT
IN CADRUL OCN BEST INVEST SRL
(actualizat conform prevederilor normative în vigoare)

I. DISPOZITII GENERALE

1.1. Programul cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului este elaborat în corespundere cu prevederile:

- a) *Legii cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului nr.308 din 22.12.2017, cu modificările și completările ulterioare (în continuare Lege);*
- b) *Legii cu privire la organizațiile de creditare nebancaară Nr. 1 din 16.03.2018;*
- c) *Regulamentul cu privire la cerințele privind prevenirea și combaterea spălării banilor și finanțării terorismului în activitatea instituțiilor financiare nebancaare aprobat prin Hotărârea Comitetului Executiv al BNM nr. 280 din 07.11.2024;*
- d) *Ghidul privind identificarea activităților sau tranzacțiilor suspecte de spălare a banilor aprobat prin Ordinul Serviciul Prevenirea și Combaterea Spălării Banilor nr. 15 din 20.07.2023;*
- e) *Ghidul privind identificarea tranzacțiilor și activităților suspecte de finanțare a terorismului aprobat prin Ordinul Serviciul Prevenirea și Combaterea Spălării Banilor nr. 16 din 20.07.2023;*
- f) *Metodologia cu privire la modul de completare și transmitere a formularelor speciale privind activitățile sau tranzacțiile care cad sub incidența Legii nr. 308/2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului aprobate prin Ordinul Serviciul Prevenirea și Combaterea Spălării Banilor nr. 20/2023 din 03.08.2023;*
- g) *Ordinul Serviciului de Informații și Securitate al RM Nr. 2 din 15-01-2016 privind listele persoanelor, grupurilor și entităților implicate în activități teroriste;*
- h) *Ordinul Serviciul Prevenirea și Combaterea Spălării Banilor nr. 22 din 15.08.2023 cu privire la aprobarea listei funcțiilor publice importante la nivel național care determină calitatea de persoană expusă politic;*
- i) *Ghidul privind identificarea și monitorizarea persoanelor expuse politic și indicilor de risc privind persoanele expuse politic (PEP) aprobat prin Ordinul Serviciul Prevenirea și Combaterea Spălării Banilor nr. 23 din 06.09.2023;*
- j) *Actele normative interne ale OCN Best Invest SRL în continuare Companie.*

1.2. Scopul prezentului Program este de a administra precaut riscul de conformitate întru evitarea pierderilor pe care le-ar putea suferi Compania ca urmare a riscurilor asociate spălării banilor - riscul legal, riscul imaginii, riscul operațional, riscul tehnologiilor informationale.

1.3. Prezentul Program definește cadrul și principiile de bază de care se conduce Compania și angajații săi pentru prevenirea implicării (intentionat sau neintentionat) în activități de spălare de bani și finanțare a terorismului.

1.4. Elementele principale ale Programului sunt stabilirea criteriilor de evaluare a riscurilor aferente spălării banilor; implementarea unui sistem de gestionare a riscurilor; abordarea bazată pe risc a clienților la etapa de acceptare, identificare și monitorizare a tranzacțiilor acestora; raportarea activităților și tranzacțiilor care cad sub incidența Legii, inclusiv tranzacțiilor suspecte, aplicarea procedurilor specifice de control intern.

IL. NOTIUNI PRINCIPALE UTILIZATE

2.1. În sensul prezentului Program următoarele noțiuni semnifică:

- **spălare a banilor** - acțiuni, stabilite în Codul penal art.243, orientate spre atribuirea unui aspect legal sursei și provenienței veniturilor ilicite ori spre tănuirea originii sau apartenenței unor astfel de venituri;

- **finanțare a terorismului** - acțiuni, stabilite în Codul penal art 279, orientate spre punerea la dispoziție ori spre colectarea intenționată, efectuată de orice persoană fizică sau persoană juridică prin orice metodă, direct sau indirect, a bunurilor de orice natură, dobândite prin orice mijloc, fie spre oferirea de suport material sau financiar de orice natură, în scopul utilizării acestor bunuri ori servicii sau cunoștința faptului că vor fi utilizate, parțial sau integral, în activități teroriste;

- **bunuri** - mijloace financiare, orice categorie de valori (active) corporale sau incorporale, mobile sau imobile tangibile sau intangibile, acte sau alte instrumente juridice în orice formă, inclusiv în formă electronică ori digitală, care atestă un titlu ori un drept, inclusiv orice cotă (interes) cu privire la aceste valori (active);

- **venituri ilicite** - bunuri destinate, folosite sau rezultate, direct sau indirect, din săvârșirea unei infracțiuni, orice beneficiu obținut din aceste bunuri, precum și bunuri convertite sau transformate, parțial sau integral, din bunuri destinate, folosite sau rezultate din săvârșirea unei infracțiuni și din beneficiul obținut din aceste bunuri;

- **beneficiar efectiv** - persoană fizică ce controlează în ultimă instanță o persoană fizică sau juridică ori persoană în al cărei nume se realizează o tranzacție sau se desfășoară o activitate și/sau care deține direct sau indirect dreptul de proprietate sau controlul asupra a cel puțin 25% din acțiuni sau din dreptul de vot al persoanei juridice;

- **persoane expuse politic** - persoane fizice care exercită sau care au exercitat funcții publice importante la nivel național și/sau internațional, precum și membrii familiilor și persoanele asociate lor;

- **persoane fizice care exercită funcții publice importante la nivel internațional** - sunt persoane fizice care dețin sau care au deținut funcțiile de : șefi de state, de guverne și de cabinete de miniștri; viceministri, membri ai guvernelor, șefi ai cancelariilor de stat; deputați; persoane de conducere ale partidelor politice; judecători ai curților supreme de justiție; membri ai curților de conturi și consiliilor băncilor naționale; ofițeri cu grade militare superioare și supreme și funcții de conducere de nivel înalt; membri ai organelor de conducere și de administrare ale întreprinderilor cu capital de stat; membri ai familiilor regale; ambasadori și personal de rang superior din cadrul misiunilor diplomatice; directori, vicedirectori și membrii consiliilor de administrare a organizațiilor internaționale.;

- **Persoane fizice care exercită funcții publice importante la nivel național** - sunt persoane fizice care dețin sau care au deținut funcțiile de: demnitate publică proeminente în conformitate cu legislația națională; membrii organelor de conducere și de administrare ale întreprinderilor de stat, întreprinderilor municipale; membrii organelor de conducere și de administrare ale societăților comerciale cu capital majoritar de stat; persoane de conducere ale partidelor politice; ofițeri cu grade militare superioare și supreme; alte persoane fizice care execută funcții publice importante la nivel național;

- **Membri ai familiilor persoanelor expuse politic** sunt soțul/soția sau copiii și soții/soțiile lor sau concubinul/concubina, părinții unei persoane expuse politic.

- **Persoane asociate persoanelor expuse politic** - sunt persoane despre care este cunoscut că sunt în strânsă legătură cu o persoană expusă politic, fie din punct de vedere social sau profesional, colegi de afaceri, apropiați de afaceri și/sau consilieri personali, în special consultanți financiari sau persoane care acționează într-o capacitate financiar-fiduciară.

- **Persoană cu funcții de conducere de rang superior al entității raportoare** - este un responsabil sau un angajat care deține cunoștințe suficiente privind expunerea instituției la riscul de spălare a banilor și de finanțare a terorismului și care ocupă o funcție suficient de înaltă pentru a lua decizii cu efect asupra acestei expuneri și care nu este necesar să fie întotdeauna un membru al consiliului de administrație.

- **relație de afaceri** – relație profesională sau comercială legată de activitățile prestate de către entitățile raportoare prevăzute la art.4 alin. (1) al Legii, despre care, la momentul stabilirii contactului, se consideră a fi de o anumită durată;

- **activitate sau tranzacție suspectă** – activitate sau tranzacție cu bunuri sau bunuri ilicite, inclusiv cu mijloace financiare și fonduri, despre care entitatea raportoare cunoaște sau indică temei de suspiciune că acțiunile de spălare a banilor, infracțiunile predicat, acțiunile de finanțare a terorismului și a proliferării armelor de distrugere în masă sînt în curs de pregătire, de tentativă, de realizare ori sînt deja realizate;

- **tranzacție** – acțiuni bazate pe înțelegerea prealabilă între două sau mai multe părți, prin care se transferă, se lichidează, se transformă, se plasează bunuri sau se realizează circulația lor ori care reprezintă contravaloarea furnizării unor servicii;

- **tranzacție complexă și neordinară** – tranzacție realizată printr-o singură operațiune sau prin mai multe operațiuni care nu corespund activității ordinare și/sau nu sînt proprii genului de activitate-a clientului;

- **tranzacție ocazională** – tranzacție realizată printr-o singură operațiune sau prin mai multe operațiuni, de către una sau mai multe persoane fizice sau juridice, în lipsa unei relații de afaceri cu entitatea raportoare;

- **tranzacție semnificativă** - tranzacție (operațiune) care depășește limita valorică stabilită în politicile interne ale instituției financiare nebancare luând în considerație riscurile asociate clienților și operațiunilor efectuate;

- **identificatorul unic al companiei (legal entity identifier)** – un cod alfanumeric, alcătuit din 20 caractere, care identifică în mod unic o persoană juridică, stabilit în conformitate cu standardul ISO 17442.

III. DEFINIREA PROCESULUI DE SPĂLARE A BANILOR

3.1. Prin spălarea banilor, conform art.243 al Codului Penal al RM, se înțeleg următoarele acțiuni:

a) convertirea sau transferul bunurilor de către o persoană care știe ori trebuia să știe că acestea constituie venituri ilicite, în scopul de a tăinui sau de a deghiza originea ilicită a bunurilor sau de a ajuta orice persoană, implicată în comiterea infracțiunii principale, de a se sustrage de la consecințele juridice ale acestor acțiuni;

b) tănuirea sau deghizarea naturii, originii, amplasării, dispunerii, transiterii, deplasării proprietății reale a bunurilor ori a drepturilor aferente de către o persoană care știe sau trebuia să știe că acestea constituie venituri ilicite;

c) dobîndirea, deținerea sau utilizarea bunurilor de către o persoană care știe ori trebuia să știe că acestea constituie venituri ilicite;

d) participarea la orice asociere, înțelegere, complicitate prin acordarea de asistență, ajutor sau sfaturi în vederea comiterii acțiunilor prevăzute la lit.a)-c)

3.2. Principalele elemente ale procesului de spălare a banilor sunt:

a) plasarea - mișcarea inițială a mijloacelor bănești sau a altor venituri provenite din activitatea infracțională cu scopul schimbării formei inițiale sau a locului acestora pentru a le face inaccesibile organelor de drept;

b) investirea - separarea de la sursa de proveniență a veniturilor obținute din activitatea criminală prin intermediul diferitor tranzacții financiare;

c) integrarea - utilizarea unei tranzacții legitime pentru a ascunde veniturile ilicite, făcând posibilă întoarcerea la infractor a fondurilor spălate.

3.3. Elementele-cheie la crearea schemelor de spălare de bani sunt:

a) anonimatul - tranzacțiile par a fi obișnuite, astfel încât nu atrag atenția asupra lor;

b) viteza - circulația rapidă a valorilor, pentru a nu putea fi detectate;

c) complexitatea - dificultatea urmăririi sursei inițiale;

d) secretul - transferul valorilor spre locuri unde implementarea legii nu este ușor de controlat.

IV. CARACTERISTICILE FINANȚĂRII TERORISMULUI

4.1. În procedeele de finanțare a terorismului au fost identificate următoarele etape :

A. OBȚINEREA FONDURILOR/COLECTAREA;

B. TRANSFERUL;

C. DEPOZITAREA;

D. DISTRIBUIREA/FOLOSIREA

A. OBȚINEREA FONDURILOR/COLECTAREA;

Cel mai probabil o organizație teroristă va căuta să strângă fonduri prin :

I. Surse legitime (inclusiv prin entități caritabile, afaceri legitime și autofinanțare)

II. Surse ilicite – activitate criminală;

III. State-sponsori, activități în “state eșuate” sau în state considerate refugii sigure – *safe heavens*

I. Dintre sursele legitime pot fi evidențiate următoarele :

a) Activități caritabile și ONG-uri

Conform unui studiu al Grupului de Acțiune Financiară Internațională (FATF-GAFI), abuzul ONG-urilor sau riscul utilizării necorespunzătoare a acestora se manifestă în cinci moduri diferite:

- Diversificarea donațiilor prin persoane afiliate organizațiilor teroriste;

- Folosirea administratorilor ONG-urilor în scopurile unei organizații teroriste;

- Abuz în utilizarea resurselor pentru a sprijini organizațiile teroriste;

- Asistență pentru recrutare în organizații teroriste;

- Crearea unor organizații ne-guvernamentale fantomă;

b) Activități antreprenoriale legale – veniturile din afaceri și activități comerciale legale sunt utilizate ca sursă de finanțare a terorismului;

c) Autofinanțare – finanțare acordată de familia teroristului sau de către teroriști înșiși, fie din venituri (salarii, economii) sau din surse de capital;

II. Surse ilicite – activitate criminală : contraband, traficul de țigări/droguri /fințe umane/armament.

III. Finanțarea prin state – sponsori, activități în “state eșuate” sau în state considerate refugii sigure – *safe heavens*

În ciuda eforturilor concertate de combatere a terorismului depuse la nivel internațional, rămân teritorii în care nu există un control efectiv sau un *stat de drept* unde acceptarea organizațiilor teroriste și a activităților teroriste este larg răspândită și unde există un sprijin activ pentru scopurile anumitor teroriști sau grupuri.

În ultimii ani, au apărut tendințe noi de finanțare a terorismului :

- Luptătorii teroriști străini (LTS);

- Obținerea fondurilor prin rețele de socializare;

- Produsele și serviciile de plată;

- Exploatarea resurselor naturale.

B. TRANSFERUL

Organizațiile teroriste transferă bani sau active în unul sau mai multe dintre următoarele moduri:

- a) Prin sistemul financiar-bancar principal;
- b) Prin acte de comerț;
- c) Prin curieri denumerar pentru a muta fizic banii;
- d) Prin sisteme alternative de remitere de bani (Western Union, PayPal);
- e) Prin utilizare organizațiilor caritabile/ONG-urilor;
- f) Monede digitale și criptomonedele.

C. DEPOZITAREA – situația în care nu se folosesc imediat fondurile ci sunt depozitate pentru a fi utilizate ulterior;

D. DISTRIBUIREA/FOLOSIREA

Fondurile sau activele colectate sunt folosite pentru :

- a) Operațiuni;
- b) Propagandă și recrutare;
- c) Instruire;
- d) Salarii și compensarea membrilor;
- e) Servicii sociale.

V. RESPONSABILITĂȚI

5.1. În vederea aplicării prevederilor Legii, actelor normative ale organelor cu funcții de supraveghere referitor la elaborarea programelor privind prevenirea și combaterea spălării banilor finanțării terorismului, în cadrul Companiei sunt desemnate persoanele menționate cu următoarele obligații și responsabilități:

(A) Directorul General are următoarele atribuții:

a) determina domeniilor de activitate ale instituției financiare nebancale vulnerabile riscului spălării banilor și finanțării terorismului;

b) desemnează persoanele investite cu atribuții de executare a Legii nr. 308/2017 cu privire la prevenirea și combaterea spălării banilor și finanțarea terorismului, inclusiv cele cu funcții de conducere de rang superior;

c) aproba tranzacțiilor semnificative ale clienților cu grad de risc sporit;

(B) Directorul Financiar, numit prin ordinul Directorului General, persoana investită cu atribuții de executare a Legii, va:

a) elabora măsurile necesare pentru implementarea politicilor și procedurilor de cunoaștere a clienților, inclusiv a celor cu grad de risc sporit;

b) pune în aplicare a programului intern privind prevenirea și combaterea spălării banilor și finanțării terorismului, inclusiv descrierea responsabilităților personalului la diferite nivele ierarhice;

c) pune în aplicare a procedurilor interne privind accesul într-un timp rezonabil al personalului responsabil la informația necesară exercitării obligațiilor de serviciu;

d) remedia deficiențelor identificate în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului, inclusiv raportarea tranzacțiilor suspecte către Serviciul Prevenirea și Combaterea Spălării Banilor;

e) verifica informația primită de la angajații Companiei, implicați în procesul de acordare a creditelor, despre cazurile suspecte relevate și va întocmi încheieri în baza acestora;

f) asigura sistematizarea și ținerea evidenței informației privind cazurile suspecte de spălare a banilor transmise organelor cu funcții de supraveghere;

g) întreprinde măsuri privind prezentarea Serviciului Prevenirea Combaterea Spălării Banilor a informației, inclusiv formularelor speciale, rapoartelor în conformitate cu legislația în domeniu;

h) colaborează cu serviciul de audit extern al Companiei în vederea verificării conformării activității Companiei legislației în vigoare în domeniul prevenirii combaterii spălării banilor și finanțării terorismului;

i) asigura înlăturarea neconformităților identificate în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului;

j) acorda consultații angajaților Companiei cu privire la întrebările apărute în timpul realizării prezentului Program, inclusiv la identificarea și examinarea clienților și evaluarea riscului de spălare a banilor și finanțare a terorismului;

k) lua decizii în baza informației primite;

(C) Inspectorii credite sunt obligați:

a) Să aplice corect procedurile de identificare a clienților, monitorizare continuă a tranzacțiilor efectuate, relațiilor de afacere ale clientului, actualizare și sistematizare a informației despre client pe întreaga perioadă de gestionare a împrumutului;

b) Să cunoască și să respecte prevederile actelor normative în vigoare în domeniul dat, inclusiv cele interne;

c) în cazul depistării unor circumstanțe care denotă caracterul suspect al operațiunilor financiare, în curs de pregătire, realizare sau deja realizate, să anunțe conducerea Companiei, care va examina situația anunțată și va întreprinde măsurile corespunzătoare.

5.2. La identificarea și evaluarea riscurilor de spălare a banilor și de finanțare a terorismului la care poate fi expusă instituția, se iau în considerare următorii factori:

a) scopul inițierii relației de afaceri, care include informații cu privire la tipul produsului solicitat, destinația plății, volumul activelor depuse sau mărimea tranzacțiilor efectuate de client, frecvența tranzacțiilor și durata relației de afaceri.

b) clienții și terții afiliați (de ex. beneficiarii efectivi a clienților/- terților părți), clienți cu structura proprietății și structura de control neobișnuite sau complexe, persoane expuse politic, identificați cu grad de risc sporit, precum și sursa bunurilor și/sau sursa averii deținute de către aceștia;

c) țările de destinație (jurisdicțiile) cu care instituția financiară nebanară efectuează tranzacții, în special, cu niveluri ridicate de criminalitate, corupție sau alte activități infracționale, țările care sunt supuse sancțiunilor, embargourilor sau măsurilor similare instituite de către organizațiile internaționale de profil, țările care nu dispun de sisteme efective de prevenire și combatere a spălării banilor și a finanțării terorismului, care acordă finanțare sau sprijin pentru activități teroriste sau pe teritoriul cărora activează organizații teroriste desemnate, țările (jurisdicțiile) cu risc sporit desemnate/ monitorizate de Grupul de Acțiune Financiară Internațională (GAFI);

d) rețele de distribuție cum ar fi tranzacțiile, produsele și serviciile oferite direct clientului și/sau prin intermediul agenților, intermediarilor în asigurări și/sau în reasigurări, lanțuri lungi de intermediari, vânzarea produselor și serviciilor (la distanță) prin intermediul tehnologiilor electronice online, poștale sau telefonice;

e) volumul obligațiilor asumate, mărimea tranzacțiilor, luând în considerare activitatea instituției financiare nebanară și profilul clienților săi.

VI. ORGANIZAREA CONTROLULUI INTERN ÎNTRU PREVENIREA ȘI COMBATerea SPĂLĂRII BANILOR

6.1. Principiul de bază al organizării controlului intern în domeniul dat este participarea tuturor angajaților Companiei, care sunt implicați în procesul de examinare, acordare și gestionare a împrumuturilor, indiferent de funcția detinută și obligațiile de serviciu, pentru a identifica operațiunile (tranzacțiile) expuse riscului spălării banilor și finanțării terorismului. Competențele și responsabilitățile persoanelor aferente domeniului dat sunt menționate în cap. V al Programului.

6.2. Organizarea controlului intern în cadrul Companiei în vederea prevenirii și combaterii spălării banilor și finanțării terorismului include un complex de metode, proceduri, măsuri ce țin de:

a) identificarea activităților în cadrul cărora Compania poate fi expusă riscului de implicare în tranzacții de spălare a banilor de către elementele criminale;

b) prevenirea cazurilor în care Compania să apară în calitate de instrument în tranzacțiile de spălare a banilor, prin intermediul elaborării politicilor și procedurilor necesare, ținând cont de riscurile aferente spălării banilor și gradul de expunere a anumitor activități ale Companiei la aceste riscuri,

c) lichidarea neajunsurilor depistate în rezultatul controalelor interne și externe, în cadrul executării prevederilor legislației privind prevenirea și combaterea spălării banilor, finanțării terorismului și prezentului Program.

6.3. Obiectul controlului intern este constituit din următoarele domenii:

- a) identificarea clienților;
- b) procedurile de detectare a operațiunilor limitate suspecte;
- c) respectarea cerințelor de monitorizare și raportare;
- d) păstrarea documentelor;
- e) păstrarea confidențialității informației.

6.4. În vederea prevenirii și combaterii spălării banilor și finanțării terorismului, în cadrul Companiei sunt stabilite politici și metode adecvate în materie de precauție privind clientela, în domeniul păstrării evidențelor, al controlului intern, al evaluării și gestionării riscurilor, în managementul de conformitate și de comunicare pentru a preîntâmpina și a împiedica activitățile și tranzacțiile legate de spălarea banilor sau de finanțare a terorismului.

6.5. Un rol aparte în cadrul sistemului de control îl are sistemul informațional al Companiei. Cerințele funcționale ale sistemului informațional al Companiei în domeniul dat au la bază :

- a) evidența informației detaliate privind identitatea clienților, operațiunile efectuate de Companie;
- b) garantarea unei raportări depline și veridice organelor cu funcții de supraveghere și Conducerii Companiei;
- c) garantarea securității informaționale a Companiei,

6.6. Compania nu se va implica în operațiuni financiare, dacă deține informații, precum că operațiunile au scopul de a ascunde originea ilicită a valorilor care constituie obiectul acestor operațiuni, nu va acorda suport persoanelor fizice și juridice, care participă la activități ilegale. Se consideră că Compania cunoaște despre proveniența banilor sau altor valori, dacă aceasta rezultă din circumstanțe obiective, confirmate prin fapte reale.

6.7. În conformitate cu prevederile art. 22 alin. 1) din Legea cu privire la organizațiile de creditare nebancară Nr. 1 din 16.03.2018, Situațiile financiare individuale ale organizațiilor de creditare nebancară sunt supuse auditului obligatoriu în conformitate cu legislația în vigoare privind auditul situațiilor financiare, (2) În termen de 180 de zile de la finele perioadei de gestiune, organizația de creditare nebancară este obligată să prezinte autorității de supraveghere raportul auditorului și îl publică pe propria pagină web oficială.

De asemenea urmează a fi efectuat și auditul de către personalul instituției financiare nebancare în vederea verificării respectării programului intern privind prevenirea și combaterea spălării banilor și finanțării terorismului. Funcțiile auditului în acest scop sunt:

- a) evaluarea independentă a programului privind prevenirea și combaterea spălării banilor și finanțării terorismului și a respectării cerințelor legislației;
- b) monitorizarea activității personalului prin testarea conformării;
- c) testarea modului de realizare a tranzacțiilor în caz de necesitate;
- d) informarea persoanelor cu funcții de conducere de rang superior, responsabile de asigurarea conformității politicilor și procedurilor, privind rezultatele verificării și recomandarea asupra măsurilor necesare a fi întreprinse pentru minimizarea riscurilor și înlăturarea neajunsurilor identificate.

VII. POLITICI ȘI PROCEDURI PRIVIND CUNOAȘTEREA CLIENȚILOR ȘI A BENEFICIARULUI EFECTIV (REGULILE "CUNOAȘTE-ȚI CLIENTUL")

7.1. Înainte de inițiere a relațiilor contractuale urmează a fi parcursă procedura de acceptare a clientului. Acest proces de cunoaștere a clienților este unul continuu și presupune:

- a) identificarea clientului pe bază de documente oficiale, date sau informații obținute direct de la client sau din surse externe, independente și demne de încredere;
- b) identificarea beneficiarului efectiv și verificarea identității acestuia;
- c) stabilirea calității de persoană expusă politic;
- d) înțelegerea și obținerea de informații privind scopul și natura relației de afaceri precum și sursa fondurilor/sursa averii;
- e) înregistrarea în sistemul informațional al Companiei a datelor de identitate ale clientului atât la inițierea relației de afaceri, cât și în cazul modificării datelor (ori de câte ori este nevoie);
- f) monitorizarea tranzacțiilor realizate pe parcursul relației de afaceri;
- g) păstrarea documentelor specifice de identificare și cunoaștere a clienților conform legislației în vigoare.

7.2. Potrivit cerințelor legislației în vigoare și a recomandărilor organizațiilor internaționale în domeniu, măsurile de identificare a persoanelor fizice sau juridice, precum și a beneficiarului efectiv se întreprind de către Companie:

- a) până la stabilirea relațiilor de afaceri;
- b) la existența unor suspiciuni de spălare a banilor sau de finanțare a terorismului, independent de derogări, scutiri sau limite stabilite;
- c) la existența unor îndoieli privind veridicitatea și precizia datelor de identificare obținute.

7.3. Măsuri aferente cunoașterii adecvate a clienților:

7.3.1. Compania întreprinde măsuri adecvate de cunoaștere a clienților:

- a) la stabilirea relațiilor de afaceri sau la efectuarea tranzacțiilor ocazionale. Identificarea clientului are loc în termeni rezonabili, la prima adresare a acestuia la Companie. Informațiile, datele prezentate de client periodic se actualizează conform cerințelor legislației în vigoare;
- b) întru depistarea persoanelor fizice și/sau juridice față de care sunt impuse restricții, sancțiuni din partea organelor de stat naționale sau internaționale în vederea neadmiterii inițierii relațiilor de afaceri și/sau efectuării tranzacțiilor ocazionale.

7.3.2. În procesul de identificare a clienților, informația prezentată de client poate fi verificată accesând surse externe, independente și demne de încredere cu respectarea cerințelor legislației în vigoare în domeniul protecție datelor cu caracter personal.

7.3.3. Compania nu va stabili relații de afaceri și nu va efectua tranzacții cu persoane fizice sau juridice în cazul în care acestea nu pot fi identificate.

7.3.4. Compania nu va stabili relații de afaceri cu persoanele, grupurile sau entitățile implicate în activități teroriste și de proliferare a armelor de distrugere în masă, incluse în lista menționată la art. 34 alin. (11) din Legea nr. 308/2017 cu privire la prevenirea și combaterea spălării banilor și finanțarea terorismului și anume :

- a) lista Consiliului de Securitate al Organizației Națiunilor Unite cu privire la persoanele, grupurile și entitățile implicate în activități teroriste;
- b) lista Consiliului de Securitate al Organizației Națiunilor Unite cu privire la persoanele, grupurile și entitățile implicate în activități de proliferare a armelor de distrugere în masă;
- c) lista Uniunii Europene cu privire la persoanele, grupurile și entitățile implicate în activități teroriste;

d) lista suplimentară a Serviciului de Informații și Securitate cu privire la persoanele, grupurile și entitățile implicate în activități teroriste.

Despre refuzul de a stabili relații de afaceri cu acestea, neîntârziat va fi informat Serviciul Prevenirea și Combaterea Spălării Banilor, în termen de cel mult 24 ore, prezentând toate datele deținute cu privire la acest caz

7.3.5. În cazul unei relații de afaceri existente, Compania va înceta relația de afaceri dacă se constată faptul că datele și informația obținute la identificarea și verificarea persoanelor fizice și juridice sunt neautentice sau neveridice și va raporta astfel de circumstanțe Serviciului Prevenirea și Combaterea Spălării Banilor.

7.3.6. Activitatea Companiei va fi desfășurată în așa mod, ca în caz de necesitate să poată demonstra autorităților competente, inclusiv organelor de supraveghere, că amplexarea măsurilor de precauție este adecvată, având în vedere riscurile de spălare a banilor și de finanțare a terorismului.

7.3.7. Subiecții supuși identificării sunt:

a) orice persoană fizică sau juridică implicată într-o tranzacție care poate impune un risc semnificativ imaginii sau alt risc;

b) persoanele expuse politic;

c) proprietarii beneficiari ai tranzacțiilor efectuate de către intermediari-profesioniști.

7.3.8. Măsurile de cunoaștere a clienților includ următoarele activități:

a) identificarea și verificarea identității persoanelor fizice, și anume:

- numele și prenumele;

- data și locul nașterii;

- cetățenia și datele documentului de identitate (IDNP, seria și numărul, data eliberării, codul organului care l-a eliberat (dacă există) sau alți indici unici dintr-un act de identitate ce conține fotografia titularului);

- adresa de domiciliu și/sau reședință;

- numărul de telefon, fax, adresa poștei electronice (e-mail, dacă există);

- ocupația, funcția deținută și/sau denumirea angajatorului;

- sursa venitului;

- identitatea beneficiarului efectiv;

- scopul și natura relației de afaceri sau a tranzacției ocazionale (scopul inițierii relației de afaceri sau al efectuării tranzacției ocazionale, tipul produsului și serviciului solicitat, tipul tranzacțiilor, volumul activelor preconizate pentru a fi depuse, volumul și frecvența tranzacțiilor preconizate, potențiala durată a relației de afaceri, etc.);

b) identificarea și verificarea identității pentru persoane juridice și întreprinzătorii individuali:

- denumirea, forma juridică de organizare, actul de constituire și actul privind înregistrarea de stat;

- sediul/adresa de activitate;

- numărul de identificare de stat (IDNO), conform certificatului de înregistrare și/sau extrasului din Registrul de stat eliberat de către organul abilitat cu dreptul de a efectua înregistrarea de stat;

- adresa de corespondență, alta decât sediul (dacă există);

- identitatea persoanei fizice împuternicită de a gestiona contul (reprezentantul), legalitatea împuternicirilor (în cazul lipsei unei astfel de persoane, se indică administratorul persoanei juridice);

- identitatea beneficiarului efectiv a persoanei juridice;

- identitatea persoanelor care dețin poziții de management superior, precum și împuternicirile acestora de reprezentare;

- drepturi și obligațiunile organului de conducere de gestionare a companiei, care reies din documentele primare de înregistrare sau actul de constituire;

- natura și scopul activității, legitimitatea acestora;

- scopul și natura relației de afaceri sau a tranzacției ocazionale (scopul inițierii relației de afaceri sau al efectuării tranzacției ocazionale, tipul produsului și serviciului solicitat, tipul tranzacțiilor, volumul activelor preconizate pentru a fi depuse, volumul și frecvența tranzacțiilor preconizate, potențiala durată a relației de afaceri, etc.);

c) monitorizarea continuă a tranzacției sau a relației de afaceri, pentru a se asigura că acestea sunt conforme profilului activității și profilului riscului, și că documentele, datele sau informațiile deținute sunt actualizate.

7.3.9. Procedurile/măsurile de cunoaștere a clienților se aplică nu doar clienților noi, dar și celor existenți în funcție de risc.

7.3.10. Cerințele detaliate privind identificarea clienților Companiei sunt prevăzute în Procedura de cunoaștere a clientului.

7.4. Măsuri de precauție simplificată privind clienții

Factorii care generează riscuri reduse de spălare a banilor și de finanțare a terorismului și care determină necesitatea aplicării măsurilor de precauție simplificată privind clienții :

- a) sume reduse pentru plăți, depuneri sau retrageri de numerar;
- b) număr de plăți, de depunere sau răscumpărare limitate, inclusiv retragerea numerarului într-o anumită perioadă de timp;
- c) contul poate stoca doar valori limitate de fonduri aferente unui produs sau serviciu;
- d) produsul sau serviciul poate fi folosit doar la nivel național;
- e) produsul sau serviciul este acceptat de un număr limitat de agenți, a căror activitate este cunoscută instituției financiare nebancale;
- f) mijloacele bănești sunt acceptate ca mijloc de plată pentru tipuri limitate de servicii sau produse cu risc scăzut;
- g) clientul este o societate ale cărei valori mobiliare sunt tranzacționate pe o piață reglementată/sistem multilateral de tranzacționare, care impune cerințe pentru a asigura transparența adecvată a beneficiarului efectiv;
- h) clientul are o istorie îndelungată cu instituția financiară nebancale sau cu agenții acestuia (dosarul clientului cuprinde informații cum ar fi subscrierea de credit, măsurile de identificare a clientului actualizate);
- i) produsele și serviciile sunt limitate și bine definite pentru un cerc de clienți, cu scopul de a spori incluziunea financiară.

În cazul în care clienții, prin natura lor, pot prezenta un risc redus de spălare a banilor sau de finanțare a terorismului urmează a fi aplicată măsuri de precauție simplificată, după cum urmează :

- verificarea identității clientului și a beneficiarului efectiv după stabilirea relației de afaceri atunci când aceasta este necesar pentru a nu întrerupe practicile comerciale normale;
- limitarea obținerii de informații specifice sau efectuarea de măsuri specifice privind scopul și natura relației de afaceri și deducerea scopului și naturii relației de afaceri din tipul tranzacțiilor sau a relației de afaceri stabilită;
- reducerea frecvenței actualizărilor datelor de identificare a clienților în cazul unei relații de afaceri stabilite;
- reducerea gradului de monitorizare continuă a tranzacției sau a relației de afaceri.

7.5. Măsuri de precauție sporite privind clienții

Instituția nebancale examinează scopul economic și sensul tuturor tranzacțiilor complexe și neordinare, precum și tipurile de tranzacții neordinare, aparent fără scop legal sau economic. Dacă riscul de spălare a banilor sau de finanțare a terorismului este sporit, urmează a fi aplicate măsuri de precauție sporită privind clienții proporțional riscului identificat, cu mărirea gradului de monitorizare a relației de afaceri pentru a determina dacă activitatea sau tranzacția este neordinară sau suspectă.

7.5.1. Factorii care generează riscuri reduse de spălare a banilor și de finanțare a terorismului și care determină necesitatea aplicării măsurilor de precauție simplificată privind clienții :

- a) clientul este o persoană juridică a cărei structură face dificilă identificarea beneficiarului efectiv sau a celor care dețin controlul acesteia;

b) clientul este reticent în a furniza informații despre beneficiar, informații cu privire la achiziționarea unui produs sau oferă informații incomplete, neveridice sau contradictorii;

c) clientul care nu se prezintă personal la identificare cu excepția clientului identificat prin aplicarea mijloacelor electronice;

d) relațiile de afaceri sau tranzacțiile la distanță, fără anumite măsuri de protecție, cum ar fi semnătura electronică;

e) persoanele juridice cu rol de structuri de administrare a bunurilor personale;

f) clientul efectuează întotdeauna tranzacții sub limita stabilită de raportare;

g) sursa averii și/sau sursa fondurilor clientului destinate pentru acordarea împrumutului/creditului sau depunerilor de economii nu este clară;

h) tranzacțiile efectuate/primate de la terți necunoscuți clientului sau neasociați acestuia;

i) operațiunea nu este însoțită de informațiile necesare despre plătitor sau beneficiar;

j) clientul rambursează împrumutul/creditul anticipat înainte de scadența obligației contractuale, dar nu poate prezenta o justificare a sursei fondurilor;

k) clientul sau un terț garantează împrumutul/creditul cu bunuri de valoare înaltă sau alte active, fără a avea un sens economic, având posibilitatea utilizării acestor bunuri sau active direct (fără a contracta un împrumut/credit);

l) nerambursarea aparent neîntemeiată a împrumutului/creditului garantat, cu scopul de a determina declanșarea procedurii de exercitare a dreptului de gaj/ipotecă;

m) clientul solicită o perioadă de rambursare a împrumutului/creditului foarte scurtă, contrar capacității financiare a acestuia, fără careva explicații plauzibile și documente care confirmă sursa mijloacelor bănești;

n) activul/bunul a fost procurat în numerar și imediat a fost gajat;

o) împrumuturile ipotecare sunt achitate integral înainte de prima rată de scadență, contrar capacității financiare a acestuia, fără careva explicații plauzibile și documente care confirmă sursa mijloacelor bănești;

p) activul/bunul gajat se află într-o jurisdicție cu risc sporit;

q) clientul solicită schimbarea metodei obișnuite de rambursare a împrumutului/creditului, fără careva argumente clare și întemeiate;

r) plățile primite de la terți necunoscuți sau neasociați;

s) bunul procurat în leasing este folosit de către o terță persoană în lipsa unor raporturi juridice determinate cu locatarul;

t) clienții și instituțiile financiare care își au reședința în țările (jurisdicțiile) cu risc sporit desemnate/monitorizate de GAFI;

u) persoanele juridice cu rol de structuri de administrare a bunurilor personale;

v) societățile care au acționari mandatați sau ale căror acțiuni sînt în custodie;

w) produsele sau tranzacțiile care ar putea favoriza anonimatul;

x) alți factori identificați în cadrul evaluării riscurilor.

7.5.2. Instituția aplică măsuri de precauție sporită privind clienții, suplimentar celor prevăzute mai sus în situațiile care, prin natura lor, pot prezenta un risc sporit de spălare a banilor sau de finanțare a terorismului, cel puțin în modul stabilit de Lege inclusiv prin:

a) obținerea informației suplimentare despre client și beneficiarul efectiv (genul de activitate, volumul activelor, cifra de afacere, altă informație disponibilă în surse publice, internet), precum și actualizarea frecventă a datelor de identificare ale clientului și beneficiarului efectiv;

b) obținerea informației suplimentare despre natura și scopul relației de afaceri;

c) obținerea informației despre sursa bunurilor clientului, ale beneficiarului efectiv și a averii deținute de către client;

d) obținerea informației despre scopul activității sau tranzacției în curs de pregătire, de realizare sau deja realizate;

e) obținerea aprobării de către persoana cu funcții de conducere de rang superior a inițierii sau continuării relației de afaceri;

f) realizarea monitorizării sporite a relației de afaceri prin creșterea numărului și a frecvenței verificărilor efectuate și prin selectarea activităților și tranzacțiilor care necesită o examinare adițională;

g) solicitarea ca prima plată a operațiunilor să se efectueze printr-un cont deschis în numele clientului la o bancă care aplică măsuri similare de precauție privind clienții.

7.5.3. Compania aplică măsuri de precauție sporită în funcție de riscul asociat tipului de client, relației de afaceri, bunului sau tranzacției în situații care prin natura lor pot prezenta un risc mai mare de spălare de bani sau finanțare a terorismului.

7.5.4. În cazul în care persoana fizică sau juridică nu este prezentă personal la identificare, Compania va întreprinde măsuri de precauție sporită de:

a) garantare că identitatea persoanei este stabilită prin documente, date sau informații suplimentare;

b) verificare și certificare suplimentară a documentelor furnizate sau confirmarea lor de către o instituție financiară;

c) garantare că prima plată a operațiunilor se efectuează printr-un cont deschis în numele persoanei la o instituție financiară.

7.5.5. În cazul tranzacțiilor sau relațiilor de afaceri cu persoane expuse politic, Compania va asigura întreprinderea măsurilor de precauție sporită prin:

a) realizarea măsurilor în funcție de risc pentru a stabili dacă persoana este expusă politic : identificarea persoanei fizice sau conducerii și beneficiarului efectiv al persoanei juridice (completarea cîmpului corespunzător din Chestionarul pentru identificarea clientului), verificarea informației disponibile public pentru a determina dacă este sau nu o persoană expusă politic;

b) obținerea aprobării Conducerii Companiei pentru stabilirea sau continuarea unor relații de afaceri cu astfel de persoane;

c) adoptarea de măsuri adecvate pentru a stabili sursa bunurilor implicate în relația de afaceri sau în tranzacție;

d) efectuarea de monitorizări sporite și permanente a relației de afaceri.

7.6. Monitorizarea continuă a tranzacțiilor

Procedurile privind monitorizarea continuă a tranzacțiilor includ:

a) determinarea operațiunilor ordinare (specifice) ale clientului;

b) monitorizarea operațiunilor clientului pentru a determina dacă acestea corespund operațiunilor ordinare (specifice) pentru acest client sau pentru clienții din cadrul categoriilor similare;

c) identificarea operațiunilor limitate sau suspecte, inclusiv cele potențiale, precum și a surselor mijloacelor folosite de client în aceste operațiuni;

d) prezentarea persoanelor responsabile a informației necesare pentru identificarea, analiza și monitorizarea eficientă a clienților și/sau a tranzacțiilor cu grad de risc sporit;

e) aprobarea tranzacțiilor semnificative ale clienților cu grad de risc sporit de către Conducerea Companiei;

f) atenționarea asupra operațiunilor de afaceri ale persoanelor expuse politic și indivizilor cu profil suspect sau cu persoanele și societățile (companiile) care în mod clar sunt în relație sau asociați cu aceștia.

7.7. Deținerea, actualizarea și păstrarea informației

7.7.1. În cadrul Companiei evidența informației și a documentelor clienților identificați este înregistrată în sistemul informațional al Companiei. Informația din sistemul informațional periodic este arhivată.

7.7.2. Documentele primare prezentate de către client la momentul stabilirii relației de afaceri, inclusiv a corespondenței se păstrează, în decurs de cel puțin 5 ani după finalizarea relației de afaceri.

7.7.3. La solicitarea parvenită din partea organelor cu funcții de supraveghere, termenul de menținere a evidenței poate fi extins pe perioada solicitată.

7.7.4. Compania asigură accesul organelor abilitate (Serviciul Prevenirea Combaterea Spălării Banilor și altor autorități de supraveghere), la documentele și informațiile disponibile privind relațiile de afaceri dintre Companie și clienți, precum și natura acestor relații, la cererea acestora.

VIII. RAPORTAREA ACTIVITĂȚILOR SAU TRANZACȚIILOR CARE CAD SUB INCIDENȚA LEGII

8.1. În cadrul Companiei, prin ordinul Directorului, sunt desemnate persoanele investite cu atribuții de executare a Legii, ale căror nume sunt comunicate Serviciului Prevenirea și Combaterea Spălării Banilor și altor organe de supraveghere, împreună cu natura și limitele responsabilităților.

8.2. Persoanele desemnate sunt responsabile de sistematizarea informației, completarea și prezentarea Serviciului Prevenirea și Combaterea Spălării Banilor a datelor sunt obligate să raporteze Serviciului Prevenirea și Combaterea Spălării Banilor, în conformitate cu art. 11 din Legea nr. 308/2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului și a Regulamentului cu privire la cerințele privind prevenirea și combaterea spălării banilor și finanțării terorismului în activitatea instituțiilor financiare nebankare aprobat prin Hotărârea Comitetului Executiv al BNM nr. 280 din 07.11.2024, informații despre:

a) bunurile suspecte, activitățile sau tranzacțiile suspecte de spălare a banilor, de infracțiuni predicat și de finanțare a terorismului, care sunt în curs de pregătire, de tentativă, de realizare sau sunt deja realizate - imediat, în cel mult 24 de ore de la identificarea actului sau circumstanțelor care generează suspiciuni;

b) activitățile sau tranzacțiile clienților în numerar în valoare de cel puțin 200 000 de lei, realizate printr-o operațiune sau prin mai multe operațiuni care au o legătură între ele, efectuate în decursul unei luni, începând cu prima zi și terminând cu ultima zi a lunii - până la data de 5 a lunii următoare lunii în care au fost efectuate activitățile sau tranzacțiile;

c) tranzacțiile clienților realizate printr-o operațiune a cărei valoare este de cel puțin 200 000 de lei și care nu se încadrează în prevederile subpt. b) - până la data de 10 a lunii următoare lunii în care au fost efectuate tranzacțiile.

8.3. Formularul special prezentat Serviciului este completat în conformitate cu cerințele *Metodologiei cu privire la modul de completare și transmitere a formularelor speciale privind activitățile sau tranzacțiile care cad sub incidența Legii nr. 308/2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului aprobate prin Ordinul Serviciul Prevenirea și Combaterea Spălării Banilor nr. 20/2023 din 03.08.2023*, este confirmat prin semnătura persoanei care l-a completat.

IX. PROCEDURI DE DETECTARE A TRANZACȚIILOR SUSPECTE

9.1. La stabilirea caracterului suspect al tranzacțiilor clienților, angajații se călăuzesc atât de informațiile parvenite din exterior de la organele de supraveghere, cât și de bănuielile asupra tranzacțiilor clienților de spălare a banilor sau de finanțare a terorismului, bazate, de regulă, pe modul neobișnuit în care acestea se produc, activitățile obișnuite ale clientului, sursa mijloacelor bănești utilizate și părțile implicate.

9.2. Informațiile specifice domeniului prevenirii combaterii spălării banilor și finanțării terorismului cuprind:

9.2.1. Listele persoanelor, grupurilor entităților implicate în activități teroriste, conform informației Serviciului de Informații și Securitate al RM (**Ordinul Nr. 2 din 15-01-2016 privind listele persoanelor, grupurilor și entităților implicate în activități teroriste**);

9.2.2. Țările de interes specific, conform Ordinului nr. 118 din 20.11.2007 al directorului CCCEC, și anume:

a) țările în care poate avea loc fabricarea ilegală a substanțelor narcotice,

b) țările care prezintă un risc sporit datorită nivelului înalt de infracționalitate de corupție,

- c) țările și/sau zonele off-shore;
- d) țările care nu dispun de norme contra spălării banilor și finanțării terorismului sau dispun de norme inadecvate în acest sens;

9.2.3. Informația care permite identificarea persoanelor expuse politic, membrii familiilor și asociații apropiați ai acestora, conform **Ghidului privind identificarea și monitorizarea persoanelor expuse politic și indicilor de risc privind persoanele expuse politic (PEP)** aprobat prin **Ordinul Serviciul Prevenirea și Combaterea Spălării Banilor nr. 23 din 06.09.2023**.

9.2.4. Informația parvenită de la organele de supraveghere și organizațiile internaționale în domeniu.

9.3. La depistarea tranzacțiilor suspecte ale clienților și identificarea persoanelor și entităților implicate în activități teroriste, angajații iau în considerare recomandările expuse în **Ghidului privind identificare tranzacțiilor și activităților suspecte de finanțare a terorismului aprobat prin Ordinul Serviciul Prevenirea și Combaterea Spălării Banilor nr. 23 din 06.09.2023**.

9.4. Tranzacțiile suspecte pot fi depistate prin intermediul:

- a) efectuării permanente a unei monitorizări a operațiunilor, în scopul stabilirii conformării lor cu operațiunile ordinare ale clientului;
- b) analizei contactelor clienților (întâlnirea și conversarea cu clienții etc.);
- c) analizei informației din surse independente (televiziune, radio, presă etc.);
- d) analizei informației deținute de către Companie despre client.

9.5. Categoriile de suspiciune în activitatea de creditare:

9.5.1. Comportamentul suspect al clientului la identificare:

- a) clientul oferă date de identificare neconforme, are rețineri în a oferi datele personale sau chiar refuză să le ofere;
- b) clientul are o atitudine defensivă în momentul în care se aplică procedura de identificare sau se pune în discuție proveniența banilor;
- c) clienții puțin versați pot fi tensionați, refuză să răspundă sau se încurcă în explicații sau, din contra, devin agresivi;

9.5.2. Activități (operațiuni, tranzacții) suspecte efectuate de client:

- a) rambursarea împrumuturilor neașteptat de repede cu fonduri din surse necunoscute;
- b) schimbarea destinației împrumutului;
- c) rambursarea împrumutului acordat unei societăți de o altă societate (cu atât mai mult dacă este o societate off-shore);
- d) solicitări de acordare de împrumuturi companiilor off-shore;
- e) cereri de solicitare a împrumutului ale clienților noi, depuse prin intermediarii de profesie (avocați, consultanți financiari, companii de intermediere).

9.6. La stabilirea caracterului suspect al unei tranzacții, angajații Companiei acordă o atenție sporită tranzacțiilor complexe, tranzacțiilor semnificative și tranzacțiilor neordinare fără un scop economic clar, solicitând clientului, după caz, precizarea conținutului tranzacției și/sau prezentarea documentelor justificative (contracte, declarații vamale, facturi, etc.), suficiente pentru a înțelege sensul economic al tranzacției și sursa mijloacelor bănești utilizate la efectuarea tranzacției.

9.7. În cazul apariției unor presupuneri, precum că un client sau beneficiarul efectiv al clientului este o persoană sau entitate implicată în activități teroriste, angajații informează despre aceasta Conducerea Companiei, care analizează cazul și emite dispoziția de sistare pe 2 (două) zile lucrătoare a acțiunilor referitoare la operațiunea persoanei suspecte de implicare în activități teroriste, cu excepția operațiunilor de încasare a mijloacelor cu informarea imediată a Serviciului Prevenirea și Combaterea Spălării Banilor. Dacă în termenul de 2 zile menționat nu primesc decizia

Serviciului Prevenirea și Combaterea Spălării Banilor de sistare a tranzacției, Compania execută tranzacția.

9.8. Dacă specificul tranzacției nu poate fi clarificat la moment, iar pentru a efectua o analiză este nevoie de o perioadă de timp nedeterminată, angajații Companiei califică tranzacția ca suspectă și o raportează în termen de 24 de ore.

9.9. Raportarea tuturor tranzacțiilor care cad sub incidența Legii are loc în conformitate cu cerințele legislației în vigoare.

X. SELECTAREA ȘI INSTRUIREA ANGAJAȚILOR

10.1. Selectarea angajaților

10.1.1. La angajarea personalului, Compania va efectua:

- a) examinarea angajaților prin intermediul testărilor profesionale specifice;
- b) angajarea, pe bază de verificări, a persoanelor cu referințe de calitate, cu înaltă ținută morală și care au o reputație bună;
- c) asigurarea încadrării stricte în limitele sarcinilor atribuțiilor cuprinse în virtutea postului.

10.2. Instruirea personalului

10.2.1. Instruirea personalului se efectuează în dependență de nivelul implicării acestuia în procesul de prevenire și combatere a spălării banilor și finanțării terorismului. Instruirea personalului (periodicitatea, forma de instruire) se efectuează în conformitate cu Planul de acțiuni al Companiei. Cerințele de instruire include:

- a) instruirea personalului nou angajat referitor la importanța Programului și cerințelor de bază în cadrul Companiei;
- b) instruirea personalului de prima - linie referitor la verificarea identității clienților noi, monitorizarea conturilor clienților deja existenți în bază continuă și detectarea indicilor de activitate suspectă;
- c) instruire periodice de actualizare a responsabilității personalului, inclusiv informarea privind noile dezvoltări de domeniu, modificări în legislație.

10.2.2. În cadrul activității de instruire continuă a personalului, se va pune accentul pe capacitatea acestuia de a sesiza acele elemente și indici în baza cărora poate ori nu conveni dacă o operațiune este sau nu suspect.

XI. RĂSPUNDEREA

11.1. Până la expirarea termenelor prevăzute de Lege cu privire la raportare, entitatea raportoare, angajații, persoanele cu funcții de răspundere și reprezentanții acestora sînt obligați să nu divulge clienților ori terților datele despre transmiterea informațiilor, în temeiul Legii, Serviciului și organelor cu funcții de supraveghere a entităților raportoare sau datele despre analizele și investigațiile financiare efectuate privind acțiunile de spălare a banilor, infracțiunile predicat sau acțiunile de finanțare a terorismului care au loc sau care pot avea loc.

11.2. Entitatea raportoare, conform instrucțiunilor aprobate de către organele cu funcții de supraveghere, asigură protecția angajaților și altor persoane fizice care nu sînt angajate în cadrul entității raportoare, dar care participă la gestiunea și activitatea acesteia, de orice amenințare sau acțiune ostilă în legătură cu furnizarea informației în temeiul prezentei legi.

11.3. Divulgarea informațiilor cu bună-credință, în scopul aplicării prezentei legi de către entitățile raportoare sau de angajații, persoanele cu funcții de răspundere și reprezentanții acestora, nu constituie încălcare a restricțiilor de divulgare a informațiilor, impuse prin contract sau printr-un act legislativ, sau printr-un act administrativ, și nu atrage răspundere chiar și în cazul neconfirmării suspiciunii activității sau tranzacției.

11.4. Furnizarea informației către organul de control al prelucrărilor de date cu caracter personal, solicitată conform competenței, nu se consideră a fi divulgare/dezvăluire.

11.5. Angajații Companiei, care vor admite încălcări ale legislației în domeniu și prevederilor prezentului Program, vor fi atrași la răspundere disciplinară, contravențională, civilă sau penală, după caz, conform măsurilor prevăzute în Codul Penal și Codul Contravențional al RM.

11.6. Angajații care în mod intenționat nu raportează despre tranzacțiile suspecte și/sau contribuie personal la derularea operațiunilor de spălare a banilor și finanțare a terorismului vor fi atrași la răspundere conform legislației în vigoare a RM.

11.7. Compania va asigura protecția angajaților contra oricărei amenințări sau acțiuni ostile în legătură cu raportarea tranzacțiilor suspecte.

11.8. Compania și angajații ei sunt exonerati:

a) de răspundere disciplinară, administrativă, civilă, penală ca urmare a executării prevederilor Legii, chiar dacă această executare a avut drept urmări cauzarea de prejudicii materiale sau morale clienților Companiei;

b) de răspundere pentru divulgarea secretului comercial în cazul acordării informației organelor de cercetare penală, organelor judiciare sau altor organe în ordinea stabilită de legislația cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului la solicitarea acestora.

XII. DISPOZITII FINALE

12.1. Prezentul Program intră în vigoare din momentul aprobării,

12.2. Prezentul Program poate fi modificat și completat în modul stabilit în baza schimbărilor parvenite în legislația în vigoare a Republicii Moldova și în actele normative interne ale Companiei,

12.3. Prezentul Program este obligatoriu în aplicare și executare pentru toți angajații Companiei.

12.4. Controlul corectitudinii și complexității realizării prevederilor prezentului Program se asigură de către Conducerea Companiei.

Administratorul
O.C.N. "BEST-INVEST" SRL
ROGOVOI ALEXANDR

