

**COMITETUL EXECUTIV
AL BĂNCII NAȚIONALE A MOLDOVEI**

**HOTARÎREA nr.....
din2018**

cu privire la modificarea unor acte normative ale Băncii Naționale a Moldovei în contextul legislației cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului

În temeiul art. 11 alin.(1), art.27 alin.(1) lit.c) și 44 lit.a) și d) din Legea nr.548-XIII din 21 iulie 1995 cu privire la Banca Națională a Moldovei (Monitorul Oficial al Republicii Moldova, 1995, nr.56-57, art.624), cu modificările și completările ulterioare), art. 95 și 99 alin.(1) din Legea privind activitatea băncilor nr.202 din 06 octombrie 2017 (Monitorul Oficial al Republicii Moldova, 2017 nr.434-439, art.727) și art.15 alin.(2) din Legea nr. 308 din 22.12.2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului (Monitorul Oficial al Republicii Moldova, 2018, nr. 58-66, art.133), art.13 alin.(1) din Legea privind aplicarea măsurilor restrictive internaționale (Monitorul Oficial al Republicii Moldova, 2016, nr. 140-149, art.289) și art.5 alin.(2) din Legea nr.114 privind serviciile de plată și moneda electronică (Monitorul Oficial al Republicii Moldova,2012, nr. 193-197, art.661), Comitetul executiv al Băncii Naționale a Moldovei

HOTĂRĂȘTE:

1. Se aprobă Regulamentul privind activitatea băncilor în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului (se anexează).
2. La data intrării în vigoare a prezentului regulament, se modifică: Textul „de 2500 lei” prevăzut la pct.2 noțiunea de „card de plată” lit.b) „card preplătit” din Regulamentul cu privire la cardurile de plată aprobat prin HCA al BNM nr. 157 din 01.08.2013 (Monitorul Oficial al Republicii Moldova, 2013, nr.191-197 art.1370), cu textul „stabilită în actele normative în vigoare privind prevenirea și combaterea spălării banilor și finanțării terorismului”;
3. La data intrării în vigoare a prezentului regulament, se abrogă:
 - a) Regulamentul privind activitatea băncilor în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului, aprobat prin HCA al BNM nr. 172 din 04.08.2011 (Monitorul Oficial al Republicii Moldova, 2011, nr.170-175 art.1554);
 - b) capitolul V „Prevenirea și combaterea spălării banilor și finanțării terorismului prin sistemele de remitere de bani” din Regulamentul cu privire la activitatea prestatorilor de servicii de plată în sistemele de remitere de bani, aprobat prin HCA al BNM nr. 204 din 15.10.2010 (Monitorul Oficial al Republicii Moldova, 2010, nr.231-234 art.900), cu modificările și completările ulterioare;
 - c) pct.24, 24¹ și 36¹, precum și capitolul VII „Cerințe privind organizarea cadrului aferent prevenirii și combaterii spălării banilor și finanțării terorismului în contextul realizării transferului de credit” din Regulamentul cu privire la transferul de credit,

aprobat prin HCA al BNM nr. 157 din 01.08.2013 (Monitorul Oficial al Republicii Moldova, 2013, nr.191-197 art.1370);

- d) pct. 11-17 din Regulamentul cu privire la cardurile de plată, aprobat prin HCA al BNM nr. 157 din 01.08.2013 (Monitorul Oficial al Republicii Moldova, 2013, nr.191-197 art.1370);
- 4. Prezenta hotărâre intră în vigoare la data publicării în Monitorul Oficial al Republicii Moldova.

**Președinte al
Comitetului executiv**

Sergiu CIOCLEA

REGULAMENT
privind activitatea băncilor în domeniul
prevenirii și combaterii spălării banilor și finanțării terorismului

Capitolul I
DISPOZIȚII GENERALE

1. Regulamentul privind activitatea băncilor în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului (în continuare – Regulament) este emis în vederea executării prevederilor Legii nr.308 din 22.12.2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului și a cerințelor standardelor internaționale în domeniu. Regulamentul stabilește cerințele privind: identificarea și evaluarea riscurilor de spălarea banilor și finanțarea terorismului; aplicarea cerințelor de precauție privind clienții, inclusiv a măsurilor de precauție simplificată și sporită; păstrarea datelor; raportarea activităților și tranzacțiilor suspecte; implementarea sancțiunilor financiare aferente activităților teroriste și de proliferare a armelor de distrugere în masă; organizarea și realizarea elementelor aferente sistemului de control intern, precum și alte cerințe în vederea minimizării riscurilor aferente spălării banilor și finanțării terorismului.

2. Banca și sucursalele băncilor din alte state aplică cerințele prezentului Regulament în relațiile de afaceri cu clienții săi și la efectuarea tranzacțiilor și operațiunilor bancare.

3. Termenii și expresiile utilizate în prezentul Regulament au semnificațiile prevăzute în Legea nr.202 din 06.10.2017 privind activitatea băncilor, Legea nr.548-XIII din 21.07.1995 cu privire la Banca Națională Moldovei, Legea nr.308 din 22.12.2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului, Legea nr.114 din 18.05.2012 cu privire la serviciile de plată și moneda electronică, Legea nr.25 din 04.03.2016 privind aplicarea măsurilor restrictive internaționale, actele normative ale Băncii Naționale a Moldovei și ale Serviciului Prevenirea și Combaterea Spălării Banilor emise întru executarea acestora. De asemenea, în sensul prezentului Regulament se utilizează următorii termeni și expresii:

program intern – politici, proceduri și alte reguli și practici aprobate în scopul implementării cerințelor privind prevenirea și combaterea spălării banilor și finanțării terorismului;

tranzacție semnificativă – tranzacția (operațiunea) care depășește limita valorică stabilită în politicile interne ale băncii luând în considerație riscurile asociate clienților și tranzacțiilor efectuate;

mijloace electronice – calculator (computer), bancomat (Automated Teller Machine), terminale de plată în numerar (terminal cash-in), telefon mobil sau oricare alt dispozitiv sau sistem de procesare a datelor electronic în mod automatizat;

transferuri de fonduri - reprezintă orice tranzacție efectuată, cel puțin parțial, prin mijloace electronice în numele unui plătitor prin intermediul unui prestator de servicii de plată, pentru a se pune fonduri la dispoziția beneficiarului plății prin intermediul unui prestator de servicii de plată, indiferent dacă plătitorul și beneficiarul plății sunt sau nu aceeași persoană și indiferent dacă prestatorul de servicii de plată al plătitorului și prestatorul de servicii de plată al beneficiarului plății sunt identici, inclusiv: transferuri de credit, debitări directe, remiteri de bani și transferuri efectuate utilizând cardul de plată;

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;

transfer de fonduri pe baza unui fișier de grup (batch file) - reprezintă mai multe transferuri ordonate de un singur plătitor către mai mulți beneficiari, care sînt grupate în vederea transmiterii.;

conturi corespondente de transfer (payable - through accounts) - serviciu bancar, care permite clienților băncii corespondente străine utilizarea directă a conturilor corespondente deschise cu scopul efectuării tranzacțiilor directe în numele acestora;

servicii bancare private (private banking) – activitatea de consiliere financiară personalizată și confidențială de administrare a mijloacelor bănești (portofoliului personalizat negociat) a clienților cu venituri mari sau care dețin active lichide însemnate.

organizațiile internaționale – Organizația Națiunilor Unite, Consiliul Europei, Uniunea Europeană, Grupul de Acțiune Financiar Internațional (GAFI-FATF), Forumul Global privind Transparența și Schimbul de Informații în materii fiscale, alte organizații recunoscute de comunitatea internațională.

Capitolul II RESPONSABILITĂȚI

4. Banca elaborează și pune în aplicare un program intern eficient privind prevenirea și combaterea spălării banilor și finanțării terorismului.

5. Banca dispune de un sistem de control intern adecvat pentru a identifica, evalua, monitoriza și înțelege riscurile de spălarea banilor și finanțarea terorismului. Banca întreprinde măsurile necesare, implicând resurse suficiente, pentru a minimiza riscurile identificate.

6. Consiliul băncii este responsabil pentru elaborarea, aprobarea și asigurarea aplicării programelor privind prevenirea și combaterea spălării banilor și finanțării terorismului. Organul executiv al băncii este responsabil de implementarea eficientă a cerințelor de prevenire și combatere a spălării banilor și finanțării terorismului.

7. Banca desemnează un membru al organului executiv al băncii pentru exercitarea funcției de persoană responsabilă de asigurarea conformării activității băncii cu cerințele legale privind prevenirea și combaterea spălării banilor și finanțării terorismului.

8. Subdiviziunea de audit intern sau alte subdiviziuni cu funcții de control efectuează evaluarea independentă, cel puțin trimestrial, a caracterului adecvat și a conformității activității băncii cu programele privind prevenirea și combaterea spălării banilor și finanțării terorismului. Rezultatele evaluării se comunică consiliului băncii, comisiei de cenzori, organului executiv al băncii, precum și Băncii Naționale a Moldovei în conformitate cu Instrucțiunea cu privire la modul de întocmire și prezentare de către bănci a rapoartelor în scopuri prudentiale, aprobat prin Hotărârea Consiliului de administrație al Băncii Naționale a Moldovei nr.279 din 01 decembrie 2011 (Monitorul Oficial al Republicii Moldova, 2011, nr.216-221, art.2008, cu modificări și completări ulterioare).

Capitolul III CERINȚE FAȚĂ DE PROGRAMUL INTERN PRIVIND PREVENIREA ȘI COMBATERICA SPĂLĂRII BANILOR ȘI FINANȚĂRII TERORISMULUI

9. Programul intern privind prevenirea și combaterea spălării banilor și finanțării terorismului reprezintă politici, proceduri și alte reguli și practici, inclusiv reguli de cunoaștere a clientului, care promovează normele de etică și profesionalism în sectorul bancar și care previn utilizarea băncii în scopul spălării banilor sau finanțării terorismului, în mod intenționat sau nu, de către elementele criminale. Aceste programe trebuie să asigure efectuarea operațiunilor bancare într-un mod sigur și prudent.

10. Banca elaborează programul intern privind prevenirea și combaterea spălării banilor și finanțării terorismului în conformitate cu prevederile Legii nr.308 din 22.12.2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului, Legii nr.202 din 06.10.2017 privind activitatea băncilor, prezentului Regulament, altor acte normative ale Băncii Naționale a Moldovei și ale Serviciului Prevenirea și Combaterea Spălării Banilor, precum și ale altor organe cu funcții de supraveghere, ținând cont de practica general acceptată în acest domeniu, inclusiv documentele Comitetului Basel și ale Grupului de Acțiune Financiară Internațională (FATF).

11. La elaborarea programului intern se iau în considerație mărimea, complexitatea, natura și volumul activităților băncii, riscurile de spălarea banilor și finanțarea terorismului identificate, tipurile (categoriile) clienților, produsele și serviciile oferite, zona geografică implicată, gradul (nivelul) de risc asociat clienților și/sau tranzacțiilor (operațiunilor) desfășurate de aceștia.

12. Programul intern privind prevenirea și combaterea spălării banilor și finanțării terorismului va prevedea, fără a se limita la următoarele:

1) obligațiile consiliului și executivului băncii, care trebuie să includă cel puțin:

a) determinarea domeniilor de activitate ale băncii vulnerabile riscului spălării banilor și finanțării terorismului, cu delimitarea exactă a atribuțiilor fiecărei subdiviziuni pentru prevenirea și combaterea spălării banilor și finanțării terorismului. Domeniile de activitate vulnerabile riscului spălării banilor și finanțării terorismului pot fi acelea care au tangență cu: acceptarea depozitelor, operațiunile de acordare/rambursare a creditelor, plățile (transferurile) internaționale, utilizarea instrumentelor de plată, operațiunile bancare corespondente, serviciile bancare private, conturile deschise de intermediarii profesioniști în procesul exercitării de către aceștia a activităților de intermediere, sisteme automatizate de deservire la distanță, sistemele de remitere de bani, operațiuni alternative de finanțare a comerțului (acreditive, emiteri de obligațiuni, etc), operațiunile de brokeraj, de administrare fiduciară etc.;

b) determinarea mecanismului de identificare, evaluare și întreprindere a acțiunilor de control și minimizare a riscurilor de spălarea banilor și finanțarea terorismului;

c) elaborarea măsurilor necesare pentru implementarea politicilor și procedurilor de cunoaștere a clienților, inclusiv a celor cu grad de risc sporit;

d) alocarea resurselor suficiente pentru îndeplinirea eficientă a activităților de prevenire și combatere a spălării banilor și finanțării terorismului;

e) desemnarea persoanelor investite cu atribuții de executare a Legii nr. 308 din 22.12.2017 cu privire la prevenirea și combaterea spălării banilor și finanțarea terorismului;

f) determinarea responsabilităților personalului băncii la diferite nivele ierarhice;

g) acordarea persoanelor responsabile a accesului într-un timp rezonabil la informația necesară executării Legii nr. 308 din 22.12.2017 cu privire la prevenirea și combaterea spălării banilor și finanțarea terorismului și prezentului regulament;

h) remedierea deficiențelor identificate în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului;

2) proceduri de identificare, evaluare, control și întreprinderea măsurilor de minimizare a riscurilor de spălarea banilor și finanțarea terorismului;

3) proceduri de acceptare a clienților care stabilesc cel puțin categoriile de clienți pe care banca își propune să-i atragă și nivelul ierarhic al personalului care aprobă începerea relației de afaceri cu aceștia, în funcție de gradul de risc asociat, tipurile de produse și servicii care le sunt furnizate;

4) măsuri de identificare, verificare și monitorizare a clienților și beneficiarilor efectivi în funcție de gradul de risc asociat (regulile de cunoaștere a clientului), criteriile și modul de trecere a clienților dintr-o categorie cu un grad de risc în alta;

5) măsurile de precauție privind cunoașterea clienților pentru fiecare dintre categoriile de clienți, produse și servicii ori tranzacții (operațiuni) efectuate;

6) proceduri de monitorizare a operațiunilor efectuate de clienți în scopul depistării tranzacțiilor semnificative, complexe și neordinare, a activităților și tranzacțiilor suspecte;

7) proceduri și cerințe privind aplicarea măsurilor de precauție simplificate pentru clienții și tranzacțiile acestora atunci când, prin natura lor, pot prezenta un risc redus de spălarea banilor și finanțarea terorismului;

8) proceduri și cerințe privind aplicarea măsurilor de precauție sporite la efectuarea tranzacțiilor complexe și neordinare fără un scop legal sau economic clar, a tranzacțiilor semnificative și a celor suspecte;

9) modul de întocmire și păstrare a informațiilor, precum și de stabilire a accesului la acestea;

10) proceduri de raportare internă și către autoritățile competente privind activitățile și tranzacțiile suspecte;

11) proceduri și măsuri de verificare a modului de conformare la normele elaborate și de evaluare a eficienței acestora;

12) standarde pentru selectare, angajare a personalului și programe de instruire a acestuia în domeniul cunoașterii clienților;

13) proceduri privind identificarea și analiza riscurilor de spălare a banilor și finanțare a terorismului, inclusiv măsurile de minimizare a acestora, legate de utilizarea tehnologiilor informaționale, inclusiv cele noi, procurate sau elaborate în cadrul produselor și serviciilor oferite de bancă.

13. Banca revizuieste (actualizează), ori de câte ori este necesar, programul intern privind prevenirea și combaterea spălării banilor și finanțării terorismului, dar cel puțin anual, ținând cont de prevederile legislației în vigoare.

Capitolul IV

EVALUAREA RISCURILOR DE SPĂLAREA BANILOR ȘI FINANȚAREA TERORISMULUI. ABORDAREA BAZATĂ PE RISC

14. Banca identifică și evaluează riscurile de spălarea banilor și finanțarea terorismului, ținând cont de amenințările și vulnerabilitățile identificate în rapoartele de evaluare la nivelul național, regional și sectorial, precum și de criteriile și factorii de risc stabiliți în acest sens. Rezultatele evaluării se aprobă de către persoana responsabilă pe bancă de asigurarea politicilor și procedurilor cu cerințele legale privind prevenirea și combaterea spălării banilor și finanțării terorismului și se prezintă consiliului băncii.

15. Banca efectuează și actualizează, cel puțin o dată la 2 ani, evaluarea riscurilor de spălarea banilor și finanțarea terorismului, proces care presupune cel puțin:

a) elaborarea unui raport scris prin care se determină țările sau zone geografice, produsele, clienții și tranzacțiile (operațiunile) cu grad de risc sporit, ponderea și impactul acestora asupra activității băncii;

b) întocmirea unui plan de acțiuni în scopul minimizării riscurilor de spălarea banilor și finanțarea terorismului identificate;

16. Banca identifică și evaluează riscurile de spălarea a banilor și finanțarea a terorismului până la:

a) lansarea și dezvoltarea de produse și servicii noi;

b) utilizarea tehnologiilor noi sau aflate în dezvoltare, atât pentru produsele și serviciile noi, cât și pentru cele existente.

17. În procesul de evaluare a riscurilor de spălarea a banilor și finanțarea a terorismului, banca utilizează diferite elemente și caracteristici ale variabilelor implicate în analiză, cum sunt: destinația contului, scopul relației de afaceri, volumul activelor implicate sau mărimea tranzacțiilor efectuate, frecvența și durata relației de afaceri, etc.

18. Banca, ca urmare a rezultatelor evaluării riscurilor de spălarea banilor și finanțarea terorismului, utilizează abordarea bazată pe risc pentru stabilirea și punerea în aplicare a acțiunilor de gestionare și minimizare a riscurilor identificate, inclusiv prin alocarea resurselor tehnologice, materiale și umane corespunzătoare.

19. Banca păstrează și actualizează datele statistice necesare procesului de identificare și evaluare a riscurilor de spălarea a banilor și finanțarea a terorismului, care vor include cel puțin:

a) date despre mărimea, complexitatea, natura și volumul activității băncii;

b) date despre tipul, numărul și volumul produselor și serviciilor acordate, numărul și tipul clienților, rezident sau nerezident, tipul tranzacțiilor (operațiunilor) efectuate de aceștia, țările sau jurisdicțiile implicate;

c) date despre tipul clienților și tranzacțiilor cu grad de risc sporit identificate, numărul și volumul acestora;

d) tranzacțiile suspecte raportate către Serviciul Prevenirea și Combaterea Spălării Banilor;

e) date despre numărul instruirilor oferite, angajații participanți, persoanele testate, numărul auditărilor independente efectuate, neajunsurile identificate și sancțiunile aplicate.

20. Banca aplică măsurile de precauție simplificate și sporite în funcție de gradul de risc implicat, inclusiv ținând cont de tipul clientului, riscul de spălarea banilor și finanțarea terorismului identificat, țară (jurisdicție), relația de afaceri, produsul/serviciul oferit sau tranzacția efectuată, rețeaua de distribuție, etc.

Capitolul V MĂSURI DE PRECAUȚIE PRIVIND CLIENȚII

Secțiunea a 1-a Proceduri de acceptare a clientului

21. Procedurile de acceptare a clientului vor conține o descriere a clienților care par să expună banca la un risc sporit de utilizare a ei în scopul spălării banilor și finanțării terorismului. În vederea minimizării acestui risc, informația privind clienții trebuie examinată sub un șir de aspecte, cum ar fi experiența clienților în domeniul de activitate, țara de origine, poziția socială, conturile legate, activitățile desfășurate sau alți indicatori de risc stabiliți de bancă, ținând cont de Recomandările cu privire la abordarea bazată pe risc a clienților de către bănci în vederea prevenirii și combaterii spălării banilor și finanțării terorismului.

22. Procedurile de acceptare a clientului vor include mai multe etape în funcție de gradul de risc al acestuia, punând accent pe clientul cu venituri înalte a cărui sursă este neclară. Deciziile de începere, continuare sau încetare a relației de afaceri cu clientul cu un grad de risc sporit se iau de către persoana responsabilă în cadrul băncii sau de către conducătorul sucursalei prin coordonarea deciziei cu subdiviziunea internă a băncii responsabilă de implementarea și conformarea cu cerințele de prevenire și combatere a spălării banilor și finanțării terorismului.

23. Banca nu va intra în relații de afaceri și nu va continua relațiile existente cu clienții și/sau beneficiarii efectivi ai cărora sunt incluși în lista persoanelor, grupurilor și entităților implicate în activități teroriste și de proliferare a armelor de distrugere în masă ținând cont de prevederile art.34 alin.(11) din Legea nr.308 din 22.12.2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului.

24. Procedurile de acceptare a clientului nu trebuie să afecteze accesul publicului larg la serviciile bancare.

Secțiunea a 2-a Măsuri de identificare a clientului și beneficiarului efectiv

25. Banca aplică măsuri de identificare a clienților, precum și a beneficiarilor efectivi:

- a) până la inițierea relațiilor de afaceri;
- b) la efectuarea tuturor tranzacțiilor ocazionale, inclusiv cu utilizarea mijloacelor electronice, în valoarea de peste 20 de mii de lei, precum și dacă tranzacțiile se efectuează prin una sau mai multe operațiuni care au legături între ele, în valoare de peste 300 mii lei;
- c) atunci când există o suspiciune de spălarea banilor sau de finanțarea terorismului, independent de derogări, scutiri sau limite stabilite;
- d) atunci când există suspiciuni privind veridicitatea, suficiența și precizia datelor de identificare obținute anterior;
- e) prin derogare de la lit.a) și b), pe baza unei evaluări corespunzătoare a riscurilor, care demonstrează existența unui risc scăzut de spălarea banilor și de finanțarea terorismului, banca în calitate de prestator de servicii de plată și emitentă de monedă electronică conform Legii nr. 114 din 18.05.2012 cu privire la serviciile de plată și moneda electronică, cu excepția cazurilor de răscumpărare sau retragere a numerarului ce depășește suma de 2000 de lei, poate omite aplicarea măsurilor de precauție privind clienții referitoare la moneda electronică sau instrumentul de plată preplătit în cazurile de respectare a următoarelor condiții:
 - i. valoarea maximă depozitată electronic nu depășește suma de 5000 de lei;

- ii. valoarea transferurilor lunare nu depășește suma de 5000 de lei, iar pentru instrumentele de plată care pot fi utilizate doar pe teritoriul Republicii Moldova, aceasta poate fi majorată pînă la 10000 de lei;
- iii. instrumentul de plată este utilizat exclusiv pentru a achiziționa bunuri și servicii;
- iv. instrumentul de plată nu poate fi finanțat cu monedă electronică anonimă;
- v. emitentul (banca) efectuează o monitorizare suficientă a tranzacțiilor sau a relației de afaceri pentru a permite depistarea tranzacțiilor suspecte.

26. La identificarea clienților în cazurile prevăzute la pct.25 banca obține cel puțin următoarele informații:

- 1) pentru clienții - persoane fizice:
 - a) numele și prenumele;
 - b) data și locul nașterii;
 - c) 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);
 - d) adresa de domiciliu și/sau reședință;
 - e) ocupația, funcția publică deținută;
 - f) sursa venitului;
 - g) scopul preconizat de utilizare a contului (numărul și volumul tranzacțiilor, tipul tranzacțiilor, scopul și frecvența tranzacțiilor preconizate);
 - h) produsul și serviciul financiar solicitat;
- 2) pentru persoanele juridice și persoanele fizice întreprinzători individuali sau care practică alt tip de activitate:
 - a) denumirea, forma legală, statutul și dovadă de încorporare/înregistrare a persoanei juridice;
 - b) sediul/adresa principală de activitate;
 - c) numărul de identificare de stat (IDNO) și codul fiscal, conform certificatului de înregistrare și/sau extrasului din Registrul de stat eliberat de către organul abilitat cu dreptul de a efectua înregistrarea de stat;
 - d) adresa de corespondență, altă decât sediul (dacă există);
 - e) identitatea persoanei fizice împuternicită de a gestiona contul și care exercită control prin intermediul proprietății deținute sau prin alte căi (în cazul lipsei acestei informații, se indică administratorul persoanei juridice);
 - f) identitatea beneficiarului efectiv a persoanei juridice;
 - g) competențe ce reglementează și obligă persoana juridică;
 - h) natura și scopul activității, legitimitatea acestora;
 - i) scopul preconizat de utilizare a contului (numărul și volumul tranzacțiilor, tipul tranzacțiilor, scopul și frecvența tranzacțiilor preconizate);
- 3) pentru persoanele juridice care gestionează bunurile aflate sub administrare fiduciară (trust, fond de investiții și alte tipuri de aranjamente):
 - a) denumirea și dovada de încorporare/înregistrare;
 - b) sediul/adresa de activitate și țara de înregistrare;
 - c) natura, scopul și obiectul activității (ca exemplu: discreționar, testamentar, etc) ;
 - d) numele și prenumele fondatorului, administratorului, protectorului (dacă există), beneficiarilor sau claselor de beneficiari, și oricare altă persoană care exercită în ultimă instanță un control efectiv asupra aranjamentului legal stabilit;
 - e) descrierea scopului/activității aranjamentului legal (constituit formal, declarație de încredere);
 - f) scopul preconizat de utilizare a contului (numărul și volumul tranzacțiilor, tipul tranzacțiilor, scopul și frecvența tranzacțiilor preconizate);

27. La identificarea clienților, în baza riscului identificat, banca va obține suplimentar următoarele informații:

- 1) pentru clienții - persoane fizice:

- a) oricare alt nume utilizat (nume marital, nume deținut anterior sau porecla);
 - b) adresa de serviciu, codul poștal, adresa de email, numărul telefonului mobil;
 - c) statutul de rezident/nerezident;
 - d) genul (sexul);
 - e) numele angajatorului, dacă există;
 - f) sursa averii clientului;
 - g) sursa fondurilor care tranzitează contul și destinația acestora;
- 2) pentru persoanele juridice și persoanele fizice întreprinzători individuali sau care practică alt tip de activitate:
- a) identificatorul unic al companiei, dacă există;
 - b) numărul de telefon și fax;
 - c) informații privind identitatea persoanelor care dețin poziții de management superior;
 - d) raportul financiar;
 - e) sursa mijloacelor bănești parvenite în cont și destinația fondurilor care tranzitează contul.
- 3) pentru persoanele juridice care gestionează bunurile aflate sub administrare fiduciară (trust, fond de investiții și alte tipuri de aranjamente):
- a) numărul de telefon și fax;
 - b) informații privind identitatea persoanelor care dețin poziții de management superior, dacă este relevant;
 - c) sursa fondurilor;
 - d) destinația fondurilor care tranzitează contul.

28. În cazul efectuării operațiunilor de schimb valutar în numerar cu persoane fizice prin intermediul birourilor sale de schimb valutar și/sau aparatelor de schimb valutar, banca aplică măsuri de cunoaștere a clientului în conformitate cu prevederile capitolului III și IV din Regulamentul privind activitatea caselor de schimb valutar și hotelurilor în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului.

29. Banca identifică beneficiarul efectiv al clientului și aplică măsuri rezonabile și bazate pe risc pentru verificarea identității lui, astfel încât să aibă certitudinea că știe cine este beneficiarul efectiv pentru a înțelege structura proprietății și structura de control a clientului. Pentru identificarea beneficiarului efectiv banca aplică măsurile descrise la pct. 26 alin.(1) și în dependență de riscul identificat, suplimentar pct. 27 alin.(1).

30. La identificarea beneficiarului efectiv al clientului – persoană juridică, inclusiv în cazul celor cu structură de proprietate complexă (persoană juridică a căror proprietari direcți nu sunt persoane fizice), banca determină beneficiarul efectiv în baza documentelor de înregistrare corespunzătoare.

31. Nu este necesară identificarea și verificarea identității beneficiarului efectiv pentru clientul persoană juridică în cazul în care acesta sau proprietarul pachetului de control al acestuia este o societate cotate a căror valori mobiliare sunt acceptate spre tranzacționare pe o piață reglementată, cu obligația de dezvăluire publică a informației.

32. Banca determină dacă persoana fizică sau juridică care deschide contul de plăți sau inițiază o relație de afaceri activează în numele său (declarația persoanei privind beneficiarul efectiv), iar în cazul în care deschiderea contului sau inițierea relației de afaceri este efectuată de către persoana împuternicită, banca solicită procura, legalizată în modul stabilit de legislație. Banca aplică măsuri de identificare a persoanei împuternicite în conformitate cu prevederile prezentului Regulament. Declarația persoanei privind beneficiarul efectiv este completată de către beneficiarul efectiv sau de către persoana împuternicită și conține informația conform pct. 26 alin.(1) și în dependență de riscul identificat, suplimentar pct. 27 alin.(1) din prezentul Regulament.

33. La identificarea clientului banca verifică informația prezentată care se referă atât la client, cât și la beneficiarul efectiv.

34. Banca verifică identitatea clientului și a beneficiarului efectiv până la stabilirea relației de afaceri sau în momentul stabilirii relației de afaceri sau efectuării unei tranzacții prevăzute la pct.25 lit.b), iar în situațiile cu risc scăzut, conform pct.51 lit.a).

35. În vederea verificării informației prezentate la identificarea clienților și a beneficiarilor efectivi, banca utilizează documente obținute din surse sigure și independente, date și informații. Verificarea informației trebuie să fie proporțională riscului pe care clientul și tipurile de documente prezentate le impun. În acest scop, banca utilizează proceduri documentare și nedocumentare de verificare:

1) pentru clienții - persoane fizice – banca verifică informația pe baza documentelor din categoria celor mai greu de falsificat sau de obținut pe cale ilicită sub un nume fals (de exemplu, actele de identitate emise de o autoritate oficială, care includ o fotografie a titularului). Verificarea informațiilor care nu se pot proba cu actele menționate mai sus se va realiza în funcție de gradul de risc prin orice altă metodă, cum ar fi:

a) pentru confirmarea datei și locului de naștere – certificatul de naștere;

b) pentru confirmarea validității documentelor de identitate – prin certificatele eliberate (de exemplu, în baza registrelor de stat sau private) de autoritățile publice sau de alte persoane competente (de exemplu, notari, ambasade etc.);

c) pentru confirmarea adresei de reședință în cazul în care nu corespunde cu domiciliul – prin solicitarea facturilor pentru serviciile comunale, a actelor privind plata impozitelor, a informației de la autoritățile publice sau de la alte persoane;

d) pentru confirmarea informației prezentate după deschiderea contului – prin contactarea clientului prin telefon, fax sau e-mail (dacă există);

e) verificarea referinței furnizate de altă bancă/insituție financiară;

2) pentru clienții - persoane juridice și persoanele fizice întreprinzători individuali sau care practică alt tip de activitate – prin orice metodă corespunzătoare în funcție de gradul de risc, astfel încât banca să se asigure de veridicitatea informației, cum ar fi:

a) verificarea existenței legale a persoanei juridice și persoanei fizice întreprinzător individual sau care practică alt tip de activitate prin verificarea înscrisului în Registrul de stat al persoanelor juridice sau, după caz, într-un alt registru public sau privat, sau altă sursă sigură independentă (ca exemplu: avocați, contabili, etc).

b) obținerea unei copii a contractului de constituire sau memorandumului de asociere, contractului de parteneriat;

c) verificarea informației despre client în bazele de date publice sau private privind relațiile de afaceri existente;

d) revizuirea ultimelor rapoarte financiare (cu excepția cazului deschiderii contului persoanei juridice nou constituite și persoanei fizice întreprinzător individual sau care practică alt tip de activitate) și a conturilor supuse auditului extern, dacă este cazul;

e) efectuarea unei analize, fie individuale sau prin intermediul altei persoane, privind existența procesului de insolvență sau lichidare, vânzare, a altor probleme financiare potențiale;

f) obținerea referinței unei bănci cu care clientul a avut anterior relații de afaceri, dacă există;

g) contactarea clientului prin telefon sau fax, prin intermediul serviciilor poștale sau e-mail, verificarea informației plasate pe pagina web a clientului, dacă există, sau efectuarea unei vizite pe teren la sediul sau la altă adresă indicată de persoana juridică și persoana fizică întreprinzător individual sau care practică alt tip de activitate;

h) verificarea identificatorului unic al companiei și datele asociate în baza de acces publică;

3) pentru persoanele juridice care gestionează bunurile aflate sub administrare fiduciară (trust, fond de investiții și alte tipuri de aranjamente), banca verifică informația cel puțin prin obținerea copieii documentului care confirmă natura și existența legală a deținătorului de cont (ca exemplu: declarația de încredere, registrul organizațiilor de caritate, etc). Alte proceduri de verificare pot include:

a) confirmarea documentelor prezentate dintr-o sursă independentă, cu reputație bună și cunoscută, așa ca, companie de avocați, contabili;

b) obținerea unei referințe bancare până la stabilirea relației de afaceri;

c) accesarea sau căutarea în bazele de date private și publice sau alte surse independente și sigure;

- d) verificarea identității persoanelor autorizate și beneficiarului efectiv;
- 4) pentru verificarea identității beneficiarului efectiv - măsurile prevăzute la subpct. 1).
- 5) în cazul în care o persoană este împuternicită în numele clientului să deschidă cont sau să efectueze tranzacții, banca verifică identitatea acesteia, precum și identitatea persoanei în numele căreia activează, utilizând aceleași proceduri descrise în prezentul Regulament.

36. Banca atrage atenție specială pentru clienții care sunt identificați cu grad de risc sporit. Surse de informație pentru aplicarea măsurilor suplimentare de verificare pot include:

- a) confirmarea adresei permanente a clientului prin utilizarea documentelor oficiale, o referință a registrului/agenției de credit sau efectuarea unei vizite la domiciliu;
- b) referința personală (de exemplu, de către un client existent al băncii);
- c) obținerea unei referințe bancare sau grup bancar până la stabilirea relației de afaceri prin contactarea directă cu bancă cu referire la client;
- d) verificarea surselor de venit, a fondurilor și a averii identificate prin măsuri adecvate;
- e) verificarea angajării și funcției publice deținute.

37. Documentele prezentate în vederea identificării clientului și a beneficiarului efectiv, precum și în vederea verificării identității acestora, trebuie să fie valabile la data prezentării lor, iar copiile acestora se stochează/arhivează de către bancă corespunzător procedurilor interne stabilite.

38. Documentele se prezintă de către client în original sau în copie (fotocopie) legalizate în modul corespunzător, dacă altceva nu este prevăzut de legislație. În cazul prezentării documentelor în copie (fotocopie), banca solicită prezentarea originalelor documentelor pentru coroborarea informației și datelor prezentate. În cazul în care clientul nu se prezintă personal la identificare, banca solicită informațiile și documentele necesare ținând cont de prevederile pct.58 din prezentul Regulament.

39. Pe parcursul relației de afaceri banca revizuieste și actualizează informația cu privire la identificarea clienților și a beneficiarilor efectivi în funcție de riscul asociat. Aceasta poate actualiza informația ori de câte ori consideră necesar, dar cel puțin, pentru clienții cu grad de risc sporit - anual, iar pentru cei cu grad de risc scăzut - o dată la 3 ani. Clientul confirmă că datele și informațiile deținute de către bancă sunt actuale și corespund scopului și naturii relației de afaceri declarat/înregistrat.

Secțiunea a 3-a

Măsuri de monitorizare a activităților și tranzacțiilor

40. Banca monitorizează continuu activitățile, tranzacțiile (operațiunile) clientului sau relația de afaceri cu acesta. Acțiunile de monitorizare continuă cuprind:

- 1) determinarea tranzacțiilor ordinare (specifice) ale clientului;
- 2) examinarea minuțioasă a tranzacțiilor pe parcursul relației de afaceri pentru a avea siguranța că acestea sânt în corespundere cu informația disponibilă la bancă, cu activitatea și riscul asociat clientului. Examinarea tranzacțiilor presupune cel puțin ca banca să dispună de mecanisme/soluții automatizate pentru depistarea activităților, tranzacțiilor și persoanelor suspecte. Depistarea activităților, tranzacțiilor și persoanelor suspecte poate fi realizată prin stabilirea limitelor valorice ale tranzacțiilor pentru o grupă particulară sau categorie de operațiuni, conturi bancare. O atenție deosebită se acordă tranzacțiilor care depășesc aceste limite valorice și tranzacțiilor ce nu au scop economic clar (de exemplu, cele care par să nu aibă un sens economic sau care implică sume mari de bani ce nu corespund așteptărilor băncii vizând clienții respectivi sau nu sânt specifice tranzacțiilor obișnuite ale acestora);

3) verificarea faptului dacă documentele și informațiile acumulate în procesul monitorizării clienților și tranzacțiilor sânt actualizate și relevante, inclusiv pentru categoriile clienților sau relațiile de afaceri cu grad de risc sporit;

4) întocmirea unei note de monitorizare în care sunt evidențiate tranzacțiile efectuate (tipul, volumul, moneda, destinația, etc) și documentele confirmative prezentate și asociate acestora, ori de câte ori este necesar în dependență de riscul implicat. Pentru clienții cu grad de risc sporit, banca va întocmi astfel de notă, cel puțin trimestrial;

5) identificarea activităților, tranzacțiilor suspecte, inclusiv a celor potențiale, precum și a surselor mijloacelor bănești utilizate în aceste activități și tranzacții;

6) raportarea către persoana responsabilă a informației cu privire la riscurile identificate cu referire la conturile și tranzacțiile clienților, inclusiv pentru clienții cu grad de risc sporit.

7) monitorizarea în timp real a tuturor tranzacțiilor efectuate de clienți sau potențialii clienți pentru a depista persoanele, grupurile sau entitățile implicate în activități teroriste și de proliferare a armelor de distrugere în masă, inclusiv în scopul identificării plăților pentru prevenirea efectuării acestora cu încălcarea sancțiunilor, interdicțiilor sau altor restricții aplicate.

41. Banca acordă atenție sporită tuturor tranzacțiilor semnificative, complexe sau care au caracter neordinar (neobișnuit), care nu au un scop economic sau juridic clar. Banca examinează natura și scopul acestor tranzacții, iar constatările le documentează în scris și ia măsuri de precauție sporită în conformitate cu cerințele prezentului Regulament. În astfel de situații banca obține documente justificative la efectuarea tranzacțiilor și determină sursa mijloacelor bănești utilizate (contracte, facturi, documente de expediție, declarații vamale, certificate despre salariu, dări de seamă fiscale, rapoarte de activitate, alte documente).

42. Banca se abține de la executarea activităților și tranzacțiilor cu bunuri, inclusiv mijloace financiare, pentru un termen de până la 5 zile lucrătoare, la stabilirea suspiciunilor pertinente care pot indica despre acțiuni de spălare a banilor, infracțiuni asociate acestora, acțiuni de finanțare a terorismului sau a proliferării armelor de distrugere în masă, în curs de pregătire, de tentativă, de realizare ori deja realizate.

43. Banca aplică cerințele pct.42 la solicitarea Serviciului Prevenirea și Combaterea Spălării Banilor sau din proprie inițiativă prin decizia (ordinul) persoanei responsabile în bancă. La aplicarea cerințelor pct.42 din proprie inițiativă, banca informează imediat, dar nu mai târziu de 24 de ore, Serviciul Prevenirea și Combaterea Spălării Banilor despre decizia luată.

44. Banca în cazul aplicării cerințelor pct.42, la necesitate, solicită clientului furnizarea datelor și informației suplimentare, inclusiv a documentelor confirmative privind tranzacțiile efectuate, în scopul aplicării corespunzătoare a măsurilor de precauție, și în special, pentru înțelegerea scopului și a naturii relației de afaceri, precum și sursa bunurilor implicate.

45. Măsurile aplicate conform cerințelor pct. 42 încetează din oficiu în baza permisiunii scrise și confirmate de Serviciu Prevenirea și Combaterea Spălării Banilor.

46. Banca este obligată:

a) să nu deschidă cont, să nu stabilească relații de afaceri, să nu efectueze tranzacții cu clientul, în cazul în care banca nu poate asigura respectarea cerințelor pct.25-29, 34 și 35;

b) în cazul unei relații de afaceri existente, să termine relația de afaceri, în cazul în care banca nu poate asigura respectarea cerințelor pct.25-29, 34 și 35;

c) raportează circumstanțele indicate la lit.a) și b) Serviciului Prevenirea și Combaterea Spălării Banilor în conformitate cu Legea nr.308 din 22.12.2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului.

47. Banca nu va deschide și ține conturi anonime sau conturi pe nume fictive, nu va stabili sau nu va continua o relație de afaceri cu o bancă fictivă sau cu o bancă despre care se știe că permite unei bănci fictive să utilizeze conturile sale.

Secțiunea a 4-a **Informația obținută de la persoanele terțe**

48. Banca, poate să recurgă la informația care aparține persoanelor terțe, pentru a realiza măsurile prevăzute la pct. 25-27, 29, 34 și 35, în următoarele condiții:

a) banca dispune de posibilitatea de a obține imediat informațiile necesare aferente măsurilor prevăzute la pct. 25-27, 29, 34 și 35, deținute de către persoanele terțe;

b) banca adoptă și implementează proceduri eficiente privind accesul operativ la copiile datelor de identificare și la alte documente aferente măsurilor prevăzute la pct. 25-27, 29, 34 și 35, deținute de către persoanele terțe;

c) persoanele terțe sunt supravegheate adecvat și îndeplinesc cerințe similare celor prevăzute de Legea nr.308 din 22.12.2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului;

d) persoanele terțe nu sunt rezidente în jurisdicțiile cu risc sporit.

49. Banca are responsabilitatea finală privind realizarea măsurilor prevăzute la pct. 25-27, 29, 34 și 35, în cazul în care apelează la persoane terțe.

Capitolul VI MĂSURI DE PRECAUȚIE SIMPLIFICATE PRIVIND CLIENȚII

50. Banca aplică măsuri de precauție simplificată privind clienții atunci când, prin natura lor, pot prezenta un risc scăzut de spălare a banilor sau de finanțare a terorismului.

51. Măsurile de precauție simplificată privind clienții cuprind măsurile de precauție privind clienții prevăzute la pct. 25 și 28, în cadrul unei proceduri simplificate aferente riscului scăzut de spălare a banilor și de finanțare a terorismului, care include:

- a) verificarea identității clientului și beneficiarului efectiv după stabilirea relației de afaceri;
- b) actualizarea datelor de identificare conform pct.39;
- c) monitorizarea continuă a tranzacției sau a relației de afaceri conform pct.40 subpct.4);
- d) obținerea de informații privind scopul și natura relației de afaceri conform pct.26.

52. Banca, în baza evaluării proprii, stabilește factorii care generează riscuri scăzute de spălare a banilor și de finanțare a terorismului și care determină necesitatea aplicării măsurilor de precauție simplificată privind clienții, inclusiv dacă:

- a) clientul este o autoritate publică sau întreprindere de stat;
- b) clientul este o societate ale cărei valori mobiliare sânt tranzacționate pe o piață reglementată/ sistem multilateral de tranzacționare care impune cerințe pentru a asigura transparența adecvată a beneficiarului efectiv;
- c) clientul este rezident al jurisdicțiilor prevăzute la lit.d) și e) care îndeplinesc cerințele standardelor internaționale de prevenire și combatere a spălării banilor și a finanțării terorismului;
- d) țara de destinație (jurisdicția) dispune de un sistem eficient de prevenire și combatere a spălării banilor și a finanțării terorismului conform standardelor internaționale și este supusă regulat evaluării în acest sens de către organizațiile internaționale de profil;
- e) țara de destinație (jurisdicția) are un nivel redus de corupție și de criminalitate conform evaluărilor oficiale;
- f) produsele și serviciile financiare sunt limitate și bine definite pentru un cerc de clienți, cu scopul de a spori incluziunea financiară;

53. Banca nu va aplica măsuri de precauție simplificate în cazul existenței suspiciunii cu privire la spălarea banilor sau finanțarea terorismului.

Capitolul VII MĂSURI DE PRECAUȚIE SPORITE PRIVIND CLIENȚII

54. În vederea aplicării legislației în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului banca stabilește categoriile clienților, activitățile și tranzacțiile (operațiunile) ce prezintă un grad de risc sporit pe baza unor indicatori stabiliți în funcție de volumul activelor sau al veniturilor, tipul serviciilor solicitate, tipul activității desfășurate, circumstanțele economice, reputația țării de origine, plauzibilitatea explicațiilor oferite de client, limitele valorice prestabilite pe categorii de tranzacții.

55. Banca aplică măsuri de precauție sporită privind clienții în situații care, prin natura lor, pot prezenta risc sporit de spălare a banilor sau de finanțare a terorismului. Factorii care generează risc sporit sunt:

- 1) relația de afaceri este desfășurată în circumstanțe neobișnuite;
- 2) clienții nerezidenți;
- 3) persoane juridice care gestionează bunurile aflate sub administrare fiduciară sau au conturi deschise în acest scop;
- 4) persoane juridice care au acționari/fondatori persoane nominale sau au emise acțiuni la purtător;
- 5) persoanele juridice ce efectuează tranzacții semnificative în numerar;
- 6) structura de proprietate a persoanei juridice este neobișnuită și excesiv de complexă luând în considerare natura activității acesteia;
- 7) țările și/sau jurisdicțiile identificate de surse credibile (decizii, evaluări reciproce și/sau rapoarte, inclusiv de monitorizare a progresului, ale organizațiilor internaționale și agențiilor/grupurilor acestora) ce nu dispun de norme contra spălării banilor și finanțării terorismului ori dispun de norme inadecvate în acest sens;
- 8) țările și/sau jurisdicțiile asupra cărora au fost aplicate sancțiuni, embargouri, interdicții sau alte restricții de către autoritățile competente naționale și în baza actelor emise de către organizațiile internaționale;
- 9) țările și/sau jurisdicțiile identificate de surse credibile (decizii, evaluări reciproce și/sau rapoarte, inclusiv de monitorizare a progresului, ale organizațiilor internaționale și agențiilor/grupurilor acestora) ce reprezintă un risc sporit din cauza nivelului înalt de infraționalitate și de corupție;
- 10) țările și/sau jurisdicțiile identificate de surse credibile (decizii, evaluări reciproce și/sau rapoarte, inclusiv de monitorizare a progresului, ale organizațiilor internaționale și agențiilor/grupurilor acestora) ce furnizează finanțare sau suport activităților teroriste, sau pe teritoriul cărora activează organizații teroriste desemnate;
- 11) clienții care beneficiază de servicii/produse de „servicii bancare private”;
- 12) tranzacții care favorizează anonimatul (care pot implica și numerarul)
- 13) tranzacții sau relații de afaceri ne față în față (la distanță);
- 14) plăți primite de la părți necunoscute sau de la terțe părți;
- 15) relațiile bancare transfrontaliere (de corespondență bancară), inclusiv la efectuarea plăților prin intermediul acestor conturi (payable through accounts);
- 16) tranzacții sau relațiile de afaceri cu persoanele expuse politic;
- 17) în cazul tranzacțiilor electronice, dacă nu există informații suficiente despre identitatea expeditorului;
- 18) produsele noi și practicile comerciale noi, inclusiv mecanismele noi de distribuție și de utilizare a unor tehnologii noi sau în curs de dezvoltare atât pentru produsele noi, cât și pentru produsele preexistente;
- 19) alți factori identificați în cadrul evaluării riscurilor.

56. Banca, la evaluarea riscului de spălare a banilor și finanțare a terorismului asociat clienților, țărilor/jurisdicțiilor, a produselor/serviciilor oferite, tranzacțiilor și canalului de distribuție asociat, va lua în considerare și variabilele de risc implicate. Aceste variabile, fie luate singular sau în combinație, pot crește sau descrește riscul asociat. Exemple de astfel de variabile includ:

- a) scopul deschiderii contului de plăți sau inițierii relației de afaceri;
- b) nivelul activelor/mijloacelor bănești depozitate de un client sau volumul tranzacțiilor efectuate;
- c) frecvența sau durata relației de afaceri;

57. Măsurile de precauție sporită aplicate de bancă presupun:

- 1) obținerea informației suplimentare despre client (ca exemplu: ocupația, volumul activelor și/sau investițiilor preconizate, activitatea preconizată a fi desfășurată, natura relației de afaceri preconizate, scopul tranzacțiilor desfășurate sau preconizate a fi desfășurate, informația disponibilă

din bazele de date publice, etc) și actualizarea mai frecventă a informației cu privire la identitatea clientului și a beneficiarului efectiv;

2) obținerea informației suplimentare privind natura și scopul relației de afaceri preconizate;

3) obținerea informației suplimentare pentru stabilirea sau verificarea sursei mijloacelor bănești și a averii clientului;

4) obținerea informației privind raționamentul tranzacțiilor efectuate sau preconizate;

5) obținerea aprobării persoanei responsabile și/sau conducătorului sucursalei pentru stabilirea sau continuare a relației de afaceri;

6) monitorizarea sporită și permanentă a relației de afaceri, prin creșterea numărului controalelor aplicate și selectarea tipurilor de tranzacții ce necesită examinare suplimentară, pentru solicitarea de informații suplimentare necesare confirmării legalității tranzacțiilor și corespunderea acestora genului de activitate declarat;

7) solicitarea ca prima plată să fie efectuată de client prin intermediul unui cont deschis la o bancă care aplică cel puțin aceleași standarde și măsuri de precauție privind clientul;

8) implementarea sistemelor informatice specializate în scopul asigurării eficienței gestiunii informației cu referire la identificarea, analizarea și monitorizarea clienților și tranzacțiilor acestora, precum și raportarea către Serviciul Prevenirea și Combaterea Spălării Banilor a tranzacțiilor suspecte de spălare a banilor și finanțare a terorismului.

9) atenționarea clienților ale căror activități sau tranzacții impun un risc sporit de spălare a banilor și finanțare a terorismului despre necesitatea sporirii măsurilor de cunoaștere a partenerilor de afaceri, iar, după caz, despre terminarea relațiilor de afaceri sau refuzul în efectuarea operațiunilor cu astfel de clienți.

10) în cazul relațiilor transfrontaliere, limitarea sau terminarea desfășurării relației de afaceri sau efectuării tranzacțiilor, în cazul constatării aplicării neadecvate și nerespectării cerințelor de prevenire și combatere a spălării banilor și finanțării terorismului de către instituția parteneră/corespondentă;

11) măsuri suplimentare prevăzute la pct. 58 - 62.

58. În cazul prevăzut la pct.55 subpct.13) banca aplică clientului care nu se prezintă personal la identificare (de exemplu, în cazul relațiilor prin corespondență sau prin telefon, e-mail, internet sau alte mijloace electronice) măsuri de precauție sporită prin utilizarea de mecanisme de tipul semnăturii digitale, a metodelor biometrice, cheilor de sesiune etc. Cu ocazia primei vizite a clientului la sediile băncii, banca solicită documentele și informațiile conform cerințelor prezentului Regulament. Suplimentar, banca aplică una sau mai multe din următoarele măsuri:

a) solicită documentele de identificare a clientului eliberate de către o autoritate sau un organ competent, inclusiv a specimenului de semnătură, alte documente, după caz, pentru completarea dosarului clientului;

b) ia măsuri de protecție a autenticității documentelor în formă electronică transmise băncii;

c) utilizează informația prezentată de o bancă în care clientul are deschis un cont și care aplică cel puțin aceleași măsuri de cunoaștere a clientului și este supusă unei supravegheri efective;

d) solicită ca prima plată să fie efectuată în numele clientului printr-un cont de la o altă bancă, care aplică cel puțin aceleași măsuri de cunoaștere a clientului și este supusă unei supravegheri efective, la necesitate;

e) stabilirea și menținerea unei modalități de contact cu clientul, independentă de modalitatea prin care sînt realizate tranzacțiile cu clientul la distanță.

59. În relațiile transfrontaliere banca acumulează informații suficiente despre banca (instituția, organizația) corespondentă pentru a înțelege pe deplin sfera de activitate a acesteia. În acest scop banca:

1) obține cel puțin informațiile privind:

a) consiliul și organul executiv al instituției corespondente, activitățile ei cele mai importante, locul desfășurării acestora și măsurile aplicate de aceasta în vederea prevenirii și combaterii spălării banilor și finanțării terorismului;

b) beneficiarii efectivi ai instituției corespondente;

c) scopul deschiderii contului;

d) reputația instituției corespondente și calitatea supravegherii, inclusiv dacă aceasta a constituit subiectul unei investigații sau măsuri de remediere legate de spălarea banilor sau finanțarea terorismului, din sursele disponibile public;

2) evaluează cât de adecvate și eficiente sunt politicile instituției corespondente privind prevenirea și combaterea spălării banilor și finanțării terorismului;

3) stabilește relația de corespondență după obținerea aprobării persoanei responsabile în bancă;

4) stabilește documentar responsabilitățile în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului ale instituției corespondente, precum și faptul că instituția corespondentă verifică identitatea clienților săi, dispune de reguli eficiente de cunoaștere a clientului;

5) în contextul tranzacțiilor prin intermediul „conturi corespondente de transfer”, banca realizează acorduri prin care i se permite să verifice procedurile urmate de instituția corespondentă în vederea cunoașterii clienților și să transmită/primească, la solicitare, documente și informații aferente clienților, activității și tranzacțiilor acestora.

60. În relațiile de afaceri sau în cazul tranzacțiilor cu persoanele expuse politic banca aplică cel puțin următoarele măsuri:

1) dispune de un sistem de gestionare a riscului care:

a) permite determinarea dacă un client, un potențial client și/sau beneficiarul efectiv al acestuia este sau nu persoană expusă politic;

b) presupune solicitarea informației relevante de la client și/ sau beneficiarul efectiv al acestuia, existența unei referințe la o sursă de informație disponibilă public sau accesarea unei baze de date electronice comerciale cu informații despre persoanele expuse politic;

2) obține aprobarea persoanei responsabile în bancă pentru stabilirea relației de afaceri, iar în cazul în care clientul sau beneficiarul efectiv al acestuia a devenit ulterior persoană expusă politic, pentru continuarea relației de afaceri;

3) stabilește și verifică sursa averii și a mijloacelor bănești implicate în relația de afaceri sau în tranzacție;

4) solicită informații privind membrii familiei și persoanele asociate persoanei expuse politic. Banca aplică măsurile de precauție față de aceștia în aceeași măsură ca în cazul persoanelor expuse politic, conform cerințelor prezentului Regulament;

5) monitorizează sporit relația de afaceri și tranzacțiile efectuate de persoana expusă politic, inclusiv actualizează periodic informațiile despre acesta.

61. În cazul persoanelor juridice care stabilesc relația de afaceri în scopul investiției și administrării fiduciare a bunurilor, banca identifică persoana pe numele căreia se stabilește relația de afaceri, beneficiarul în numele căruia acționează persoana, precum și determină detaliile privind natura aranjamentelor existente. Măsurile de identificare vor cuprinde, de asemenea, pe fondatorii administrării fiduciare, orice alte persoane care au predat bunuri în administrare fiduciară, orice beneficiar al administrării fiduciare și persoanele cu drept de dispoziție asupra bunurilor.

62. În cazul în care clienții care acționează în numele altor persoane, indicați la pct.55 subpct.3) și 4) nu au dreptul să furnizeze băncii informația necesară privind beneficiarii efectivi, banca nu va deschide cont sau nu va stabili o altă relație de afaceri.

Capitolul VIII

CERINȚE PRIVIND INFORMAȚIILE CARE ÎNSOTESC TRANSFERURILE DE FONDURI

63. Prezentul capitol se aplică transferurilor de fonduri, în orice monedă, care sunt transmise sau primite de către o bancă sau de o bancă intermediară.

64. Prezentul capitol nu se aplică transferurilor de fonduri efectuate utilizând un card de plată, un instrument de monedă electronică sau orice alt dispozitiv digital sau informatic preplătit, cu caracteristici similare, în cazul în care sunt îndeplinite următoarele condiții:

a) cardul, instrumentul sau dispozitivul respectiv este utilizat exclusiv pentru a plăti bunuri sau servicii; și

b) numărul cardului, instrumentului sau dispozitivului respectiv însoțește toate transferurile care decurg din tranzacție.

Cu toate acestea, prezentul capitol se aplică atunci când un card de plată, un instrument de monedă electronică sau orice alt dispozitiv digital sau informatic preplătit, cu caracteristici similare, este folosit pentru a efectua un transfer de fonduri între persoane.

65. Prezentul capitol nu se aplică transferurilor de fonduri care implică retragerea de numerar de către plătitor din contul de plăți propriu.

Secțiunea a 1-a **Obligațiile băncii plătitorului**

66. Banca asigură că transferurile de fonduri sunt însoțite de următoarele informații cu privire la plătitor:

a) numele plătitorului;

b) numărul de cont de plăți al plătitorului; și

c) adresa plătitorului, numărul actului de identitate, numărul de identificare al clientului sau data și locul nașterii.

67. Banca asigură că transferul de fonduri este însoțit de următoarele informații cu privire la beneficiarul plății:

a) numele beneficiarului plății; și

b) numărul de cont de plăți al beneficiarului plății.

68. Prin derogare de la pct.66 lit. b) și pct.67 lit.b), în cazul transferurilor care nu se efectuează din sau către un cont de plăți (bancar), banca plătitorului se asigură că transferul de fonduri este însoțit de un cod unic de identificare a tranzacției în locul numărului (numerelor) de cont de plăți (bancar).

69. Banca, înainte de a transfera fondurile, verifică plenitudinea și exactitatea informațiilor menționate la pct. 66 pe baza documentelor, a datelor sau a informațiilor obținute dintr-o sursă credibilă și independentă, ținând cont de prevederile prezentului Regulament.

70. Banca asigură că toate transferurile de fonduri transfrontaliere sunt însoțite cu informații privind numele plătitorului și beneficiarului plății, și numărul contului sau un cod unic de identificare a tranzacției/plății, precum și completarea corespunzătoare a câmpului „destinații plății/transferului”.

71. În cazul transferurilor de credit pe baza unui fișier de grup efectuate de un singur plătitor către mai mulți beneficiari ai căror prestatori de servicii de plată activează în afara Republicii Moldova, pct. 66 nu se aplică transferurilor individuale grupate, cu condiția ca fișierul de grup să cuprindă informații complete cu privire la plătitor conform pct. 66 și ca transferurile individuale să fie însoțite de codul IBAN al plătitorului.

72. Banca nu va executa/efectua transferul de mijloace bănești dacă nu este asigurată respectarea cerințelor pct.66-71.

Secțiunea a 2-a **Obligațiile băncii beneficiarului plății**

73. Banca instituie proceduri eficiente, inclusiv, acolo unde este cazul, control a posteriori sau control în timp real, pentru a depista dacă acele câmpuri referitoare la informațiile privind plătitorul și beneficiarul plății din sistemul de plată și decontare, utilizat pentru efectuarea transferului de fonduri, au fost completate corespunzător cerințelor pct. 66 și 67 din prezentul Regulament.

74. Banca, înainte de a înregistra transferul de fonduri în contul beneficiarului plății sau de a pune mijloacele bănești la dispoziția acestuia, verifică plenitudinea și exactitatea informațiilor menționate la pct. 67 pe baza documentelor, a datelor sau a informațiilor obținute dintr-o sursă credibilă și independentă, ținând cont de prevederile prezentului Regulament.

75. Banca verifică plenitudinea și exactitatea informațiilor referitoare la beneficiarul plății, pe baza documentelor, a datelor sau a informațiilor obținute dintr-o sursă credibilă și independentă, ținând cont de prevederile prezentului Regulament, în cazul transferurilor de fonduri în cuantumul ce nu depășește limita stabilită la pct.25 lit.b) în următoarele situații:

a) când plata este efectuată în numerar sau în monedă electronică anonimă, dacă tranzacțiile par a avea legătură între ele;

b) când există motive întemeiate pentru a suspecta că este vorba despre o activitate de spălare a banilor sau de finanțare a terorismului.

76. Banca pune în aplicare proceduri eficiente bazate pe evaluarea riscurilor, pentru a determina dacă să execute, să respingă sau să suspende un transfer de mijloace bănești în cazul căruia informațiile complete privind plătitorul și beneficiarul plății lipsesc, inclusiv în cazul în care nu este completat corespunzător câmpul „destinații plății/transferului”.

77. Banca, dacă constată că la primirea transferului de fonduri, informațiile menționate la pct.66 și 67 lipsesc sau sunt incomplete respinge transferul sau solicită informațiile cerute privind plătitorul și beneficiarul plății, înainte înregistrării transferului de fonduri în contul beneficiarului plății sau de a pune mijloacele bănești la dispoziția acestuia, în funcție de riscul asociat.

78. În cazul în care instituția/banca care efectuează plata omite în mod regulat să furnizeze informațiile obligatorii cu privire la plătitor sau beneficiarul plății, banca beneficiară ia măsuri care pot consta, mai întâi, în emiterea unor avertismente și stabilirea unor termene-limită, înainte fie de a respinge orice transfer de fonduri care provine de la aceasta, fie de a decide, dacă este cazul, să restrângă sau să înceteze relația comercială cu respectiva instituție/bancă. Banca informează despre astfel de situații Serviciul Prevenirea și Combaterea Spălării Banilor conform actelor normative în vigoare.

Secțiunea a 3-a **Obligațiile băncii intermediare**

79. Banca instituie proceduri eficiente, inclusiv, acolo unde este cazul, control a posteriori sau control în timp real, pentru a depista dacă acele câmpuri referitoare la informațiile privind plătitorul și beneficiarul plății din sistemul de plată și decontare, utilizat pentru efectuarea transferului de fonduri, au fost completate corespunzător cerințelor pct. 66 și 67 din prezentul Regulament.

80. Banca asigură că transferurile de fonduri pe baza unui fișier de grup conține numărul contului de plată al plătitorului sau un cod unic de identificare a tranzacției/plății, iar fișierul de grup deține informațiile privind plătitorul și beneficiarul plății, care are trasabilitate completă.

81. Banca pune în aplicare proceduri eficiente bazate pe evaluarea riscurilor, pentru a determina dacă să execute, să respingă sau să suspende un transfer de mijloace bănești în cazul căruia informațiile cerute privind plătitorul și beneficiarul plății lipsesc, inclusiv în cazul în care nu este completat corespunzător câmpul „destinații plății/transferului”.

82. Banca, dacă constată că la primirea transferului de fonduri, informațiile menționate la pct.66 și 67 lipsesc sau sunt incomplete, fie respinge transferul sau solicită informațiile cerute privind plătitorul și beneficiarul plății înainte sau după transmiterea transferului de fonduri, în funcție de riscul asociat.

83. În cazul în care instituția/banca care efectuează transferul/plata omite în mod repetat să furnizeze informațiile cerute cu privire la plătitor sau beneficiarul plății, banca intermediară ia măsuri care pot consta, mai întâi, în emiterea unor avertismente și stabilirea unor termene-limită, înainte de respingerea oricărui transfer de fonduri care provine de la aceasta, fie de a decide, să restrângă sau să înceteze relația comercială cu respectiva instituție/bancă. Banca informează despre astfel de situații Serviciul Prevenirea și Combaterea Spălării Banilor conform actelor normative în vigoare.

84. Banca ia în considerare informațiile lipsă privind plătitorul sau beneficiarul plății ca factor pentru a evalua dacă transferul de fonduri sau orice tranzacție conexă este suspectă și dacă aceasta trebuie raportată Serviciului Prevenirea și Combaterea Spălării Banilor.

Capitolul IX RAPORTAREA ACTIVITĂȚILOR ȘI A TRANZACȚIILOR

85. Banca este obligată să informeze Serviciul Prevenirea și Combaterea Spălării Banilor despre:

1) bunurile suspecte, activitățile sau tranzacțiile suspecte de spălare a banilor, de infracțiuni asociate acestora 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;

2) activitățile sau tranzacțiile clienților realizate în numerar, printr-o operațiune cu o valoare de cel puțin 100 mii de lei (sau echivalentul acesteia) sau prin mai multe operațiuni în numerar care par a avea o legătură între ele - în decurs de 10 zile calendaristice;

3) tranzacțiile clienților realizate prin virament, printr-o operațiune cu o valoare de cel puțin 500 mii de lei (sau echivalentul acesteia) - cel târziu la data de 15 a lunii următoare lunii de gestiune.

Sunt exceptate de la obligațiile de raportare conform pct.(2) și (3) operațiunile între bănci, între bănci și Banca Națională a Moldovei, între bănci și Trezoreria de Stat, între Banca Națională a Moldovei și Trezoreria de Stat, precum și operațiunile de încasare a comisioanelor de la deservirea conturilor bancare și a spezelor bancare. În sensul prezentului alineat, noțiunea de „bancă” include doar entitățile raportoare conform Legii nr.308 din 22.12.2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului.

86. Banca va dispune de:

a) proceduri clare, reieșind din prevederile Legii nr.308 dn 22.12.2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului, aduse la cunoștința întregului personal, care prevăd raportarea de către personal a tuturor bunurilor suspecte, activităților sau tranzacțiilor suspecte de spălare a banilor, de infracțiuni asociate acestora și de finanțare a terorismului;

b) sisteme de depistare a activităților și tranzacțiilor suspecte conform criteriilor și indicilor stabilite, inclusiv de autoritățile competente;

c) proceduri de informare a persoanei responsabile în bancă și la necesitate a serviciului de securitate internă privind problemele ce țin de prevenirea și combaterea spălării banilor și finanțării terorismului.

87. Banca informează Banca Națională a Moldovei sau alte organe cu funcții de supraveghere a entităților raportoare în conformitate cu Legea nr.308 din cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului, despre bunurile, activitățile sau tranzacțiile suspecte de spălare a banilor, de infracțiuni asociate acestora și de finanțare a terorismului, și cazurile de fraudă ce afectează esențial siguranța, stabilitatea sau reputația băncii.

Capitolul X PĂSTRAREA DATELOR

88. Banca păstrează toate documentele și informațiile despre clienți și beneficiarii efectivi, obținute în cadrul măsurilor de precauție privind clienții, inclusiv copiile documentelor de identificare, arhiva conturilor și documentelor primare, corespondența de afaceri, rezultatele analizelor și cercetărilor efectuate privind identificarea tranzacțiilor complexe și neordinare, pe perioada activă a relației de afaceri și pe o perioadă de 5 ani după terminarea acesteia sau după data efectuării tranzacțiilor ocazionale și transferurilor de mijloace bănești.

89. Procedurile de păstrare a documentelor și informației vor include cel puțin următoarele, după caz:

1) ținerea unui registru al clienților și al beneficiarului efectiv identificați, care va conține cel puțin: denumirea/numele clientului; IDNO/IDNP, după caz; numărul contului; data deschiderii; data închiderii;

2) păstrarea tuturor documentelor primare, inclusiv a corespondenței de afaceri;

3) păstrarea dosarelor privind identificarea și verificarea clienților, a beneficiarilor efectivi privind monitorizarea operațiunilor clienților și păstrarea documentelor justificative aferente operațiunilor;

4) păstrarea informației privind tranzacțiile efectuate și notele de monitorizare aferente, inclusiv pentru cele complexe și neordinare;

5) arhivarea informației privind tranzacțiile și corespondența de afaceri în sistemele tehnologiilor informaționale (TI) și păstrarea arhivei în condiții de siguranță și disponibilitate operativă;

90. Banca asigură că, în caz de solicitare, documentele și informația privind identificarea și verificarea clienților, a beneficiarilor efectivi, privind monitorizarea operațiunilor clienților, inclusiv documentele justificative aferente operațiunilor sunt accesibile și disponibile autorităților competente. La solicitarea autorităților competente termenul privind deținerea și păstrarea informației aferentă clienților și operațiunilor acestora poate fi prelungit pentru o perioadă determinată în solicitare, dar nu mai mult de 5 ani.

Capitolul XI

CERINȚE PRIVIND SISTEMUL DE CONTROL INTERN

91. În scopul asigurării respectării programului privind prevenirea și combaterea spălării banilor și finanțării terorismului, banca va dispune de sisteme de control intern care vor asigura conformarea continuă a băncii actelor normative și programului intern în domeniu și vor contribui la minimizarea riscurilor aferente.

92. La deschiderea de filiale și sucursale pe teritoriul altor state, precum și pe parcursul activității acestora, banca va aplica cerințele de prevenire și combatere a spălării banilor și finanțării terorismului în conformitate cu sistemul de control intern propriu, politicile și procedurile interne și actele normative ale Republicii Moldova care implementează Recomandările FATF, în măsura în care legislația țării gazde permite. În cazul în care, în țara gazdă cerințele de prevenire și combatere a spălării banilor și finanțării terorismului sunt insuficiente, banca trebuie să asigure implementarea cerințelor actelor normative ale Republicii Moldova, în măsura în care legislația țării gazde permite. Dacă țara gazdă nu permite aplicarea corespunzătoare a cerințelor actelor normative ale Republicii Moldova, banca aplică măsuri suplimentare corespunzătoare în vederea micșorării riscului de spălare a banilor și finanțare a terorismului și informează Banca Națională a Moldovei în decurs de 2 luni despre acest fapt. Banca Națională poate efectua controale suplimentare pentru supravegherea respectării de către filialele și sucursalele deschise pe teritoriul altor state a actelor normative în vigoare aferente domeniului dat, iar dacă se constată nerespectarea acestora, Banca Națională a Moldovei poate limita activitatea sau retrage aprobarea emisă pentru deschiderea filialelor și sucursalelor deschise pe teritoriul altor state.

93. Banca comunică și implementează prevederile programului propriu pentru prevenirea și combaterea spălării banilor și finanțării terorismului în cadrul sucursalelor, filialelor și altor subdiviziuni deținute, inclusiv al celor situate în alte țări. În scopul prevenirii și combaterii spălării banilor și finanțării terorismului, banca efectuează schimb de date cu sucursalele, filialele și alte subdiviziuni deținute în condițiile respectării cerințelor actelor normative în vigoare.

94. Sistemul de control intern trebuie să includă cel puțin următoarele elemente:

1) efectuarea de către personalul băncii sau de o persoană independentă a auditului în vederea verificării respectării programului privind prevenirea și combaterea spălării banilor și finanțării terorismului. Funcțiile auditului în acest scop sunt:

a) evaluarea independentă a procesului aplicat de identificare, evaluare și monitorizare a riscurilor de spălare a banilor și finanțarea terorismului, precum și a mecanismului utilizat de minimizare a riscurilor identificate;

b) evaluarea independentă a programului privind prevenirea și combaterea spălării banilor și finanțării terorismului și a respectării cerințelor legislației în vigoare;

c) monitorizarea activității personalului prin testarea conformării;

- d) testarea tranzacțiilor în caz de necesitate;
 - e) informarea organelor de conducere privind rezultatele verificării;
- 2) desemnarea unui membru din cadrul organului executiv al băncii, responsabil de asigurarea conformării programelor privind prevenirea și combaterea spălării banilor și finanțării terorismului cu cerințele legislației și aplicării lor adecvate (în continuare – persoană responsabilă). În acest scop persoana responsabilă are următoarele atribuții:
- a) acordă consultații angajaților băncii în problemele ce apar în timpul realizării programului privind prevenirea și combaterea spălării banilor și finanțării terorismului, inclusiv în ce privește identificarea și examinarea clienților băncii și evaluarea riscului de spălare a banilor și finanțare a terorismului;
 - b) aprobă tranzacțiile semnificative ale clienților cu grad de risc sporit (sau delegarea atribuției de aprobare conducătorului sucursalei, după caz);
 - c) ia decizii în baza informației primite;
 - d) întreprinde măsuri privind raportarea Serviciului Prevenirea și Combaterea Spălării Banilor a informației în conformitate cu legislația în vigoare;
 - e) organizează instruirea angajaților băncii în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului;
 - f) prezintă, cel puțin o dată la 2 ani, consiliului băncii Raport privind rezultatele evaluării riscurilor de spălare a banilor și finanțării terorismului întocmit conform cerințelor prezentului Regulament și a planului de minimizare a riscurilor identificate;
 - g) prezintă în scris, cel puțin o dată pe an, consiliului băncii un raport privind rezultatele realizării programului privind prevenirea și combaterea spălării banilor și finanțării terorismului;
 - h) colaborează cu serviciul de audit în vederea îndeplinirii scopului acestuia privind verificarea conformării activității băncii la legislația în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului;
 - i) îndeplinește alte funcții în corespundere cu prezentul Regulament și documentele interne ale băncii;
- 3) prevederi interne privind răspunderea angajaților care în mod intenționat nu informează/raportează despre activitățile sau tranzacțiile suspecte persoana responsabilă, serviciul securității sau direct autoritatea competentă și/sau contribuie personal la efectuarea operațiunilor de spălare a banilor și finanțare a terorismului.

95. Banca va dispune de programe de selectare și instruire continuă a personalului în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului. Banca asigură deținerea de către personalul și persoana responsabilă în bancă a cunoștințelor, calităților și abilităților corespunzătoare pentru îndeplinirea eficientă a responsabilităților de conformare la cerințele de prevenire și combatere a spălării banilor și finanțării terorismului.

96. Programele de selectare și instruire indicate la pct.95 vor cuprinde diverse aspecte ale procesului de prevenire și combatere a spălării banilor și finanțării terorismului și obligațiunile conform legislației în domeniu, inclusiv:

- a) instruirea personalului nou angajat referitor la importanța și cerințele de bază ale programelor respective;
- b) instruirea personalului de „prima linie” (angajații care nemijlocit intră în contact cu clienții) referitor la identificarea clienților, verificarea identității acestora, monitorizarea conturilor/tranzacțiilor clienților existenți pe bază continuă, depistarea indicilor și raportarea activităților și tranzacțiilor suspecte și a celor supuse raportării;
- c) actualizarea regulată a responsabilităților personalului;
- d) noile tehnici, metode și tendințe de spălare a banilor și finanțare a terorismului;
- e) nivelul implicării personalului în procesul de prevenire și combatere a spălării banilor și finanțării terorismului.

Conținutul și programul instruirii personalului trebuie să fie adaptat la necesitățile individuale ale băncii.

Capitolul XII

CERINȚE PRIVIND APLICAREA MĂSURILOR RESTRICTIVE INTERNAȚIONALE

97. Banca aplică imediat măsuri restrictive în privința bunurilor, inclusiv a celor obținute din sau generate de bunuri care aparțin sau sunt deținute ori controlate, direct sau indirect, de persoanele, grupurile și entitățile implicate în activități teroriste și de proliferare a armelor de distrugere în masa care fac obiectul măsurilor restrictive, precum și de persoanele juridice care aparțin sau sunt controlate, direct sau indirect, de aceste persoane, grupuri și entități.

98. Pentru punerea în aplicare a măsurilor restrictive conform pct.97, banca elaborează proceduri și reguli interne care trebuie să includă cel puțin următoarele elemente:

a) proceduri de elaborare și actualizare a listei persoanelor, grupurilor și entităților implicate în activități teroriste și de proliferare a armelor de distrugere în masă care fac obiectul măsurilor restrictive internaționale (inclusiv prin utilizarea bazelor de date existente), conform cerințelor Legii nr.308 din 22.12.2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului și Legii nr.25 din 04.03.2016 privind aplicarea măsurilor restrictive internaționale;

b) proceduri de verificare/depistare a persoanelor sau entităților desemnate și a tranzacțiilor (operațiunilor) în care sunt implicate bunuri, aplicabile potențialilor clienți, clienților existenți și solicitanților de tranzacții ocazionale și de transfer a mijloacelor bănești;

c) competențele persoanelor cu responsabilități în implementarea procedurilor și regulilor interne pentru punerea în aplicare a măsurilor restrictive internaționale de blocare a fondurilor;

d) procedurile de informare/raportare, intern și către autoritățile competente (Serviciul Prevenirea și Combaterea Spălării Banilor, Serviciul de Informații și Securitate, Ministerul Afacerilor Externe și Integrării Europene și Ministerul Finanțelor).

99. Banca la identificarea bunurilor care aparțin sau sunt deținute ori controlate, direct sau indirect, de persoanele, grupurile și entitățile implicate în activități teroriste și de proliferare a armelor de distrugere în masa care fac obiectul măsurilor restrictive, întreprinde succesiv următorii pași:

a) prin decizia (ordinul) persoanei responsabile în bancă, se abține, pentru un termen nedeterminat, de la executarea activităților și tranzacțiilor în favoarea sau beneficiul, direct sau indirect, al persoanelor, grupurile și entitățile implicate în activități teroriste și de proliferare a armelor de distrugere în masa care fac obiectul măsurilor restrictive;

b) informează imediat, dar nu mai târziu de 24 ore, Serviciul Prevenirea și Combaterea Spălării Banilor și Serviciul de Informații și Securitate despre abținerea, pentru un termen nedeterminat, de la executarea activităților și tranzacțiilor în favoarea sau beneficiul, direct sau indirect, al persoanelor, grupurile și entitățile implicate în activități teroriste și de proliferare a armelor de distrugere în masa care fac obiectul măsurilor restrictive. Informația transmisă în adresa autorităților menționate va cuprinde cel puțin următoarele elemente:

- i. date și informații (nume/denumire; IDNO/IDNP, dacă există; țara de origine/rezidență; lista autorității/organizației la care face referință măsura restrictive aplicată, etc) despre persoana, grupul sau entitatea identificată;
- ii. date și informații (volumul; moneda; destinatarul; destinația, etc) despre bunul identificat;
- iii. informarea despre decizia persoanei responsabile în bancă cu privire la abținerea, pentru un termen nedeterminat, de la executarea activităților și tranzacțiilor cu referire la bunul identificat;
- iv. solicitarea de a furniza opinia scrisă în decurs de 5 zile, conform legislației în vigoare, despre necesitatea menținerii sau nu a măsurilor restrictive;

c) dacă este cazul, banca acceptă plăți suplimentare, efectuate de o parte terță, sau majorarea valorii bunurilor identificate și extinde aplicabilitatea măsurii de abținere asupra bunurilor, ținând cont de cerințele pct.99 lit.a), precum și informează despre acest fapt autoritățile menționate ținând cont de cerințele pct. 99 lit.b);

d) la primirea răspunsului în formă scrisă de la cel puțin una dintre autoritățile sesizate (în cazul opiniilor diferite ale autorităților sesizate, banca aplică măsura restrictivă cea mai dură, respectiv solicitarea de aplicare a măsurilor restrictive), banca întreprinde următoarele:

- i. în cazul opiniei despre necesitatea neaplicării măsurilor restrictive - prin decizia (ordinul) persoanei responsabile în bancă, măsura de abținere se anulează/abrogă;
- ii. în cazul opiniei despre necesitatea de aplicare a măsurilor restrictive:
 - prin decizia (ordinul) persoanei responsabile în bancă, bunurile sunt blocate;
 - dacă este cazul, banca acceptă plăți suplimentare, efectuate de o parte terță, sau majorarea valorii bunurilor identificate și extinde aplicabilitatea măsurii de blocare a acestora și informează despre acest fapt autoritățile menționate la pct. 99 lit.b);
 - se informează suplimentar despre decizia luată Ministerul Afacerilor Externe și Integrării Europene și Ministerul Finanțelor, ținând cont de cerințele pct.99 lit.b) cifra (i) și (ii);

e) informează Banca Națională a Moldovei despre măsura restrictivă aplicată, ținând cont de cerințele pct.99 subpct.b) cifra (i) și (ii);

f) prin dispunerea încheierii/hotărârii instanței de judecată sau altei autorități competente, bunurilor blocate li se atribuie statutul indicat în încheiere/hotărâre.

100. Banca asigură monitorizarea permanentă a Monitorului Oficial precum și paginilor web oficiale ale Organizației Națiunilor Unite, Uniunii Europene, Serviciului de Informații și Securitate și Ministerului Afacerilor Externe și Integrării Europene, pentru asigurarea aplicabilității corespunzătoare a măsurilor restrictive asupra persoanelor, grupurilor și entităților implicate în activități teroriste și de proliferare a armelor de distrugere în masă.

101. Banca nu stabilește și nu continuă relația de afaceri cu persoanele, grupurile sau entitățile implicate în activități teroriste și de proliferare a armelor de distrugere în masă. Despre refuzul de a stabili sau a continua relația de afaceri cu acestea, banca informează Serviciul Prevenirea și Combaterea Spălării Banilor ținând cont de prevederile legale în vigoare.

Capitolul XIII **MĂSURI DE REMEDIERE ȘI SANCTIUNI**

102. În cazul în care se constată încălcarea prevederilor prezentului Regulament, a obligațiilor prevăzute de legislația privind prevenirea și combaterea spălării banilor și finanțării terorismului, Banca Națională a Moldovei poate aplica măsuri de remediere și sancțiuni în conformitate cu art.35 alin.(2) din Legea nr.308 din 22.12.2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului și art.141 din Legea nr.202 din 06.10.2017 privind activitatea băncilor.

103. În scopul lichidării încălcărilor și neajunsurilor constatate, precum și a condițiilor ce favorizează comiterea acestora Banca Națională a Moldovei, pe lângă măsurile de remediere și sancțiunile menționate la pct.102, poate dispune următoarele măsuri:

a) să prescrie modificarea programelor privind prevenirea și combaterea spălării banilor și finanțării terorismului;

b) să prescrie efectuarea unei evaluări repetate a riscurilor de spălare a banilor și finanțare a terorismului;

c) să prescrie întocmirea unui nou plan de minimizare a riscurilor identificate de spălare a banilor și finanțare a terorismului;

d) să prescrie aplicarea măsurilor de precauție sporită de cunoaștere a clienților pentru produse, servicii, tranzacții (operațiuni) ori clienți, în cazul în care programul privind prevenirea și combaterea spălării banilor și finanțării terorismului stabilește aplicarea de măsuri standard de cunoaștere a clienților;

e) să prescrie înlocuirea persoanei responsabile.